SECURITY ENHANCEMENT IN P2P 3D STREAMING OVER THIN MOBILE DEVICES

A thesis submitted to the

University of Petroleum and Energy Studies

For the Award of

Doctor of Philosophy

in

Computer Science and Engineering

BY

P Srikanth

December 2021

Supervisor

Dr. Adarsh Kumar

SCHOOL OF COMPUTER SCIENCE

University of Petroleum and Energy Studies

Energy Acres, P.O. Bidholi via Prem Nagar,

Dehradun, 248007: Uttarakhand, India.

SECURITY ENHANCEMENT IN P2P 3D STREAMING OVER THIN MOBILE DEVICES

A thesis submitted to the

University of Petroleum and Energy Studies

For the Award of

Doctor of Philosophy

in

Computer Science and Engineering

BY

P Srikanth

SAP ID : 500033300

December 2021

Supervisor

Dr. Adarsh Kumar

Senior Associate Professor

Dept. of Systemics, SoCS

University of Petroleum and Energy Studies

SCHOOL OF COMPUTER SCIENCE

University of Petroleum and Energy Studies

Energy Acres, P.O. Bidholi via Prem Nagar,

Dehradun, 248007: Uttarakhand, India.

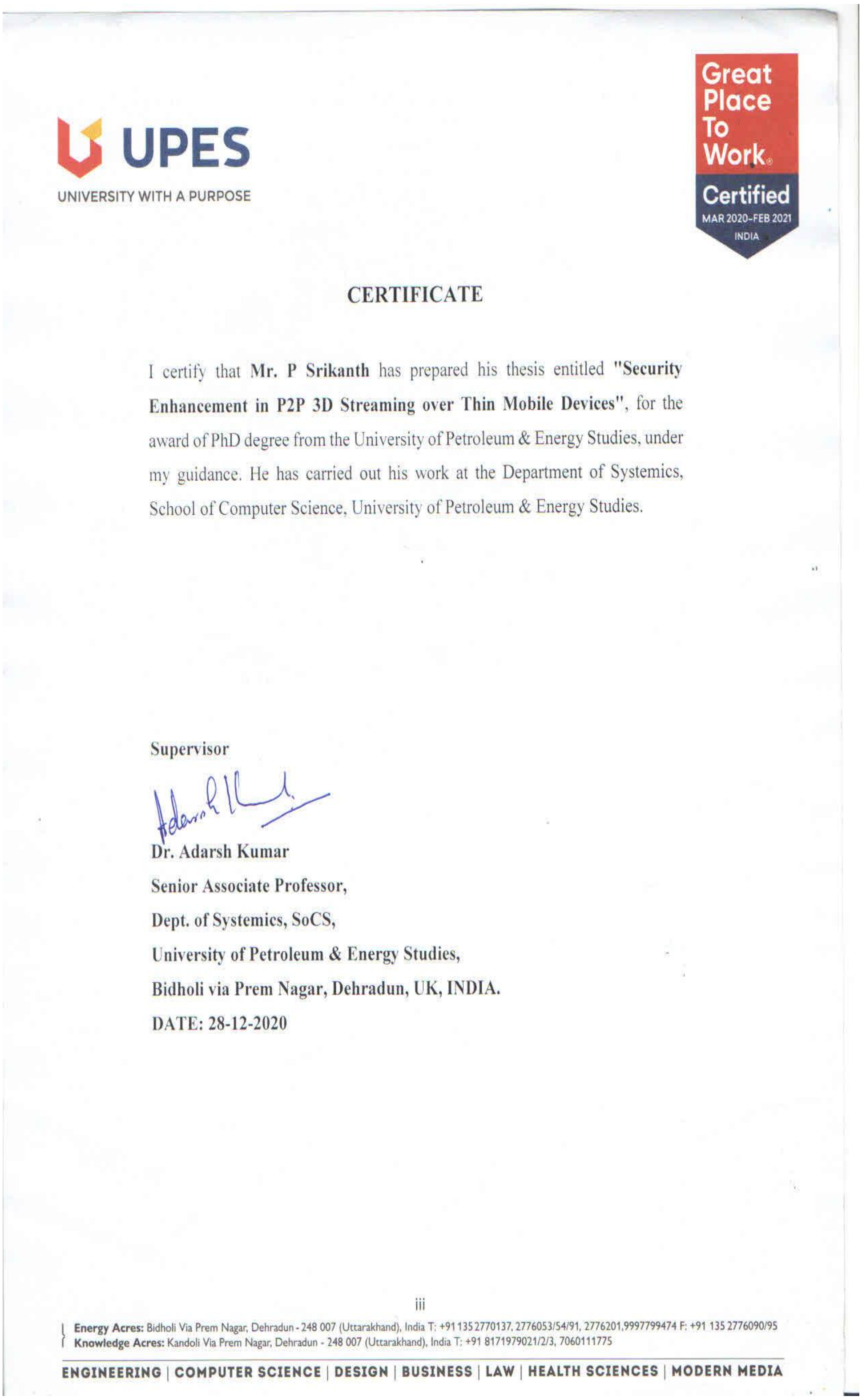
DECLARATION

I declare that the thesis entitled **"Security Enhancement in P2P 3D Streaming over Thin Mobile Devices"** has been prepared by me under the Supervision of Dr. Adarsh Kumar, Senior Associate Professor, Department of Systemics, School of Computer Science at University of Petroleum & Energy Studies. No part of this thesis has previously formed the basis for awarding any degree or fellowship.

P Srikanth

School of Computer Science,
University of Petroleum & Energy Studies,
Bidholi via Prem Nagar, Dehradun, UK, INDIA.
DATE: 28-12-2020

CERTIFICATE



UPES
UNIVERSITY WITH A PURPOSE

Great Place To Work® Certified
MAR 2020-FEB 2021
INDIA

CERTIFICATE

I certify that **Mr. P Srikanth** has prepared his thesis entitled **"Security Enhancement in P2P 3D Streaming over Thin Mobile Devices"**, for the award of PhD degree from the University of Petroleum & Energy Studies, under my guidance. He has carried out his work at the Department of Systemics, School of Computer Science, University of Petroleum & Energy Studies.

Supervisor

Dr. Adarsh Kumar
Senior Associate Professor,
Dept. of Systemics, SoCS,
University of Petroleum & Energy Studies,
Bidholi via Prem Nagar, Dehradun, UK, INDIA.
DATE: 28-12-2020

ABSTRACT

Massive growth in virtual environment applications in recent years has resulted in the development of 3D Streaming. The 3D streaming applications are intended to leverage client-server architecture. However, numerous studies have revealed that client-server architecture has various pitfalls. Thus, 3D streaming applications move towards the Peer to Peer (P2P) environment. The P2P 3D streaming applications are empowered by leveraging mobile devices and wireless networking. The advancement in mobile technology witnessing the significant growth in thin mobile devices applications includes the virtual walkthrough, augmented reality, media streaming, massively multiplayer online games, social networks and many more. However, 3D Streaming over thin mobile devices has to deal with a dynamic environment resulting in players' mobility, connection breakages and security. As a result, 3D Streaming over thin devices is related to selecting the trustworthy partner and content protection strategies to determine the partners' trust, enabling the required 3D data to stream in a protected manner to the requesters quickly and effectively.

The present research proposes a trustworthy partner selection and content protection scheme. Primarily, the thesis introduces P2P 3D Streaming over thin mobile devices. Further, a detailed literature review has been conducted and found some techniques provides the better trust assessment as an absolute trust. Further, it has been observed that lack of uncertainty trust assessment models are employed and requires improvement. Similarly, content protection using the watermarking scheme provides better security. Moreover, it has been observed that most of the approaches are used DWT that suffers the geometric and non-geometric attacks. Additionally, most schemes use the fixed-size watermark information embedded in the host image. Thus, variable size watermark information embedding is still open for Anaglyph 3D images. Hence, the proposed framework includes the trustworthy partner selection scheme using improved three-valued subjective logic (I-3VSL) with Trustwalker (TW) algorithm and content protection for Anaglyph 3D images using

DWT_HD_SVD and particle swarm optimization to determine the optimized scaling factor.

The I-3VSL model assesses trust using direct and indirect trust assessment strategies. Direct trust evaluates the trust of the known players, whereas indirect trust is evaluated through the reputation and recommendations from a friend of a friend that propagates the trust. However, the multiple players' reputations and recommendations that track the opinions of the various paths then perform the trust fusion. Further, the TW algorithm is designed leveraging I-3VSL that computes the trust between the trustor to a selected trustee. The TW algorithm is created using the iterative approach, and it performs the one to many trust assessment. The TW algorithm computes the trust in depth limited breadth-first search (BFS) fashion, and it provides the faster execution such as $O(n^2)$. Further, the trusted network is designed by leveraging the Travian dataset, then the performance of I-3VSL with TW is validated by comparing 3VSL with AT Algorithm. The I-3VSL with TW algorithm provides the 10% enhancement in accuracy and trust assessment over the 3VSL with AT.

Conversely, the content protection algorithm is designed to protect the red-cyan Anaglyph 3D images. These images are viewed through thin mobile devices such as red-cyan glasses. The red-cyan and other Anaglyph 3D images are protected by designing a watermarking system such as DWT_HD_SVD. The proposed watermarking works with the variable sizes of the watermark logos. Initially, the Anaglyph 3D images are created from stereoscopic images. The stereoscopic image consists of the left and right images with slight differences. From the left image, extract the red color and the right image, extract the green and blue colors that generate the cyan color image. Then combine these two images with incorporating the depth as a third dimension produces the Anaglyph 3D image. The proposed watermarking scheme extracts the blue color channel from the Anaglyph 3D image then decompose that image using 3D DWT. The 3D DWT decomposes the image into 8-subbands to select the LLL sub-band. After that, apply the HD on LLL that produces the H matrix and then use the SVD on H and the watermark logo. Further, the PSO algorithm is applied to select the optimized embedding scaling factor. Then perform the embedded operation to incorporate the watermark logo into the Anaglyph image. Further, it uses various geometric and non-geometric attacks on the watermarked image and then performs the extraction operation. The performance of the proposed watermark is validated through MSE, PSNR, SSIM and NCC. The proposed approach provides high robustness under various attacks that enhance 2% of the robustness over the existing approach. Similarly, assess the imperceptibility against multiple attacks that produces the 10% improvement over the current watermarking scheme.

In a gist, the present research program "Security enhancement in P2P 3D Streaming over the Thin Mobile devices" provided the framework along with approaches to employ the benefits of trustworthy partner selection and protecting the Anaglyph 3D images effectively in virtual online games.

ACKNOWLEDGEMENTS

First and foremost, I express my deepest love, appreciation, and gratitude to God for providing me with grace, wisdom, good health, a loving family, an exceptional supervisor, and a lovely working environment during my research work.

I express my heartfelt gratitude and profound admiration to my research supervisor, Dr. Adarsh Kumar, Senior Associate Professor, Department of Systemics, SoCS, University of Petroleum & Energy Studies, for his enthusiasm, intriguing guidance, and endless support with my research work. His suggestions were always valuable to me, not just in research but also in everyday life. My research work's quality has steadily increased under his supervision. He taught me how to comprehend a problem (in all aspects) and investigate the best feasible solutions. I am inspired by his humility, positivism, sincerity, and diligence every instant of my life. I hope to be as honest and disciplined as he is for the rest of my life. This PhD would not have been possible without his ongoing assistance, mentoring, and critique.

I like to express my profound gratitude to Dr. Amit Aggarwal and Dr. Venkatadri M. for their significant support during the first step of this voyage. I'm especially thankful to Dr. Hanumat G. Sastry for his encouragement as a colleague and a friend. His thoughts and recommendations are very informative during all of the conversations. I feel happy and fortunate to have a professor like him who allows me to explore various aspects of research in my unique approach. I respect how compassionate and constructive he has been to me.

I like to appreciate my friends and colleagues at UPES, Dehradun, especially Dr. Neelu Jyoti Ahuja, Dr. Sunil Kumar, Dr. Prem Kumar, Mr. Saurabh Jain, and Mr. Deepak Kumar Sharma, for their invaluable assistance during this voyage. I would like to thank everyone whose names have not been stated individually but who have assisted me directly or indirectly in this effort.

I am blessed with a beautiful and supportive family. I am eternally grateful to my father, mother, elder sister Ms. Shobha Rani, younger brother Mr. Praveen

Kumar, Ms. Soujanya, Mr. Dhanunjaya, Mr. Naveen Kumar, Mr. Nagaraju, Ms. Lavanya and my nephews and niece. I'd also want to express my sincere gratitude to Lasya and my cheeky son Asrith for always believing in me and supporting me to pursue my aspirations.

My Wife has been at my side every step of the way during my PhD, and without whom, I would not have had the strength to continue on this journey. She retains my hand even if she isn't around. She is the one person who understands the secret to my happiness and has given my life meaning. It's tough to express my feelings for the person who works relentlessly every day to stay motivated.

P SRIKANTH

TABLE OF CONTENTS

DECLARATION...ii

CERTIFICATE iii

ABSTRACT...iv

ACKNOWLEDGEMENTS vii

TABLE OF CONTENTS ix

LIST OF FIGURES xiii

LIST OF TABLES xv

LIST OF SYMBOLS AND NOTATIONS...xvi

LIST OF ABBREVATIONS...xix

LIST OF PUBLICATIONS xxiii

1. INTRODUCTION...1

1.1. An Overview: 3D Streaming 2
1.2. P2P 3D Streaming Characteristics 3
1.3. P2P 3D Streaming Applications..5
1.4. Challenges and Issues 6
1.5. Research Motivation 8
1.6. Research Objective..8
1.7. Thesis Contribution 9
1.8. Thesis Navigation 10
1.9. Summary 11

2. LITERATURE REVIEW ON TRUST ASSESSMENT AND CONTENT PROTECTION...12

2.1. Review on Trust Assessment 12
2.1.1. Significance of trust models...12
2.1.2. Definition of trust..13
2.1.3. Significance of reputation models 15
2.1.4. Definition of reputation..16
2.1.5. Trust scope 16

2.1.6. Trust properties 18
2.1.7. Trust information sources 20
2.1.8. Trust models 21
2.1.8.1. Topology based trust model (TTM) 21
2.1.8.2. Interaction based trust model (ITM) 22
2.1.8.3. Hybrid trust model (HTM) 23
2.1.8.4. PageRank-based trust model (PRTM) 23
2.1.8.5. Probability-based trust model (PBTM) 24
2.1.8.6. Subjective logic-based trust model (SL) 24
2.1.8.7. Three-valued subjective logic (3VSL) 25
2.1.9. Trust propagation models 26
2.1.9.1. Trust reputation models 26
2.1.9.2. Visualization models 32
2.1.10. Analysis 32
2.1.11. Critical analysis 34
2.2. Review on Content Protection 35
2.2.1. Content protection 36
2.2.1.1. Encryption 37
2.2.1.2. Digital right management (DRM) 37
2.2.1.3. Digital fingerprinting 38
2.2.1.4. Digital watermarking 38
2.2.2. Significance of digital watermarking 40
2.2.3. Provisions for digital watermarking 43
2.2.4. Classification of digital watermarking 45
2.2.4.1. Content-based watermarking 46
2.2.4.2. Human perception 47
2.2.4.3. Application 48
2.2.4.4. Domain 48
2.2.4.5. Comparison between spatial and transformation domains . 53
2.2.5. Classification of watermark extraction methods 54
2.2.6. State-of-the-art on 3D Anaglyph watermarking methods 54
2.2.6.1. Watermarking techniques on 3D Anaglyph images 55
2.2.6.2. Watermarking techniques on 3D Anaglyph videos 58
2.2.7. Critical analysis 63

2.3. Summary 63

3. PROPOSED FRAMEWORK FOR TRUSTWORTHY PARTNER SELECTION SCHEME 65

3.1. Theoretical Framework 65

3.2. Discounting Operation 66

3.2.1. Improved discounting operation 67

3.3. Combining Operation 68

3.4. Expected Belief 70

3.5. Design of Network Structure 70

3.5.1. Arbitrary network topology 73

3.6. Design of TrustWalker (TW) Algorithm 74

3.6.1. Analysis of time complexity 77

3.7. Summary 78

4. PROPOSED FRAMEWORK FOR ROBUST WATERMARKING SCHEME 79

4.1. 3D Anaglyph Image 79

4.2. Theoretical Framework 81

4.2.1. 3D Discrete wavelet transformation 81

4.2.2. Hessenberg decomposition 84

4.2.3. Singular value decomposition 84

4.2.4. Particle swarm optimization 85

4.3. Proposed Watermarking Scheme 86

4.3.1. Watermarking embedded procedure 88

4.3.2. Watermarking extraction procedure 89

4.3.3 Optimization of scaling factor using PSO 90

4.4. Summary 92

5. RESULTS AND DISCUSSIONS 93

5.1 Simulation Setup for Trust Assessment 93

5.1.1. Dataset 94

5.1.2. Trusted network design 95

5.1.3. Evaluation parameters 96

5.1.3.1 Computation of MAE 96

5.1.3.2 Computation of RMSE 97

5.1.3.3 Accuracy 97

5.1.4. Results and discussion 97

5.1.4.1 Evaluating MAE 97

5.1.4.2 Evaluating the RMSE 98

5.1.4.3 Evaluating the accuracy 99

5.1.4.4 Evaluating the trust assessment 99

5.1.5. Statistical analysis 100

5.1.5.1 Statistical analysis for MAE 100

5.1.5.2 Statistical analysis for trust assessment (TA) 101

5.2 An Experiment of Content Protection 102

5.2.1 Experimental setup 102

5.2.2 Performance metrics 103

5.2.3 Experimental results 105

5.2.3.1 Analyzing the optimal scaling factor 105

5.2.3.2 Imperceptibility assessment 107

5.2.3.3 Robustness assessment 109

5.2.4 Comparative Analysis 112

5.3 Summary 113

6. CONCLUSION 115

6.1 Contributions 116

6.2 Future research directions 117

REFERENCES 119

LIST OF FIGURES

Figure 2.1 Trust provisions 15
Figure 2.2 Trust scope 17
Figure 2.3 Trust relationships 17
Figure 2.4 Trust properties 18
Figure 2.5 Building blocks of trust 20
Figure 2.6 Taxonomy of content protection techniques 36
Figure 2.7 Flow of the watermarking method 40
Figure 2.8 Classification of attacks on the watermarked image 41
Figure 2.9 Provisions of digital watermark 44
Figure 2.10 Classification of watermarking schemes 46
Figure 2.11 Classification of watermark embedded domains 49
Figure 2.12 Level-2 decomposition 52
Figure 3.1 Serial topology for trust propagation 67
Figure 3.2 Parallel topologies for trust fusion 68
Figure 3.3 Distinguishing the distortion and original opinion 70
Figure 3.4 Arbitrary networks with non-series-parallel topology 73
Figure 4.1 Red-cyan Anaglyph 3D image construction 80
Figure 4.2 Level-1 decomposition flow of 3D DWT 82
Figure 4.3 Level-2 3D DWT decomposition 82
Figure 4.4 Functional flow of watermark embedding 87
Figure 4.5 Function flow of watermark extraction 87
Figure 4.6 Flow of the optimization of scaling factor 91
Figure 5.1 Sample trusted network 96
Figure 5.2 MAE optimization 98
Figure 5.3RMSE optimization 98
Figure 5.4 The accuracy comparison between I-3VSL_TW with 3VSL_AT 99
Figure 5.5 Trust probabilities of the trustees 100
Figure 5.6 **Cover images:** (a) cones (b) flowerpots (c) dolls (d) classroom (e) backpack (f) Adirondack (g) art **Watermark logo:** (h) Surf Coffee 103

Figure 5.7 **Cover images:** (a) True Anaglyph (b) Red-cyan Anaglyph (c) Mono Anaglyph **watermark logos:** (d) Color Anaglyph (e) Half-color Anaglyph (f) optimized-color Anaglyph 3D images 103

Figure 5. 8 Performance under various attacks with different scaling factors 106

Figure 5. 9 Invisibility with the perspective of MSE, PSNR, SSIM and NCC 107

Figure 5.10 Attacked watermarked Cone red-cyan color Anaglyph images . 109

Figure 5.11 Different attacks for dynamic parameters 111

LIST OF TABLES

Table 2.1 Summary of various trust models 25

Table 2.2 Comparative analysis of reputation-based trust models 30

Table 2.3 Summary of trust literature 33

Table 2.4 Comparison between cryptography, steganography, and watermarking 39

Table 2.5 LSB digital watermarking model for 1-bit 49

Table 2.6 Properties of SVD 53

Table 2.7 Examines the spatial and transform domains 53

Table 2.8 Comparative analysis of recent studies over 3D Anaglyph image and video watermarking schemes 59

Table 4.1 Initial parameter for PSO optimization..91

Table 5.1 Parameter for simulation..94

Table 5.2 Statistical analysis of MAE..101

Table 5.3 Statistical analysis of trust assessment...101

Table 5. 4 Types of attacks with specifications 105

Table 5.5 PSNR values for various red-cyan Anaglyph images with different sizes..108

Table 5.6 Imperceptibility performance based on MSE, PSNR, SSIM and NCC 108

Table 5.7 Recovered watermark logos with NCC values 110

Table 5.8 Comparison of performance metrics between the proposed approach and the Koley approach 112

LIST OF SYMBOLS AND NOTATIONS

Notations	Meaning of the notations
W_{AB}	Player A's opinion on player B
b_{AB}	Player A's trust opinion on player B
d_{AB}	Player A's distrust opinion on player B
n_{AB}	Player A's posterior uncertain opinion on player B
e_{AB}	Player A's prior uncertain opinion on player B
a_{AB}	Base rate
r_{AB}	The communication among players A and B is true positive
s_{AB}	The communication among players A and B is false positive
o_{AB}	Uncertain communication among players A and B
$E(W_{AB})$	Expected trust among players A and B
Δ	Discounting operator
Θ	Combining operator
$G = (V, E)$	Graph with 'n' vertices and edges
$E\ (A, u_i)$	Player A has interactions with u_i players
G'	Sub-graph
Ω_{ij}^{d}	Individual player's trust opinion from i on j at depth 'd'
M_{O}	Opinion matrix
$\mathrm{V}^{\mathrm{d}}{}_{\mathrm{i}}$	Trust vector of player' i' with all other players at depth 'd'
I	Absolute trust (identical)
d	Hop count
D	Maximum depth
$\odot$	intuition of operator
$\cup$	Prior uncertain opinion
$\mathrm{R}_{\mathrm{L}}, \mathrm{G}_{\mathrm{L}}, \mathrm{B}_{\mathrm{L}}$	Left image R, G, B colors
$\mathrm{R}_{\mathrm{R}}, \mathrm{G}_{\mathrm{R}}, \mathrm{B}_{\mathrm{R}}$	Right image R, G, B colors

L	Low Pass filter
H	High Pass filter
$LLL, LHL, LHH,$ $LLH, HLL, HLH,$ $HHL, and\ HHH$	Different frequency sub-bands of 3D DWT
$\mathrm{\phi_{i,p,q,r}(x, y, z)}$	Scaling function
$\mathrm{\psi^{j}_{i,p,q,r}(x, y, z)}$	Translation function
$\mathrm{W_{\phi}(i_0, p, q, r)}$	Discrete wavelet coefficient scaling function
$\mathrm{W^{j}_{\psi}(i_0, p, q, r)}$	Discrete wavelet coefficient translation function
P	Orthogonal matrix
H	Hessenberg matrix
U, V	Left and right orthogonal matrix
S	Diagonal matrix
$\mathrm{u_j, v_j}$	Rotation in "j" direction
$\mathrm{S_j}$	Scaling in the "j" direction
$\mathrm{Pb_i}$	The ith particle best solution
$\mathrm{G_{best}}$	Global best position
$\mathrm{X^{m}_{i}}$	The ith particle position
$\mathrm{V^{m}_{i}}$	The ith particle velocity
$\mathrm{C_I}$	Cover image
$\mathrm{W_I}$	Watermark logo
$\mathrm{M^{RGB}_{I}}$	Watermarked image
$\mathrm{M^{ext}_{I}}$	Extracted watermark logo
$\mathrm{I_w}$	Inertia weight
$\mathrm{c_1, c_2}$	Acceleration parameters
$\mathrm{r_1, r_2}$	Random numbers
R	Level of decomposition
$\mathrm{C_W}$	Watermark embedding
α	Scaling factor
$\mathrm{C_{wat}}$	Inverse SVD
$\mathrm{LLL_{wat}}$	Inverse HD
$\mathrm{S_{bwat}}$	Extraction process

f	Fitness function
n	Number of operations on the watermarked image
m	Population size
μ	Mean
σ^2	Standard deviation
$T_{u,v}$	Actual trust
$E_{u,v}$	Expected trust
p, q, r	Image dimensions

LIST OF ABBREVATIONS

Acronym	Meaning of Abbreviation
2D	2 Dimension
3D	3 Dimension
3VSL	Three-Valued Subjective Logic
ACM	Arnold's Cat Map
ADM	Adaptive Dither Modulation
AOI	Area of Interest
AR	Augmented Reality
AT	Assess Trust
At	Attitude
ATr	Absolute Trust
Be	Behavior
BFS	Breadth-First Search
BI	Belief
BN	Bayesian Network
BP	Belief Propagation
BPN	Back Propagation Network
C	Compose
$\boldsymbol{C_I}$	Cover image
CAD	Computer-Aided Design
CDN	Content Distribution Network
CI	Confidence Interval
CL	Classification
CR	Compression Ratio
CRT	Cathode Ray Tubes
CS	Context-Specific

CTM	Cuboid Trust Model
D	Dynamic
DCT	Discrete Cosine Transformation
DFS	Depth First Search
DFT	Discrete Fourier Transformation
DM-QIM	Dither modulation with QIM
DRM	Digital Right Management
DSPG	Direct Series Parallel Graph
DVE	Distributed Virtual Environment
DWT	Discrete Wavelet Transformation
EETM	Enhanced Eigen Trust Model
ETM	Eigen Trust Model
Ex	Experience
FPP	False Positive Problem
FrFT	Fractional Fourier Transform
FWHT	Fast wavelet Hadamard Transformation
GA	Genetic Algorithm
GOP	Group of Pictures
GPTM	Grid Peer Trust Model
GTM	Gossip Trust Model
HD	Hessenberg Decomposition
HE	Histogram Equalization
HFTM	Hierarchical Fuzzy Trust Model
HMD	Head Mounted Devices
HMM	Hidden Markov Model
HTM	Hybrid Trust Models
HVS	Human Visual System
I	Reference image

I-3VSL	Improved Three Valued Subjective Logic
ICT	Information and communication technologies
I-DWT	Inverse DWT
ITM	Interaction based Trust Models
JPEG	Joint Photographic Expert Group
LM	Linear Model
LPA	Label Propagation Algorithm
LSB	Least Significant Bit
LWT	Lifting Wavelet Transformation
MAC	Medium Access Control
MAE	Mean Absolute Error
MANET	Mobile Ad-hoc Networks
MMOG	Massively Multiplayer Online Games
MSE	Mean Square Error
NCC	Normalized Cross-Correlation
P2P	Peer to Peer
PBTM	Probability-Based Trust Model
PCA	Principal Component Analysis
PDA	Personal Digital Assistant
Prob	Probabilistic
PRTM	PageRank-based Trust Model
PSNG	Pseudo-Random Noise Generator
PSNR	Peak Signal-Noise Ratio
PSO	Particle Swarm Optimization
PT	Peer Trust Model
PTM	Power Trust Model
QF	Quality Factor
QIM	Quantization Index Modulation

QoS	Quality of Service
Re	Recommendation
RMSE	Root Mean Square Error
SL	Subjective Logic
SSIM	Structural Similarity Index Measure
SSM	Spread Spectrum Modulation
SVD	Singular value decomposition
T	Transitive
TA	Trust Assessment
TNA-SL	Trust Network Analysis Subjective Logic
T-SVD	Tensor-SVD
TTM	Topology based Trust Model
TVAA	Trust Vector Aggregation Algorithm
TW	TrustWalker
UTr	Uncertainty Trust
VE	Virtual Environment
VTM	Vector Trust Model

LIST OF PUBLICATIONS

Journal Publications

1. P Srikanth and Adarsh Kumar, "A TRUSTWORTHY PARTNER SELECTION FOR MMOG USING AN IMPROVED THREE VALUED SUBJECTIVE LOGIC UNCERTAINTY TRUST MODEL", *J Arch.Egyptol*, vol. 18, no. 4, pp. 5677-5698, Mar. 2021.
2. P Srikanth and Adarsh Kumar, "COPYRIGHT PROTECTION OF 3D ANAGLYPH COLOR IMAGE WATERMARKING OVER THIN MOBILE DEVICES", *J Arch.Egyptol*, vol. 18, no. 6, pp. 15-36, Apr. 2021.
3. P Srikanth, and Adarsh Kumar et al., "Blockchain and Autonomous Vehicles: Recent Advances and Future Directions", IEEE Access, 9, 1-65, 2021.
4. P Srikanth and Adarsh Kumar, "A TRUSTWORTHY PARTNER SELECTION FOR VIRTUAL ONLINE GAMES BASED ON THREE-VALUED SUBJECTIVE LOGIC", International Journal of Information Systems and Change Management, 2021. (Scopus-Under Review)
5. P Srikanth and Adarsh Kumar, "3D ANAGLYPH IMAGE CONTENT PROTECTION AND INTEGRITY BASED ON BLOCKCHAIN & DIGITAL WATERMARKING", Imaging Science Journal, 2021. (SCOPUS/SCIE-Under Review)

Conference Papers

6. P Srikanth, and Adarsh Kumar, "A Decision-Based Multi-layered Outlier Detection System for Resource Constraint MANET", Advances in Intelligent Systems and Computing, Singapore: Springer Singapore, vol. 1166, pp.595-610,2021.
7. **Patent:** P Srikanth and Adarsh Kumar, "BLOCKCHAIN BASED SYSTEM INFORMATION RECORDER AND METHOD THEREOF." Application Number 202011010492, 2020.

CHAPTER 1
INTRODUCTION

With the advancement in mobile technology, mobile devices are classified as thin and thick devices. The thick mobile devices take the input from the physical world, process it, and produce the output. In contrast, thin mobile devices take the input depending on the users' physical activities portrayed in the virtual environment (VE). Thus, to view the VE information, thin mobile devices are essential, such as Personal Digital Assistant (PDA), Google Glasses, Head Mounted Devices (HMD), iPhone, and many others. As a result, the thin mobile device based applications such as virtual walkthrough [1], [2], Augmented Reality (AR) [3], social networks, Massively Multiplayer Online Games (MMOGs)[4], and a plenty of other applications emerged. Most of these applications are primarily applied to the client-server architecture. The client machine stores the entire VE application, which is not feasible due to the mobile devices' memory constraints. Hence, to address this problem 3D streaming technique is leveraged. The 3D Streaming permits the gradual downloading and 3D rendering to interact with the virtual world without complete downloading or pre-installation [5]. However, the remote visualization of the 3D Streaming with client-server architecture consumes more bandwidth. Nevertheless, this architecture has other problems includes server bottleneck, lack of scalability, latency, single point of failure, and many others. In order to overcome the challenges mentioned above, a peer-to-peer (P2P) network is established.

P2P 3D streaming applications such as MMOG permit millions of people of different ages worldwide to interact with other players in virtual online games. The interactions are either contest, supportive, or merely exchanged at a massive scale for the collective aspect between MMOGs. The MMOGs have various categories depending on the gameplay provision includes first-person shooter, real-time strategy, role-playing game, simulation, social, and others[4]. The MMOG players' acquisitions the game software by rewarding one-time payments and recompenses month-wise subscription charges. However, the most popular MMOG games are World of Warcraft, Sony Ever Quest, Travian, and many browser-based games. Hence, the players can play the game via connecting to the browser without downloading the content.

Although, the players interact with the other players in the network based on the players' Area of Interest (AOI). However, the players' behaviour is abandoned because of the dynamic nature. The adversary partners are selected based on random strategy then share the resources. Thus, it leads to numerous glitches includes request contention[6], cheating in online games [7], content protection [8], uncertainty behaviour of the players [9], and many others. To overwhelm these problems, the trustworthy partner selection strategies and content protection techniques are essentials. Therefore, the researchers have recognized the importance of trust assessment and content protection strategies to enhance performance.

1.1. An Overview: 3D Streaming

Incessant and real-time 3D content delivery permits users to establish VE interactions without full download or prior installation [5]. Although, Streaming is prevalent nowadays as a media, video, and 3D streaming model. These models have diverse representations supporting different design decisions and distinct characteristics. However, the significant difference between 3D Streaming, media, and video streaming approaches relies on the following terms.

- **Object manipulation:** in media and video streaming, the content is available as 2D images, and the object manipulation (i.e., rotation, zoom-in, zoom-out, etc.) requires the additional information in the form of images. In 3D Streaming, content is available in 3D textures, meshes, animations, and scene graphs. The 3D content permits object manipulation without additional information because local processing imposes changes on the available content.

- **Content access pattern:** in media and video streaming, the content is accessible in the sequence of frames, and it permits the user to predict the subsequent frames. In 3D Streaming, the content is accessible in a non-linear fashion according to the user's interest, i.e., viewing angle and distance from the viewing object.
- **Partner selection:** In media and video streaming, the opponent partner (i.e., trustee) is selected through the file-sharing approaches based on the content availability [10]. In 3D Streaming, the partner is determined based on the location, i.e., AOI and resources availability. Therefore, the 3D content is diverse from the media and video streaming.

1.2. P2P 3D Streaming Characteristics

The P2P 3D Streaming has been proposed to overcome the challenge of the remote rendering problem because specific users are participating in the VE and communicating with one other to acquire the content in a fully distributed environment. As a result, it possesses the more essential characteristics described below.

- **Decentralization**: P2P 3D streaming systems are classified as centralized or decentralized based on the resource discovery mechanism. In centralized P2P 3D Streaming, the central server manages the discovery of the resource, and the resource downloading is done in a distributed manner. In this approach, the central server monitors the peers' behavior in the network. In decentralized P2P 3D Streaming, the resource discovery and downloading are completed distributed. The behavior of peers is uncertain because lack of a central server. Moreover, this approach increases the robustness and fault tolerance (i.e., no single point of failure) because of the decentralized nature.
- **Scalability:** It can accommodate many users without compromising the quality of service (QoS) or performance. In P2P 3D Streaming, the scalability categorizes structural, load, space, and space-time scalability [11]. Structural scalability can increase the number of peers in the network

without critical amendments. Load scalability is the ability to deal with resource availability and latency. Space scalability deals with application memory requirements that permit users at certain levels. The space scalability is achieved through various programming techniques such as sparse matrix or compression. Space-time scalability is a continuous function as the number of objects it encompasses increases by order of magnitude. The space-time scalability is achieved through the data structures and algorithms. However, in P2P 3D Streaming, scalability requirements are application-specific.

- **Consistency:** In P2P 3D Streaming, the peers share the resources or experiences based on the ability in the same virtual world state through substantial latency. Although, the level of consistency depends on the application requirements and technical boundaries. The application requirements are determined through strict consistency, eventual consistency, or inconsistency. The strict consistency at every node is provided through the complex algorithms, whereas inconsistency is hard to avoid because of violation and visual divergence. Thus, predictive techniques are employed to optimize the effect of inconsistency, but cheating is another type of inconsistency that occurs due to changing the fairness rules. Therefore, in P2P 3D Streaming, inconsistency is a critical problem.
- **Resource sharing:** In P2P 3D Streaming, each peer collaboratively shares the resources with other peers. However, the free-riders or selfish peers leverage the available resources, but they never contribute. Therefore, to enhance the fairness in P2P 3D Streaming, various strategies are employed, such as auditing, incentives, resource sharing, and micro-payment techniques.
- **Peer cooperation:** In P2P 3D Streaming, the peers search for the resources through broadcasting the messages to neighboring peers, and then neighboring peers forward the message to their neighbors, and so on. The peer responds to the requested peers' notice based on the resource availability. If a neighboring peer is a malicious behavior, thus it does not forward the message and respond to the statement. Thus, it leads to

communication and computational overhead to the requested peer. Therefore, P2P 3D streaming cooperation depends only on the known or self-interested peers.

- **Autonomy:** In P2P 3D Streaming, each peer communicates with other peers based on their interest and shares the resources without imposing any protocol on the peers' behavior. Thus, the participant peers in the network maintain the resources or content by themselves.

1.3. P2P 3D Streaming Applications

The contemporary P2P 3D streaming technologies are prevalent because of the practical construction of 3D physical objects. Thus, it leads to various applications of 3D content includes e-commerce, e-tourism, e-learning, socializing meta-verses, online virtual games, military affairs, chemistry, cultural heritage, and medicine. These applications have a common objective as remote visualization for different aspects. However, most of the applications involve various security challenges such as privacy-preserving and content protection described below.

- **Social networks:** The 3D social networks application such as Second Life [12] are created through the computer-generated artificial world that enables interactions between individuals in the virtual environment. Individual users can generate their content and interact with other users by sharing it in real-time. However, content protection and partner selection are vulnerable security threats in this application.
- **Business and e-commerce:** With the advancement in 3D technologies, the physical world products are moved towards the virtual world to support remote visualization. For example, most business organizations conduct business meetings and conferences with their customers and trade partners using the virtual world. Collaborative projects such as product design use the virtual worlds to interact with employees, clients, and providers through 3D graphical platforms. The virtual clothing and furniture are the best example of a virtual business that generates the revenue for companies and enhance users' satisfaction with 3D visualization. However, virtual accessories are valuable products to

trade; thus, it requires content protection and trustworthy users are essential.

- **Education and training:** The classroom activities are essential among student and teacher interactions in the 3D synthetic environment, especially for distance learnings. For instance, the practical based on the real-world entities visualized in the virtual world by the students in view depend on rotating the objects based on their interest. Thus, these objects can be paid or unpaid. The paid customers can access the entire scene of objects. However, outstanding customers can interact with freely available virtual objects. Therefore, the paid 3D content protection is essential to mitigate the illegal distribution between paid and unpaid customers.
- **Animations and gaming:** An animations and gaming products are leveraged in various applications, especially for health problems. For example, child obesity is a critical problem that leads to numerous life-threatening circumstances, including diabetes, heart disease, high blood pressure, and mental health problems [13]—the mental health problems as loneliness, depression, anxiety, and many more. Thus, to address the child obesity problem, a combination of exercise and 3D virtual games are designed as mobile collaboration exergames. The children's plays collaborate exergames by moving the larger area using thin mobile devices. Thus, physical exercise and collaboration with other children will reduce obesity—however, the virtual exergames suffering from security problems such as partner selection and content protection.

Additional challenges are also considered in addition to security disputes while designing 3D virtual environment applications over thin mobile devices. Hence, integrating mobile ad-hoc networks (MANET) with P2P 3D Streaming imposes the additional challenges described in the subsequent section.

1.4. Challenges and Issues

Mobile devices have various challenges and limitations that affect the wireless network design. However, several challenges need to be considered before streaming the 3D content over thin mobile devices. The most critical challenges are as follows.

- **Thin mobile devices:** These are resource-constrained devices such as restricted storage volume, low processing speed, inadequate battery life, limited graphical accelerators, limited graphics hardware, and many more [14]. Due to these limitations, the complex 3D content rendering over the thin mobile devices is the bottleneck.
- **Wireless network bandwidth:** The mobile devices leverage the wireless medium to share the resources among the nodes. Hence, it produces unpredictable throughput because of the interventions, which leads the communication breaks as a result high rate of packet loss. However, the P2P 3D Streaming over thin mobile device applications suffers from extra bandwidth consumption due to broadcasting the updated messages to all the nodes in the wireless network.
- **Nodes mobility:** In an ad-hoc wireless network, the mobile nodes move freely inside or outside the AOI. Thus, it leads to dynamic changes in the network. This causes frequent changes in the routing path from source to destination.
- **Peer and piece selection:** In an ad-hoc wireless network, the mobile nodes form the communities based on common interests. Thus, it leads to streaming quality optimization based on the available bandwidth. However, the peers requested content is available with many peers because the peers request content within or outside the AOI. Suppose the invited peer selects the partner randomly, leading to the request contention. The acceptable content may maliciously damage the fairness rules. Therefore, peer and piece selection are critical problems.
- **Security:** In an ad-hoc wireless network, security is a massive and critical problem because of the distributed environment. The peers share the content easily among other peers, which are associated with numerous challenges to deliver content securely. Thus, guarantee secure and trustworthy peer interactions and maintain shared content integrity [15].

1.5. Research Motivation

Over the past decades, P2P 3D Streaming over thin mobile device applications such as MMOG has become very popular in the gaming industry. The primary characteristics of these games allow an enormous number of players and engage the interaction over the internet. In MMOG, the players interact with the other players and exchange resources over the internet. The players request the neighboring peers based on similar content available within the AOI. The players having the requested content will respond positively. The invited peer selects the opponent player randomly, which causes various security problems such as uncertainty behavior of the players, cheating in online games. However, while sharing the content, the eavesdroppers may modify or illegally distribute content once they receive the content. Hence, choosing the right partner and providing content integrity are critical challenges in the virtual world. These challenges influence this research to provide a solution by selecting a trustworthy partner and sharing the 3D content in a protected manner. The primary contemplation of this research is emphasized below.

1. The trustworthy partner selection through the uncertainty trust model.
2. An efficient trust assessment algorithm to compute trustees' trustworthiness from the trustors' perspective.
3. 3D content is protected through the digital watermarking algorithm.

1.6. Research Objective

The primary objective of the research work is to formulate the uncertainty trust model operations to assess the trust opinion of unknown players based on the known player recommendations. The players' trust opinions are computed based on normal probability distribution. Hence, all trustees' effective and accurate trustworthiness is assessed from the trustor's perspective. The secondary objective is to design the digital watermarking technique to protect the 3D content integrity of color images and validate the performance under various watermarking attacks. The following objectives are achieved in the course of the proposed research.

The objective of the thesis

- Design & Implement an algorithm to enhance the trustworthiness of partner selection and content protection in P2P 3D Streaming over thin mobile devices.

Sub Objectives:

  - Devise a trustworthy partner selection scheme for P2P 3D Streaming over thin mobile devices.
  - Design an effective trustworthiness computing algorithm to assess the trust of all trustees from the trustors' perspective.
  - Design the 3D content /copyright protection scheme for color images.
  - To verify and validate the proposals using simulation based on the study.

1.7. Thesis Contribution

The present work focused on the "Security enhancement of P2P 3D streaming over thin mobile devices", and its significant contributions are described below.

1. A comprehensive study about the various trust recommendation techniques, trust assessment models in the P2P environment and identifying its limitations.
2. The state-of-the-art of 3D anaglyph content protection techniques and their limitations.
3. The proposed a trustworthy partner selection scheme for MMOG using an improved Three Valued Subjective Logic (I-3VSL) uncertainty model.
   a. Formulate the I-3VSL uncertainty trust model operations: discounting and combing.
   b. An efficient trust assessment algorithm to compute the trustworthiness of all trustees from the trustors' perspective.
4. Design a robust digital watermarking scheme for 3D anaglyph content protection for color images.

1.8. Thesis Navigation

A summary of the thesis structure is described below:

Chapter 2 Literature Review on Trust Assessment and Content Protection: Describes the background details of trust assessment. Emphasizes the various conventional trust models and recommendation approaches associated with the P2P environment. Determines the gaps related to trust models and recommendation approaches. The prevailing gaps provide the prospects for this work. Correspondingly, it describes the digital watermarking techniques. The state-of-the-art 3D anaglyph content protection techniques through digital watermarking strategies identify the gaps associated with these strategies.

Chapter 3 Proposed Framework for Trustworthy partner selection scheme: The improved three-valued subjective logic operations—design of the Trustwalker algorithm to compute the trustworthiness of all trustees from trustors' point of view. The trusted network design, such as non-series parallel network, i.e. arbitrary network design and problems associated with series and parallel network, improved three-valued subjective logic operations.

Chapter 4 Proposed Framework for Robust watermarking scheme: A robust 3D anaglyph content protection technique for color images using Discrete Wavelet Transformation, Hessenberg Decomposition, and Singular Value Decomposition. The watermark embedded strength or scaling factor is optimized through the Particle Swarm Optimization (PSO). The optimized scaling factor determination under a no-attack scenario.

Chapter 5 Results and Discussion: presents the experimental setup to assess the trust—the accuracy and error computation through MAE, RMSE and accuracy. Similarly, the robustness and imperceptibility are computed through MSE, PSNR, SSIM and NCC under various attacks with different watermark logos. Further, it presents the comparative analysis of the proposed schemes over the existing approaches.

Chapter 6 Conclusion: Concludes the thesis summary and presents a future direction of work.

1.9. Summary

This chapter emphasizes the introduction of thin mobile devices and their applications. The significance of 3D Streaming over the media and video streaming and essential characteristics of P2P 3D Streaming. The real-time applications of P2P 3D Streaming and their challenges related to trust and content protection. Further, the security concerns in P2P 3D Streaming over thin mobile devices. Lastly, it presents the research motivation, objective and thesis orientation. Hence, the proposed work enhances the security of trustworthy partner selection and 3D anaglyph content protection for color images.

CHAPTER 2

LITERATURE REVIEW ON TRUST ASSESSMENT AND CONTENT PROTECTION

The relevance of trust management and content protection solutions that have emerged in the P2P environment is discussed in this chapter. The extensive study of the trust assessment and reputation models and the research challenges involved with them are presented. Further, the content protection strategies and the relevance of digital watermarking concerning various attacks are investigated. The Anaglyph 3D images and video content protection are thorough examinations. Later, it discusses the critical challenges of the trust assessment and content protection of Anaglyph 3D images.

2.1. Review on Trust Assessment

The distributed virtual environment (DVE) applications based on mobile devices have emerged faster. Thus, privacy protection of conventional security such as confidentiality, integrity, and content availability is impossible in ad-hoc wireless networks based on the policies. However, the DVE applications work in a collaborative environment. The collaboration depends on the ideology behavior and integrity of the players involved in the network. Therefore, the collaboration scheme is employed through trust and reputation.

2.1.1.Significance of trust models

Trust models are emerging in thin mobile device applications such as MMOG. In MMOG, each player act as a client and service provider. A client player selects the opponent player based on the content availability and location. Suppose the requested content is available with multiple players inside or outside the AOI[6]. Then, choosing the right player is imperative to identify the players' behavior before establishing the communication. The selected player acts as a service provider, and the content is exchanged over the internet. In this case, the requestor and service providers don't have control over each other. The requestor believes the content provider is trustworthy. The service provider believes that the trustworthy requestor accesses the content in a protected manner[16]. Hence, this can be possible through the trust that optimizes the risk, increases productivity, and builds strong relations among the participants. The trust models are also responsible for establishing and managing the trust relationships among the players.

2.1.2.Definition of trust

The term trust signifies the belief or confidence that one person has in another person's events. The trust has been extensively employed in many fields of computer science such as e-commerce, social networks, MMOG, and many others [17]. Several authors define trust in different domains, and the definitions are as follows.

- Diego Gambetta [18], trust is evaluated as "The requestor assigns the subjective probability opinion to the service provider when the service provider performs the assigned work."
- Lucas [19] privileges, "trust permits the requestor to know the challenges of the service provider based on that the requestor decides whether to interact or not."
- Bhattacherjee [20]," trust is leveraged as an effective monitoring tool for any scenario. Trust as an institutional control scheme that prevents the damage, imposes restrictions on adverse selection, optimizes the administrative roles, encourages the interactions and promotes the strong relationships for long-term."
- Blomqvist and Stahle [21] defined it as "the trustors' expectation on the trustees' competency, benevolence or friendliness and identity are proven through the experience." As a result, the trustees' behavior and trust vary depending on the evidence of these components.

- Rousseau[22] stated as "Trust is an important state characterized by the willingness to tolerate the weakness in the compensation of optimistic beliefs about another's intentions and actions."
- According to the oxford glossary[23], "trust is the secure belief in the person's trustworthiness or fact or asset." At the same time, Webster's dictionary outlines trust as confidence dependent on personality, capability, asset, or fact.

Regardless of the numerous definitions of "trust," it can be summarized as a combination of expectation and vulnerability. Correspondingly, some of the essential features from the illustrations were recognized as illustrated in Figure 2.1 and particulars as follows.

- **Interaction:** Trust is defined as the actual or prospective interaction between two parties in the form of trust relationships.
- **Expectation:** Trust implies that one party expects something from the other, or both parties expect something from the other party. As a result, the trustees' desired behavior indicates the subjective probability, which relies on the trustors' willingness. In a trust relationship, the party can serve as trustor and trustee.
- **Uncertainty:** Trust means removing the hesitation while establishing engagement between the trustor and trustee.
- **Vulnerability:** Trust means one party has faith in another party that becomes susceptible to a negative outcome. The ramifications of the negative effect are the risk that the trustor is willing to receipts. As a result, trust includes the decision or action.
- **Context:** Trust between certain parties is never the same since trust is influenced by the environmental factors and applications implicated. As a result, a diverse level of trust emerges between the same parties in different ecological scenarios.

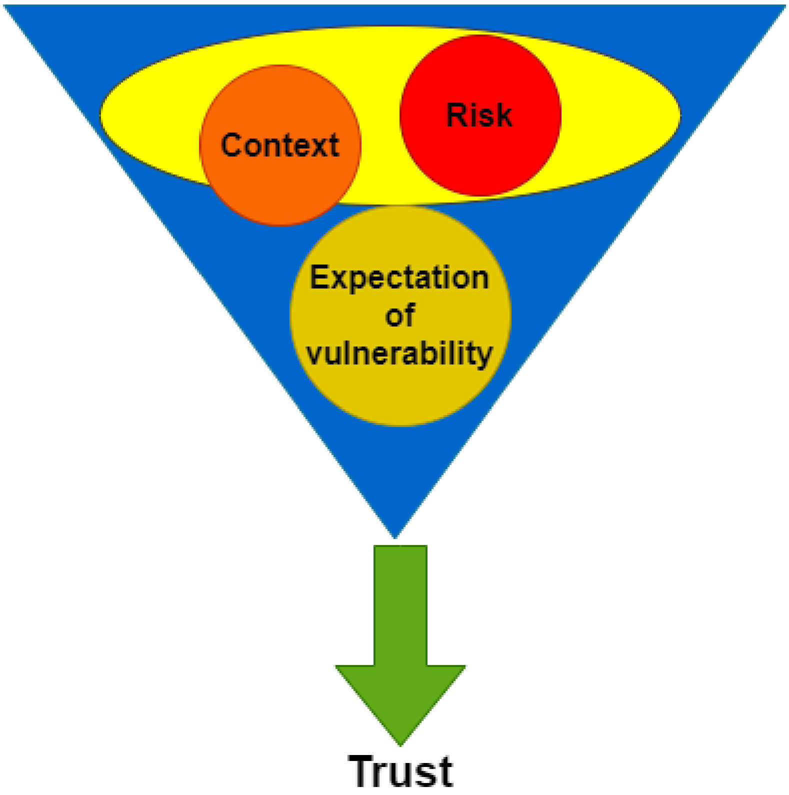


Figure 2.1 Trust provisions

Although trust is ordinarily messy with reputation, these two terms are entirely distinct. Reputation is a belief about an individual or personality. Therefore, reputation is assessed of trustworthiness through the recommendations or feedbacks from the general opinions. The trust is formed based on the own experience. Nonetheless, the own experience is lacking, and then the trust is evaluated through the referrals such as reputations.

2.1.3.Significance of reputation models

Conventional security schemes employ credential-based models to protect against malicious parties in a distributed environment. These models verify the authentication and authorization of the requested users before accessing the requested content, then permit the authorized users to access the content. Conversely, this approach suffers from various problems includes quality of service (QoS), inconsistent and behavior control strategy of the user. As a result, VE applications loose clients. Apart from this, adversarial users explore the network vulnerabilities and capture critical information while interacting. Therefore, trust-based reputation models are essential to address these problems. The reputation model computes the users' reputation based on previous interactions, such as direct or indirect opinions. Thus, the reputation score determines the quality or personality of the user. In other words, reputation is a report of past transactions, while trust is the future expectation or objective. Therefore, the primary purpose of the reputation models is to optimize the malicious activities in the network by extricating the users' behavior as trustworthy and untrustworthy. Moreover, the reputation models form strong trust relationships by computing the unknown users' reputations, which are disseminated geologically.

2.1.4.Definition of reputation

The term "reputation" refers to a broad concept that includes various elements in distributed computing study from many perspectives.

- According to Merriam-Webster [24] glossary and Wikipedia [25], "reputation is the communal opinion of the public that have about a person, i.e., the general people judge a person based on personality or eminence."
- Daniel Threlfall [26] stated that "reputation is the subjective qualitative confidence a person has concerning a product, somebody, firm, trademark or facility."
- Abdul-Rahman and Hailes [27] are said as "reputation is anticipation about someone or entity's behavior based on knowledge or observation correlates to previous behavior.

There are numerous definitions for the term "reputation," [24]–[27] it is summarized as "indirect trust that is assessed based on the public opinion on the person or behavioral information relating to previous interactions."

2.1.5.Trust scope

To measure the trust of one party relies on the other party's decision. Hence trust scope is distinct according to the relying party, as illustrated in Figure 2.2.

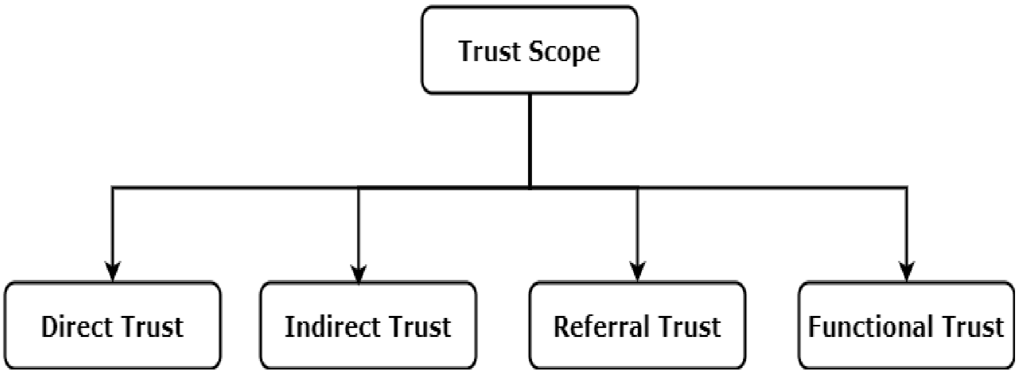


Figure 2.2 Trust scope

- ❖ **Direct trust:** The trust derived from own experience or opinion.
- ❖ **Indirect trust:** The trust derived from other participants' recommendations.
- ❖ **Referral trust:** The trusted party recommend someone that performs the function.
- ❖ **Functional trust:** the selected party trust is derived from the trusted party recommendations or referral trust.

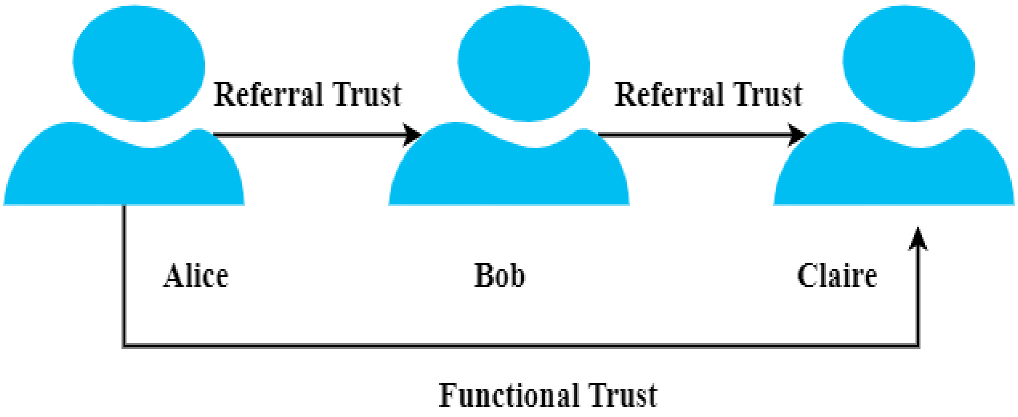


Figure 2.3 Trust relationships

Consider a situation from Figure 2.3, Alice has previous interaction with Bob, then Alice derives trust based on their own experience. Similarly, Bob has their own experience with Claire. This derived trust is known as direct trust, whereas Alice never interacted with Claire, but Bob recommended Claire to Alice. Thus, Alice initiates the relationship with Claire depending on Bob's reference, which is referred to as indirect trust, and here Bob acts as a referral trust. Based on the referral, the trust is derived from Alice to Claire is known as Functional trust.

2.1.6.Trust properties

The trust properties classification is illustrated in Figure 2.4. The trust properties are crucial in determining trust. However, trust qualities might differ depending on subjective or period.

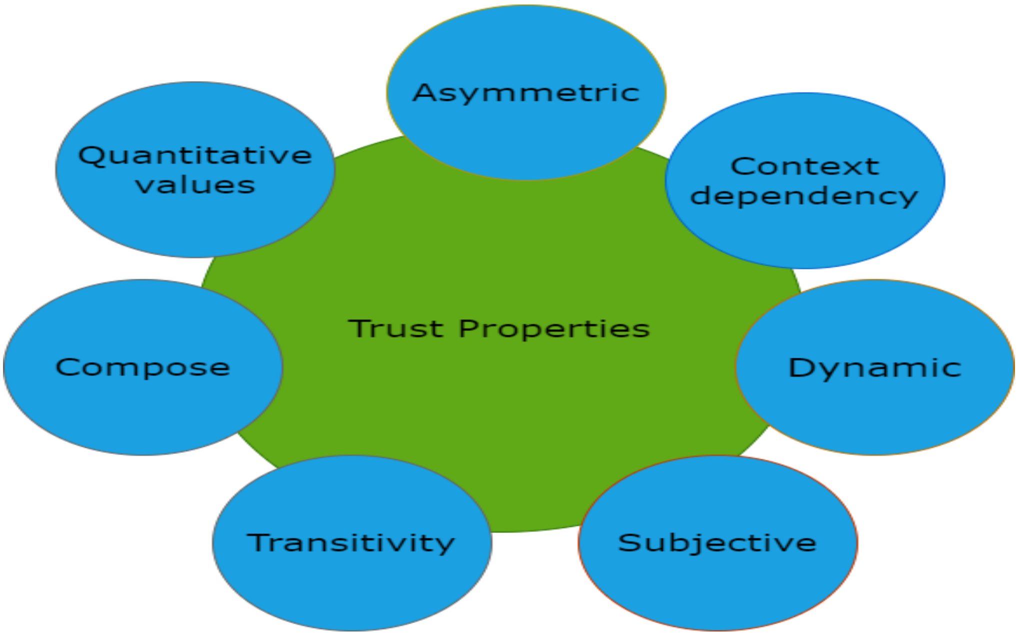


Figure 2.4 Trust properties

- **Asymmetry:** Trust is one-way relation between two or more parties. For example, two parties, A and B, interact with each other. The trust is measured between A to B, denoted by some quantity of belief. Similarly, trust evaluated between B to A is represented in some amount of faith. Therefore, the opinion from A to B and B to A is not symmetrical, i.e., node A believes node B, but the same belief cannot be expected from node B to A; hence trust is asymmetry [28], [29].
- **Context dependency:** The trustor node has different trust opinions for the same trustee in different perspectives such as computational power, data transfer rate, resource quality, and many others. For instance, node A is a patient, node B is a doctor, and node B trusts node B as a doctor's perspective. However, node A never relies upon node B to repair a car from a mechanic perspective. Therefore, trust opinion changes depending on the context [30], [31].

- **Dynamic:** In an ad-hoc wireless network, the nodes move freely based on their interest and establish new interactions. Therefore, the trust opinions vary with new experiences, observations, and interactions[32]. New experiences are essential in assessing trust rather than old experiences. Therefore, a dynamic trust assessment is necessary.
- **Subjective:** Trust is a subjective probability where the trustor is computing the trustees' trust based on the recommendations of the others. The opinions of the recommenders are personal, and it leads to personalized trust computation [33]. However, the topology changes, node behavioral changes, and recommenders' preferences impact the evaluated trust review.
- **Transitivity:** This property plays a vital role in an indirect trust assessment based on the recommendations. For example, if node A trusts node B and node B trusts node C. Node A never interacted with node C then derives the trust from node A to node C through the recommendation of node B. Hence, the trust opinions are transferred from one to another member that forms the trust chains [28], [34], [35].
- **Compose:** This property plays a vital role while a participant forms trust about someone or entity that did not interact earlier. However, when several parties recommend different amounts of faith about a participant, the trustor composes all the trust information. For instance, Claire is recommended to Alice by several participants in the network with different trusts. Alice collects all trust information received from various parties. Then, Alice decides whether Claire is a trust or not.
- **Quantitative values:** Trust can be represented as numeric, discrete, or continuous values. The numeric trust represents the level of trust scale with ratings or labels. The discrete faith is expressed in either binomial or multinomial Bayesian systems. The binomial Bayesian discrete belief is positive or negative, whereas multinomial discrete trust is in trust levels such as excellent, good, moderate, and destructive.

In general, trust can be classified as trust information sources, trust assessment, trust propagation, and their sub-categories are shown in Figure 2.5. The details are available in the subsequent section.

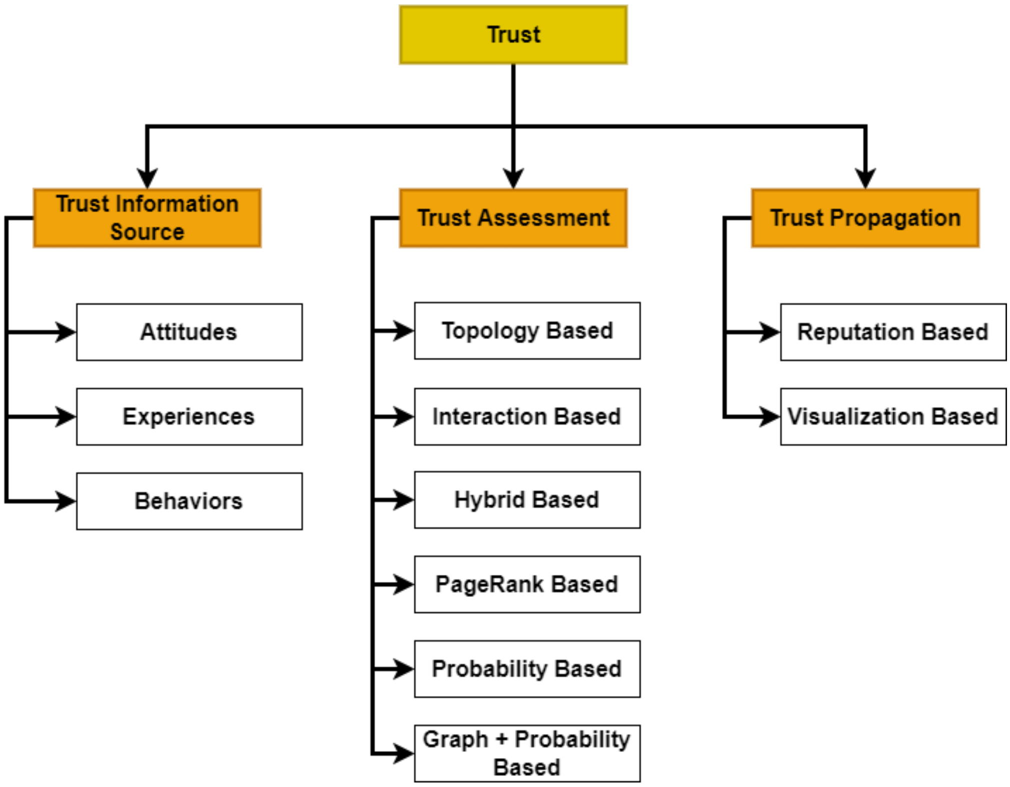


Figure 2.5 Building blocks of trust

2.1.7.Trust information sources

The trust assessed in online games is based on the interaction between the player's such information can be collected using Attitudes, experiences, and behavior are described briefly as follows

- **Attitudes:** It is defined as the participant satisfaction or dissatisfaction with an individual or entity. This information is derived from players' interactions that scale strongly agree-5, agree-4, neutral-3, disagree-2, and strongly disagree-1[36].
- **Experiences:** In the P2P environment, the experience is critical information to compute the trust among the peers' interaction. The backgrounds (i.e., direct belief) are collected based on the interaction ratings between the trustor and the trustee through a feedback mechanism[36]. The experience can be immediate and indirect, which

are affected by attitudes and behaviors[37]. However, most reputation-based models such as peer-trust and power-trust models are employed based on the users' experiences as a source of trust information.

- **Behaviors:** Trust is assessed by analyzing the interaction pattern among the players. For instance, the player is an active member in the online game and unexpectedly drops. Thus, the trust value decreases and reflects on the individual behavior. Therefore, the individual behavior demonstrates the experience among user to user, user to a group (depends on the category of the interaction, frequency, or change of interaction) [37].

2.1.8.Trust models

Trust is fabricated based on the interaction between players, and how to exemplary the trust in DVE has fascinated extra contemplation in contemporary online game studies. Various trust modelling approaches exist that are briefly discussed.

2.1.8.1.Topology based trust model (TTM)

The TTM model fabricates the trusted network based on the participants. The participants are represented as nodes in the graph, and interactions among other participant nodes represent direct edges that form the trust relationship. The advantage of the TTM model is (i). The nodes with higher in-degree have a higher level of trust, (ii). The node establishes the interaction with a higher out-degree node; thus, the trust level increases, and (iii). TTM model controls the random walk trust assessment.

Although, the TTM model analyzes the network topology to identify trustworthy nodes by distinguishing between unreliable and trustworthy network regions[38]–[41]. Further, leveraging the depth-first search (DFS) strategy, a trustor determines the trustee's trust based on reachability probability. A low probability signifies that the trustee is the untrustworthy region and vice versa. Later on, the trust inference is leveraged to assess the indirect trust using the trust values between the participants. The trust relations among two participants are represented as a probability value. The widespread TTM indirect trust inference model is Tidal trust, which derives belief from trustor to trustee by considering the neighbors' higher rating [42]. Thus, compute the threshold trust value for the trusted network then selects the neighbours with an edge value $\geq$ to the threshold. However, the indirect trust inference is a critical problem in the TTM model as network reachability [43]. TTM model examines the trust in the same group or society and depicts it as an absolute trust. As a result TTM model excludes the uncertainty trust.

2.1.8.2.Interaction based trust model (ITM)

This model employs the user interactions that establish the network to compute the trust. The trust is evaluated through the participants' interaction patterns, identifying patterns based on user activities and interaction between two parties[44]. The user activities are observed in terms of shared information measurement such as number of rates, number of reviews, length of the comments, and many others. The interaction relations between the parties include novelist to the rater, novelist to novelist, and rater to the rater. Further, this model also consists of the time difference between users' responses while establishing a relationship as a "temporal aspect." The machine learning techniques are leveraged to predict trust through information obtained from the interaction between users. Then, the information factor originates from training the classifiers that predict the users' trust.

A social network is established based on user interactions to assess social trust[45]. This model consists of two types of trust: reputation and involvement trust. Reputation trust refers to accepting a community member and certifying a member's trustworthiness from other members' perspectives in the network. The involvement trust relates to participation in the community and representing their trust towards the community. The reputation trust is measured by how many members read, follow, and positive feedback on comments. The involvement trust is measured by how frequently users visited the site, how many members followed, and how many posts read and commented. The social trust of the community is determined by merging the reputation and involvement trust. Although social trust is computed based on the interaction-based model, it ignores the social network's topology. The social network structure provides critical information about the member's relationship with others in the network.

2.1.8.3.Hybrid trust model (HTM)

This model is designed using interaction and topology-based trust models to assess social trust, which is referred to as an "opportunistic network" [46]. This network permits the users to participate in numerous interactions and share the resources. This model uses the two approaches to assess social trust, such as implicit and explicit social trust. An explicit trust is fabricated through conscious social relations between two users, exchanging their friends' list and storing it as a friendship graph. The friendship graph consists of the list of friends and their respective trust values that establish the direct trust relations. Implicit trust is fabricated based on the duration and frequency of interaction between two users based on the familiarity and similarity of the users. Familiarity represents the duration of the interaction among the two users, and similarity denotes the degree of coincidence between two users. Although, explicit trust is based on topology, and implicit trust is based on the interactions in the network. This approach considers only the duration and frequency of interactions. However, the nature of the interaction between two users is critical in the social trust assessment. For instance, two parties interact pretty often, but they are debating, then the trust between these two users is high, but it is not possible in real-time.

2.1.8.4.PageRank-based trust model (PRTM)

The PRTM model determines the trustee's trustworthiness according to the trustor's interests. The PRTM leverages the PageRank algorithm to classify the users by referring to prior transactions. On the other hand, it leverages the standard graph search techniques to find the trustor's path to a trustee. The trust value determines the trustee's trust value along that path at each edge. The PRTM technique adaptions are Eigen Trust [47] TrustRank[48].

For instance, the Eigen Trust approach proposed for P2P environment searches trustworthy peers based on the policies. The trustworthy peers are selected based on the higher trust score and higher moving probability among the other peers. After that, the TrustRank algorithm is proposed to detect spam web pages.

This algorithm leverages the page rank algorithm to rank the trustworthiness of the web pages. However, these algorithms are leveraged to trust rankings, not for the absolute trust values of the peers or pages.

2.1.8.5.Probability-based trust model (PBTM)

The PBTM indulgences the direct trust as probability distributions, in which the trustor determines the trustee's trust derived from the prior transactions and circumstances that defines future behavior probability[49]. PBTM analyses the trust more accurately by employing the probability and statistics such as Maximum Likelihood Estimation, Hidden Markov Chain [50], [51], and many others. For instance, direct trust is assessed through the discrete multinomial distribution then trust is measured using likelihood estimation through distribution attributes depending on the evidence. Similarly, the discrete binomial distribution is employed to assess whether the user's trust is trustworthy or not, and then likelihood is accomplished through Beta distribution [52]. If the trust model is a continuous random variable, then Gaussian distribution is used for non-discrete where the results are constant[53].

Further binominal distribution is extended to multinomial distribution to handle the multiple random discrete variables. Hence, the trust assessment of multinomial distribution is accomplished through the Hidden Markov Model (HMM) and Bayesian analysis [54]. The evidence includes reputation score and similar preferences consequently assess the dynamic trust.

2.1.8.6.Subjective logic-based trust model (SL)

Josang proposes the SL model by employing probability-based models and graph theory [55]. The SL model assesses the direct trust by using the Beta distribution based on the evidence in positive and negative. The benefit of the SL model is that it judges the users' trust by considering the uncertainty. The uncertainty exists in the trust assessment because it is difficult to measure with absolute certainty, i.e., whether a user is trustworthy or not[56]. Further, the trust assessment accuracy is enhanced by replacing summation and average operations with discounting and consensus operations. The discounting function derives the new trust relationship from the existing trust relations [57]. The consensus operation combines the different trust opinions from trustor to trustee that derives the new trust opinion [58]. Therefore, indirect trust is measured between the two connected players [59], [60]. SL model preserves the uncertainty evidence as a constant throughout trust assessment. Thus, it produces inaccurate results for complex networks such as bridges or arbitrary networks.

2.1.8.7.Three-valued subjective logic (3VSL)

The 3VSL model is an enhanced version of the SL trust model. The 3VSL model further classifies the uncertainty evidence into prior and posterior evidence. This model assesses the trust more accurately for complex networks based on the trustors' perspective. 3VSL model also uses discounting and combining operations to evaluate the indirect trust assessment[61]–[64]. However, this model requires improvement in discounting function because it ignores the trustors' distrust evidence. Hence, the distrust and posterior evidence changes are not influences in the trust opinions between two players. Table 2.1 presents the synopsis view of the above-stated trust assessment models.

Table 2.1 Summary of various trust models

T_m	T_c	T_u	D_t	I_t	Findings
TTM	√	×	√	√	Network reachability problem while assessing the unknown players' trust. Assess the trust within the community
ITM	√	×	√	–	This model ignores the social network's topology while assessing the trust
HTM	√	×	√	–	This model ignores the nature of the interaction between two users, which is essential in trust assessment.
PRTM	√	×	×	×	The ratings are assigned based on previous transactions. Trust propagation produces inaccurate results.

PBTM	√	×	√	×	Only focus on the direct trust assessment of the known users.
SL	×	√	√	√	Preserves the uncertainty evidence as a constant throughout trust assessment and produces inaccurate results for complex networks such as a bridge or arbitrary networks.
3VSL	×	√	√	√	An improvement is required in discounting operations because it ignores the trustors' distrust evidence. Hence, the distrust and posterior evidence changes are not influences in the trust opinions.

T_m : Trust models, T_c: Certainty trust, T_u: Uncertainty trust,D_t: Direct trust assessment,I_t: Indirect trust assessment

According to Table 2.1, the existing trust assessment models represent the trust as absolute, and their assessment is accurate for only direct trust assessment. However, the indirect trust assessment results are inaccurate. At the same time, SL and 3VSL accurately evaluate the direct and indirect trust and represent the trust as an uncertain trust. Nevertheless, the SL trust model estimates the trust accurately for simple networks but not for complex networks. Similarly, the 3VSL trust evaluates trust accurately for complex networks; still, this model requires enhancement in their indirect assessment.

2.1.9.Trust propagation models

In a P2P environment, various techniques propagate trust information. The popular propagation approaches are recommendation or reputation and visualization models.

2.1.9.1.Trust reputation models

The primary objective of the trust reputation model is to produce personalized recommendations through aggregating the trust opinions from other members in the trusted network. This study explores the most widely used reputation and recommendation schemes in the P2P environment. Adopting is the accounts of such reputation and recommendation systems.

Eigen trust model (ETM): ETM determines the global trust by leveraging the eigenvector matrix, which comprises the local reputational values. The local reputations are determined through the satisfaction or dissatisfaction of other peers' judgements, which is standardized to [1, 0][47]. This strategy reduces the amount of un-authentic file downloads that the malicious peers transmit. ETM can identify harmful peers from the trusted peers' group (i.e. pre-trusted network) and leverages optimal bandwidth. The ETM model is experiencing the following problems, which are described below:

- The reputation is derived by the pre-trusted peers merely by examining the surrounding nodes. As a result, several peers earned poor evaluations despite being truthful and jeopardized their performance.
- The pre–trusted network member acquires un-authentic content from a deceptive peer, and the file is thought to be authentic by other participants. Therefore, several peers can access and shares the forged file.
- The peers can simply report a lack of credibility and diversity in a stable pre-trained community.

Enhanced eigen trust model (EETM): "Honest Peer," peers with the highest reputational values play an additional role in assessing other peers' global reputation values. The honest peers are selected automatically in terms of credibility and quality [65], [66]. In some situations, the legitimate peer sends an un-authentic file, and then other peers can easily download that file. The reputation value of the selected honest peer will be deceased; thus, select the next trustworthy peer.

Peer trust model (PT): The PT reputation scheme analyses and maintains the peer's trust value in a distributed context by leveraging the earlier contacts. The peers' trust is determined by considering a variety of characteristics such as the number of peers contacts, peers feedback, feedback sources repute and transaction dependability, and the relevance of the community [67]. The peers' trust is determined by aggregating trust indices and all aspects of trust. Therefore, it mitigates attacks, including man-in-the-middle, tampering with the nodes, and distributing suspicious messages. However, PT has the following pitfalls.

- The trustworthiness of peers is evaluated leveraging a variety of criteria. As a result, the minimum number of interactions is necessary to determine recently joined peers' legitimacy.
- The highest peer trust value always provides reliable feedback; however, this is unattainable.
- Since peers' performance evolves over time; thus, they emphasize the more contemporary peer reputation value instead of prior accomplishments while assessing the trustworthiness.

Grid peer trust model (GPTM): This is an enhanced version of the PT model. GPTM includes satisfaction criteria, decay function, and parameters used in the peer trust model. These additional parameters are used for initial trust ratings, which also satisfy the satisfaction criteria. Here, satisfaction criteria vary from application to application. Additionally, a decay function is also used. The purpose of the decay function is to update the number of interactions, feedbacks, and transaction context factors for feedback of each transaction. These decay function updates are essential because they consider all the previous transaction records. The transaction records are collected from communities developed in peer-to-peer communications. Further, all of these communities deal with a specific set of problems, vulnerabilities and summarize all of these factors in evaluating peers' trustworthiness [68]. In various observations [68], it has been observed that this model helps overcome the various security threats, remove bogus peers, identify hidden hostile communities, and push down the integrity of trusted peers.

Cuboid trust Model (CTM): CTM uses relationships between three factors (trustworthiness, nodes participation, and Quality of Services (QoS)) for trust computation. The local and global trust values are helpful for the final trust calculation. The global trust value of each interaction is measured with the power iterations. Power iteration is calculated from trustworthiness value, current node participation, and QoS. CTM model is popularly known for reducing un-authentic downloads even though the network includes malicious peers [69].

Power trust model (PTM): This trust model evaluates each participating node's trustworthiness based on power-law feedback property. Here, nodes having high power feedback are considered power nodes. PTM uses a distributed ranking algorithm in selecting the power nodes at random. PTM is well known for increasing performance and accumulating global trust reputation speed [70]. In experimentation, if the power chosen node is a malicious pre-trusted peer, the system is considered highly susceptible to damage. On the other hand, most peers' preferred nodes are deployed to communicate with power nodes, which may cause the collusion problem[70].

Gossip trust model (GTM): GTM is designed for an unstructured P2P network. GTM uses a gossip-based protocol to accumulate global trust reputations accurately and rapidly. In GTM, peer-to-peer communication occurs for trust score propagation and reaching a global consensus on peer reputation [71]. Peer-to-peer communications add overheads because of the aggregation of local reputation values from different neighbours. However, the absence of an error recovery mechanism makes GTM lighter compared to deterministic protocols.

Belief propagation (BP/P2P): In BP/P2P, the peer interacts with other peers in the malicious peers' presence. After successful interaction, the peers provide the Quality of Service (QoS) rating. This QoS rating helps assess peers' trustworthiness and filters the malicious peers from the decentralized network[72], [73]. Further, this strategy helps reduce the errors in the peers' reputation calculations. However, this model suffers from the communication overhead like GTM.

Vector trust model (VTM): In a P2P network, the peers interact with other peers and store their feedback in the local trust table, also known as the vector trust table. In VTM, Trust Vector Aggregation Algorithm (TVAA) is applicable if no historical interaction between pairs is available [74]. In TVAA, multiple trust propagation paths are possible, and each trust path aggregates the trust propagation of the selected peers. Finally, aggregated trust is updated in the vector trust table. In VTM, the global reputation value is calculated dynamically rather than stored in a vector trust table. This approach increases the complexity of the model.

Hierarchical fuzzy trust model (HFTM): This model evaluates the trustworthiness of peer-based on the history of local trust, local trust index, and global trust value through cumulative local transaction information [75]. Hence, this model enhances the accuracy and minimizes inauthentic downloads. HFTM aggregates the local transaction information collected from all peers to produce each peer's global reputation. However, this model suffers from computation and communication overhead.

Trust network analysis subjective logic (TNA-SL): This model uses the trust opinions in trust, distrust, neutral, and base rate. The final quantified trust value is measured from the trust propagation and trust fusion mechanisms[35], [49], [52], [76]. However, this model forms the trusted network based on Direct Series Parallel Graph (DSPG) and expresses it in the canonical form, resulting in information loss[55], [77], [78]. Table 2.2 summarizes the performance of the existing reputation models on various parameters.

Table 2.2 Comparative analysis of reputation-based trust models

Reputation-Based Trust Models	**A**	**B**	**C**	**D**	**E**	**F**
Kamvar et al.[47]	M	M	H	M	H	L
Xiong et al. [67]	-	H	H	M	M	L
Zhou et al. [70]	M	M	M	H	M	L
Gupta et al.[71]	H	M	L	H	L	H
Gaeta et al.[72]	H	M	M	H	-	H
Zhao et al.[74]	H	M	L	H	-	H
Lin et al.[75]	L	M	L	H	-	H
Jøsang et al.[77]	H	L	L	H	-	H

H: high, M: moderate, L: low, A: Convergence speed, B: Message Overhead, C: Computational Overhead, D: Malicious peer detection, E: Inauthentic downloads, F: Scalability.

According to Table 2.2, the above-listed reputation-based trust models provides high computational and communication overhead, low inauthentic downloads, high scalability and detection rate of malicious peers is high. Although in P2P file-sharing systems, the peers employ the trust ratings to select the trustee peer from a group of peers based on the higher trust value. Therefore, the trustor peer moves towards the trustee peer based on the high probability and higher trust value. With this principle, the Eigen Trust [47] and Trust Rank [48] algorithms are employed to assign the trust scores to peers in the network based on the earlier transactions. However, Mole trust [79] and Tidal trust [42] searches for the high probability node in the network. The mole trust model travels through the network commencing the incoming edges that have a larger than a predefined threshold. The trust aggregation is also dependent on edges trust values or weights. Thus, the trust values or weights are considered by selecting the best possible path and its corresponding trust value from source to destination[79].

The Tidal Trust model applies Breadth-First Search (BFS) to find the shortest and reliable route in trust aggregation. Thus, the trust aggregation procedure searches the path from source to destination and covers every possible intermediate node. The current or recently available trust values are only considered in this search. However, there is always a chance to change trust value very frequently, which may cause the losing rates problem in the network[42].

The searching process also considers the user's interest in the selected node for trust aggregation and communication. All calculations in trust estimation, collection, and propagation are based on direct trust calculation rather than any form of indirect trust calculation. Cardoso et al.[59], [60] designed a user trust model for online games using BFS-DFS (Depth First Search) that integrated search traverses the trustor's path to a trustee with more reliable and high trust score values. In this process, the trustworthiness of all trustees is evaluated accurately by considering all possible directions. However, this approach works well for simple networks but not for complex networks because it consists of more loops; hence, the results are inaccurate. The Assess Trust [61] model also uses BFS and accurately assesses the trust between any two users in the network. However, this approach is more computational intensive because of the search's depth, i.e., the hop's maximum number.

2.1.9.2.Visualization models

The propagation of trust information is visualized through the graph representation that consists of the connection among the trusted pair of nodes. A node with a higher in-degree means that a closer trust relationship. The trusted network visualization is represented with various tools such as social network visualization [80], network visualization [81], graph visualization[82], NetworkX [83], and many others. The visualization approaches are employed to examine and determine the trust in the community that identifies the trustworthy peers. Further, the trust visualization controls the peers' behavior by taking preventive actions includes the new exciting or relevant information, by evaluating the trust values to a predefined threshold. The trust value above the threshold then inspires the affirmative behavior otherwise adverse behavior.

2.1.10. Analysis

Table 2.3 depicts the comparative study of the trust literature based on the trust-building blocks. Computer science assesses the trust values and compares the peers' absolute trust with the threshold or higher trust value that establishes the trust relations with other peers. Thus, some of the findings are described below based on the literature.

i. Context-specific trust is essential while performing the trust propagation (transforming the faith from one to another), but more miniature trust models are considered. For instance, mobile manufacture releases new models in the market, and the trust of these models depends on past models. In this context, the trust is transformed from one Scope to another. Likewise, a patient trusts the doctor, and the doctor as a mechanic is distrustful. In this case, trust cannot be transferable. Hence, the research requires identifying when to transform the belief and when it cannot.

ii. Most trust models emphasize the topology-based models and represent the trust as a single quantity, i.e., absolute trust. However, it is challenging to determine if a peer is entirely reliable or not in instantaneously. Hence, the research needs to focus on the uncertainty trust models.

iii. The source of trust information collection is focused on the literature's experiences or behavior. However, attitudes play a vital role in analyzing the user's behavior with other members' in-network while establishing interactions within the community.

Table 2.3 Summary of trust literature

Method	**Trust type**	**Trust model**	**Trust Property**	**Trust computation**	**Trust information**	**Trust Propagation**
ETM [47]	ATr	TTM, PRTM	S,T	LM	Ex	Re
EETM [65]	ATr	TTM	S,T	LM	Ex	Re
PT[67]	ATr	TTM	CS,D,S,T	LM	Ex	Re
GPTM [68]	ATr	TTM	CS,D,S,T	LM	Ex, At	Re
CTM [69]	ATr	TTM	D,S	LM	Ex, At	Re
PTM [70]	ATr	PBTM	S,T,D	BN	Ex	-
GTM [71]	ATr	TTM	D,S,T	LM	Ex	-
BP/P2P [72]	ATr	TTM	D,S,T	Prob	Ex	Re
VTM [74]	ATr	TTM	S,T	LM	Ex	-
HFTM [75]	ATr	TTM	D,S,T	Prob	Ex	Re
Tidal trust [42]	ATr	TTM	C, S,T	Prob	Ex	Re
Mole trust [79]	ATr	TTM	C, S,T	Prob	Ex	Re
TrustRank [48]	ATr	PRTM	S,T	LM	Ex	Re

Interaction trust [44]	ATr	ITM	D	CL	Be	-
STrust[45]	ATr	ITM	CS,D,S	LM	Be	-
Hybrid trust [46]	ATr	HTM	S, T	LM	Be, Ex	-
Probabilistic trust [49]	ATr	PBTM	CS,S	HMM	Ex	-
HMM trust [50]	ATr	PBTM	D,S	HMM	Ex	-
HMM trust [51]	ATr	PBTM	CS,D,S	HMM	Be, Ex	-
Probabilistic trust [56]	ATr	PBTM	D,S,T	Prob	Ex	Re
TNA-SL [77]	UTr	SL	C,D,S,T	Prob	BI	Re
SL trust [59], [60]	UTr	SL	C,D,S,T	Prob	BI	Re
3VSL trust [61]	UTr	3VSL	C,D,S,T	Prob	BI	Re
3VSL trust [63]	UTr	3VSL	C,D,S,T	Prob	BI	Re

ATr: Absolute Trust, UTr: Uncertainty Trust, CS: Context-Specific, C: Compose, D: Dynamic, S: Subjective, T: Transitive, LM: Linear Model, Prob: Probabilistic, BN: Bayesian Network, CL: Classification HMM: Hidden Markov Model, Be: Behavior, Ex: Experience, BI: Belief, At: Attitude, Re: Recommendation.

2.1.11. Critical analysis

The significant challenges in trust and reputation models have been identified in a comparative analysis of various models [42], [47], [48], [59]–[61], [67], [70], [77], [79]:

(i) The communication and computation overheads are associated with reputation and trust management.

(ii) The inability to deal with uncertainty in trust evaluation strategy.

(iii) The statistically intensive examination of uncertainty models in real-world applications.

(iv) The dynamic trust evaluation platforms include the trust characteristics alterations in trust models to determine the most appropriate circumstance.

(v) Direct interaction and trust opinions uncontrolled variations for the target network.

(vi) Unpredictable change in belief opinions with either variation in player's trust or source of trust propagation.

(vii) Trust misses management because of un-authentic trust score or players' distrust approaches.

(viii) Lack of trustworthiness among trustee nodes when trust probabilities vary in both predictable and unpredictable fashion.

(ix) Error rate variations in searching the trustee nodes and trusted paths.

(x) Variants in computation time are inevitable while performing an in-depth search employing trustworthiness or peers interaction criteria.

2.2. Review on Content Protection

The richness of digital and information technologies in the modern world has opened innovative prospects for producing and supplying unconstrained 3D content leveraged in movies, gaming, virtual reality, computer-aided design (CAD), healthcare, medicine, military, bioinformatics, and many others. However, the internet has emerged with the digital revolution as a proficient content distribution that includes enormous data transmission, collaborative applications, web cache updating, continuous digital media streaming, and immersive or multiplayer gaming. Therefore, the content owners employ the service architecture to deliver their digital media effectively to requestors. The conventional service delivery model, such as client-server architecture, depend on a centralized server to deliver the media to a group of customer or customer. However, this distribution approach suffers from various problems includes server bottleneck, congestion, and single point of failure. Therefore, to enhance the service quality and productivity by using the Content Distribution Network (CDN) [84]. The CDN is a dedicated server widespread across the internet and delivers content to users. However, the content providers need to sustain infrastructure expenditures, high server maintenance costs, and limited scalability that impact network performance. Therefore, P2P networks are essential.

P2P networks deliver the content effectively to numerous users over the internet. The P2P technology provides various benefits such as low-cost infrastructure, fault tolerance, scalability are fascinating to the content providers towards the amendment of the P2P models. Further, the content distribution cost is much lower for content providers. As a result, the buyers' prices are also lower; thus, it increases the revenue of the content owners or industry. Despite its benefits, the major hindrance is an illegal distribution of content that produces financial loss to the organizations or content providers. Hence, the content protection techniques are essential [85]–[87].

2.2.1.Content protection

The content protection includes several characteristics such as confidentiality, authentication, authorization, and copyright protection through encryption, digital rights management, digital fingerprinting, and digital watermarking, as shown in Figure 2.6.

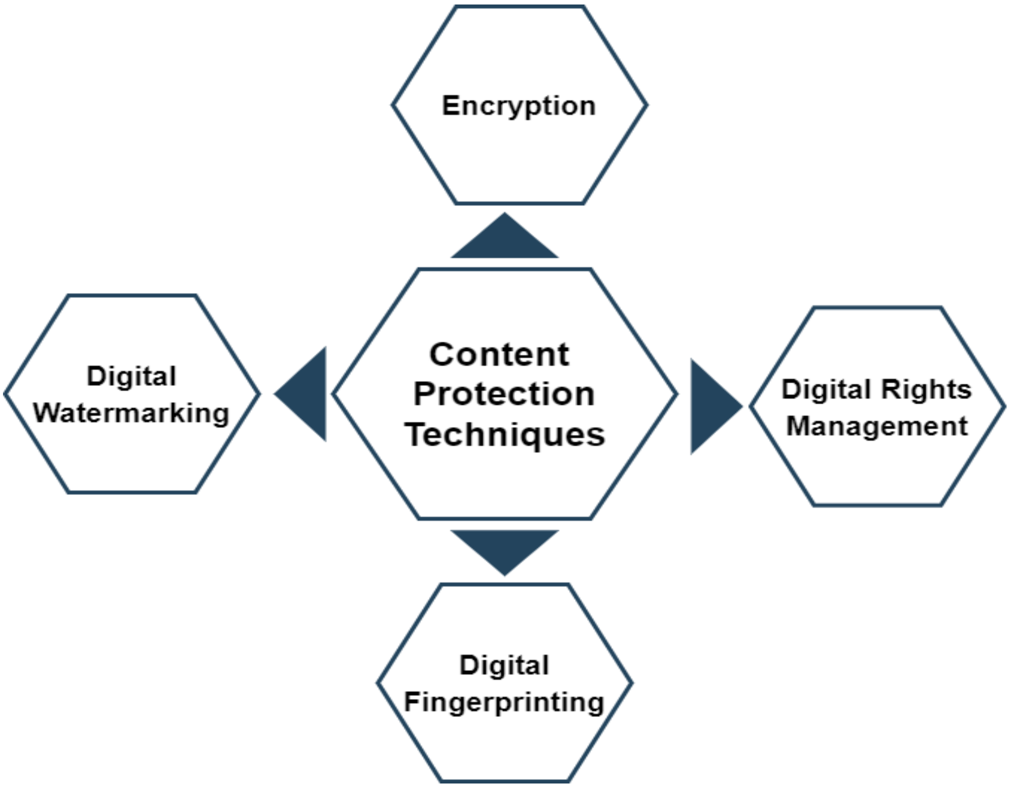


Figure 2.6 Taxonomy of content protection techniques

2.2.1.1.Encryption

This approach offers secure content delivery to authorized users, and the authorized users access the content through decryption. This approach provides content protection in terms of confidentiality, authentication, and authorization [88]. The conventional encryption techniques provide content protection for images [89], audio [90] and video[91]. However, the encryption techniques are computationally high and provide the security while transferring the data from the sender to the receiver. Once the receiver obtains the content, the content owner has no control over the data, and the receiver can illegally distribute the content to others [16]. Therefore, encryption techniques alone do not prevent the illegal distribution of content [92].

2.2.1.2.Digital right management (DRM)

DRM strategy ensures the dissemination of content and the owner's rights against suspicious users. DRM permits the content owners to define their business model for content control, including time-driven access, membership, multiple downloads of a single video, and restrictions on content transfer to mobile devices. A DRM system operates on three stages: it establishes the ownership rights for content, supervises content distribution, and restricts re-distribution after delivery [93], [94]. To accurately manage these stages, a DRM system must adequately describe and explain three separate entities: the user, the digital media, and the usage rights associated with it, as well as their interactions [95], [96]. DRM uses the recipe of encryption and watermarking techniques that provides privacy. Encryption techniques are leveraged to control user access through a password mechanism, whereas authentication and integrity are provided through watermarking and digital signatures. Conversely, DRM techniques suffer from various challenges that are described below.

1. DRM solutions are unreliable and incompatible with others. Typically the content provider develops its own content protection rules, which results in incompatibility with DRM systems. As a result, the users constantly search for digital content acquired via their preferred device. Therefore, the customers are unwilling to use DRM solutions owing to the lack of interoperability.

2. DRM technology protects content by generating and enforcing rights, identifying users, and monitoring content usage. However, the DRM system creates a critical security problem in terms of the content owners and users' privacy [97]. Therefore, privacy-preserving and interoperable DRM systems are crucial because they ensure that any application or device can access its content without compromising the users' privacy.

2.2.1.3.Digital fingerprinting

Digital fingerprinting strategy enables digital content owners or publishers to exert greater control over the dissemination. In this method, the secret information associated with a user-specific identification is placed in the content to trace down an infringing re-distributor [98], [99]. Thus, the illegal copy is identified by extracting the fingerprint associated with the original recipient. This approach consists of three stages: generating a fingerprint, embedding the fingerprint in content, and tracing the illicit dissemination. Conversely, this technique has several drawbacks, including high computation complexity for inserting user-specific information and insignificant robustness against signal processing attacks, high communication cost, and low collusion resistance[100].

2.2.1.4. Digital watermarking

The expansion of digital content demands an effective method to protect it via watermarking. Watermarking is the process of hiding a message, image, document, video, logo, or other pieces of information within digital media [101], [102]. This method is divided into two stages: embedded operation, which incorporates the users' copyright information, and extraction operation, which identifies the owners and verifies its integrity. However, determining the security of watermarks is application-specific parameters such as invisibility and robustness. The tradeoffs between invisibility and robustness are a critical challenge in the watermark. However, the watermarking techniques are different from steganography and cryptography [103], [104]. The significant differences among these schemes are revealed in Table 2.4.

Table 2.4 Comparison between cryptography, steganography, and watermarking [88], [103], [104]

Characteristics	Cryptography	Steganography	Watermarking
Transmission, hiding data	The ciphertext is created by encrypting the data included in an image or text file.	The stego-file is produced by hiding the contents into digital data using an optional key.	Watermark images are produced by inserting a logo onto digital content.
Cover selections	Not applicable	No restriction	Restriction
Objective	Robustness for content protection.	Capacity for secret communication.	Robustness for copyright protection.
Detection and extraction process	No protection is required to extract data.	No protection is required for completely replicating content.	Cross-correlation is essential for content copying, and the cover image is exploited in the extraction process.
media and visibility coverage	Encryption makes hidden data visible. Although, it's not simple to interpret data.	Information is not often correlated with cover and is invisible to the human vision.	Watermarks are occasionally visible to the human vision and constitute cover image features.

According to Table 2.4, cryptography and watermark techniques are essential for content protection. However, cryptography provides protection during the transmission, whereas watermark enables copyright protection. As a result, the watermarking scheme is leveraged to protect the content in this work.

2.2.2.Significance of digital watermarking

As digital content is exchanged or preserved over the internet services, the protection strategies are essential to ensure that it is secured against illegal access, intellectual property theft, ownership, and copyright infringement. As a result, to effectively address the concerns mentioned above through digital watermarking strategies [105], [106], as demonstrated in Figure 2.7.

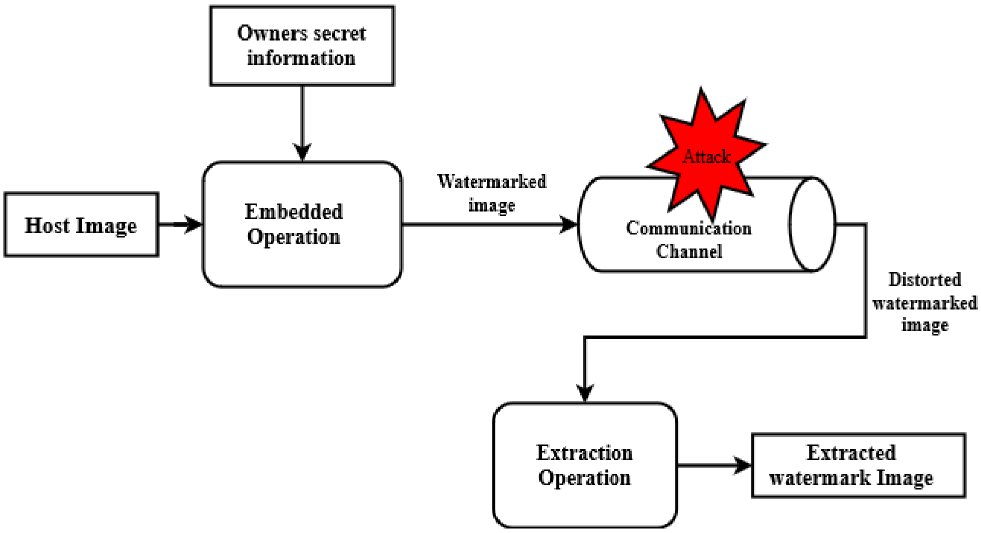


Figure 2.7 Flow of the watermarking method

This approach incorporates secret information or image into an original image without affecting the original image quality. However, the phenomenal expansion of 3D digital applications has increased public awareness of the copyright protection, authentication, and proprietorship of media exchanged across open networks [107]. Digital watermarks handle complex ownership and tamper detection [108]. Although, the watermark imperceptibility enables secure communication without compromising the host image integrity against the attacks. As based on Figure 2.7, an attack is a strategy for reducing the contents' ability to be identified or shared through a watermark. Typically, the attacks on watermark are classified into two categories: ***accidental and malicious*** [109]. The malicious attacks are directed towards removing the embedded watermark, i.e., active attacks, whereas unexpected attacks do not intend to alter the watermark explicitly, i.e., passive attacks. Active attacks are introduced during the transmission of the watermark, and these attacks reap the advantages of prior information about the limitations of computational resources and embedded approaches. The malicious attacks are further classified as ***geometric and signal processing attacks***[110]**,** illustrated in Figure 2.8.

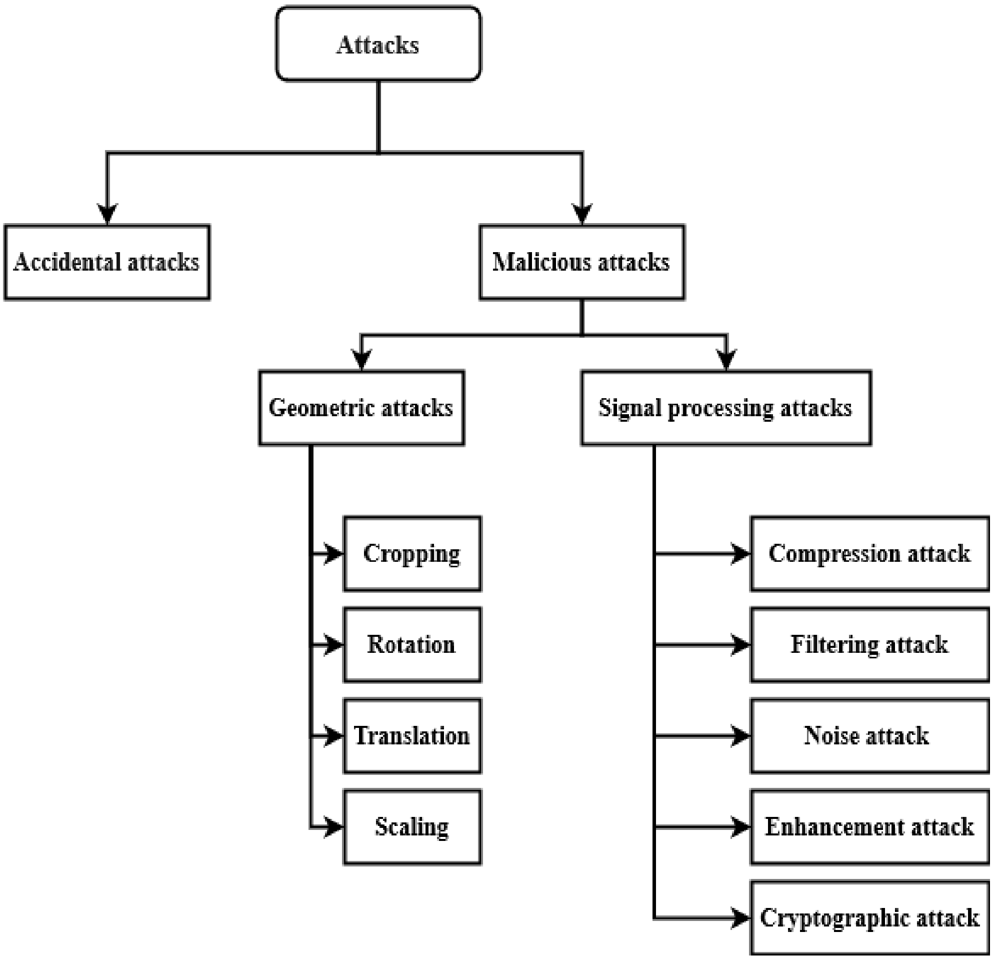


Figure 2.8 Classification of attacks on the watermarked image

- ***Geometric attacks*** are also stated as detection-disabling attacks. This attack modifies the watermarked image temporally and spatially, causing the detector not to detect the watermarked image during the extraction process. The geometric attacks include ***cropping, rotation, translation, and scaling*** [110]**,**[111] [112]. Cropping means clipping a segment from the watermarked image and discarding the rest. Rotation means flipping a pixel in an input image to its corresponding position as an output image. Image pixels are moved to a new position in the resulting image. Scaling alters the size of the picture. Therefore, the watermark must be disseminated across the dimensions to resist geometric attacks.

- ***Signal processing attacks*** are also known as removal attacks that completely remove the owners' secret information from the watermarked image without compromising the security of the watermarking algorithm. Signal processing attacks include ***compression, filtering, noise, watermark enhancement, and cryptographic attacks***[110]**,**[112]**.**
  - ***Compression*** means reducing the image size to preserve time and space. For instance, if the watermarked image is not in JPEG format, the attacker can convert it into JPEG format by reducing the "quality factor" of JPEG compression until the image loses its targeted features[113]. Thus, the attacker can also resave the image with a lower quality factor. Therefore, JPEG compression resistance is essential in robustness evaluation.
  - ***Filtering attack*** removes host image frequencies to prevent interference (electromagnetic or electrical) and background noise. However, the high-frequency features such as edge details sharpen and refine the image[110]. Low-frequency components such as smooth variations provide the base image. Therefore, smooth variations are essential rather than the details. Further, filters are classified as smoothing and blurring. The most widely applied smoothing filters are averaging, low, median, and high pass filters. A low pass filter smooths out images by removing the high-frequency features. An image using a high pass filter removes out low-frequency characteristics due to sharper edges. The median and averaging filters replace each pixel with median and average values of the adjacent pixels. The term "blurring filters" refers to a collection of filters that segment images or blur images. These filters are classified as Gaussian and motion filters; Gaussian filtering blurs images by removing noise and information by employing a Gaussian function. A motion filter directs the camera in a specific direction, creating the illusion of linear, radial, or circular motion. Apart from these filters, Wiener filters are reverse low pass filters impact[114].
  - ***Noise attacks*** are leveraged to reduce excessive signals (electromagnetic or electrical) and data quality. Noise attacks include Gaussian and salt & pepper noise. Gaussian noise is a geometric noise with the Gaussian

density function. Salt & pepper noise is represented by white and black pixels. The corrupted pixels are set to a maximum value of zero, resulting in a salt & pepper effect in the image[114].

- ***The watermark enhancement*** technology enhances output image the quality by altering the host image’s pixel intensity. Histogram equalization is widely employed to enhance the image that compresses and expands the image histograms to dynamic ranges, enhancing contrast. Sharpening enhancement improves the image edges information[114].
- ***Cryptographic attacks*** target the watermark security that extracts the owners’ secret information from the watermarked image by applying the brute-force attack. This method determines the private key used in the embedding process by identifying many possible strategies for extracting the watermark.

Consequently, copyright protection is required to resist these attacks, for that trade-off between robustness and imperceptibility is vital[115]. As a result, the researchers have emphasized the watermarking techniques to obtain imperceptibility, robustness, and security.

2.2.3.Provisions for digital watermarking

An excellent digital watermarking scheme is constructed by considering several features and properties such as imperceptibility, robustness, capacity, computational complexity, security, reliability, embedded effectiveness, and host quality[116], as illustrated in Figure 2.9. However, while designing the effective watermark, most researchers are focused on imperceptibility and robustness against various attacks such as accidental or malicious and capacity.

- **Imperceptibility:** The imperceptibility requirement concerns the visibility of the embedded information. It denotes to the perceived resemblance between the host and watermarked image. The imperceptibility is determined using two performance metrics: structural similarity index measure (SSIM) and peak signal-noise ratio (PSNR). However, the imperceptibility is measured with a watermark and considers the portion where the watermark is embedded [117].

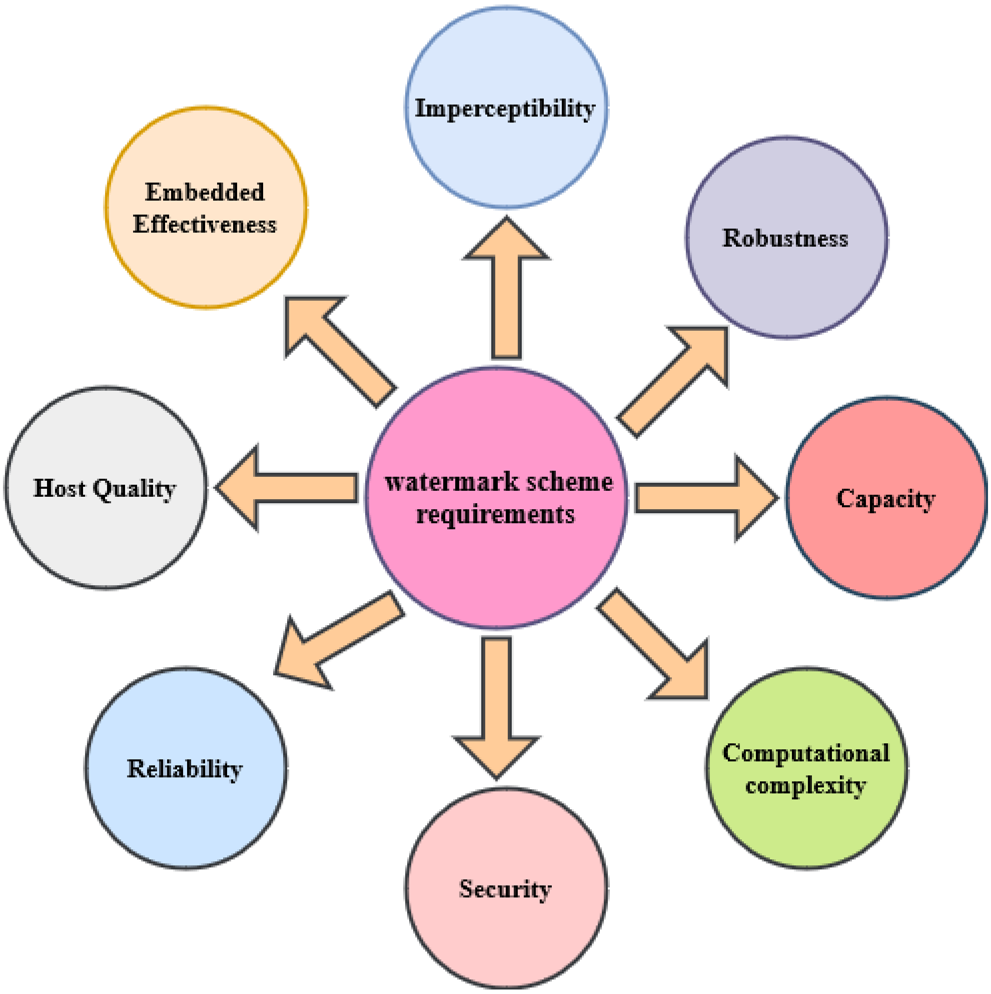


Figure 2.9 Provisions of digital watermark

- **Robustness:** The robustness requirement deals with the resistance against various attacks on the watermarked image during the transmission. The watermark robustness can vary from attack to attack, and it is an application-specific requirement. For example, tamper detection applications do not require robustness, military and medical documents do not allow quality degradation, and copyright protection applications are suitable for robustness[8].
- **Capacity:** The capacity requirement is about the amount of information embedded in the host image without degrading the quality. Especially, if the secret information has the $N - bits$ then 2^N Watermarks are possible. The watermark capacity never depends on the watermarking

algorithm and host image characteristics. The capacity requirement may change based on the application. For instance, labelling applications require several thousands of bits, security applications based on fingerprinting and copyright protection require tens of bits to embed into the host image[112].

- **Computational complexity:** The algorithm's complexity depends on the time to perform the embedding and extraction operations. Therefore, security applications are required high complexity for embedding and extraction operations, whereas real-time applications require quick execution algorithms[118].
- **Security:** The security requirement determines the efficiency of the watermark algorithm against malicious watermark extraction. Therefore, the watermark protection algorithm depends on the embedded scaling factor restricting the illegal extraction[119].
- **Reliability:** The user is frequently aware of the appropriate algorithm for extracting and deactivating the watermark rendering. As a result, the watermark is protected through the secret code. Simultaneously, if the user knows the extraction algorithm, it is impossible to identify the same secret code used during the embedded process. Thus, it increases the watermark reliability[120].
- **Host quality: The** host image quality should not be compromised owing to the watermark information embedded in the host image. As a result, it affects the watermark information, and hence the host image quality is crucial[109], [111].
- **Embedded effectiveness:** The probability of the detection assesses the effectiveness of the watermark system following the completion of the embedded process. While 100% embedding efficiency is acceptable, it is often compromised due to the impact of the other provisions[121].

2.2.4.Classification of digital watermarking

The watermarking techniques are classified according to the kind of data that includes an embedded operation for information security. As shown in Figure 2.10[122].

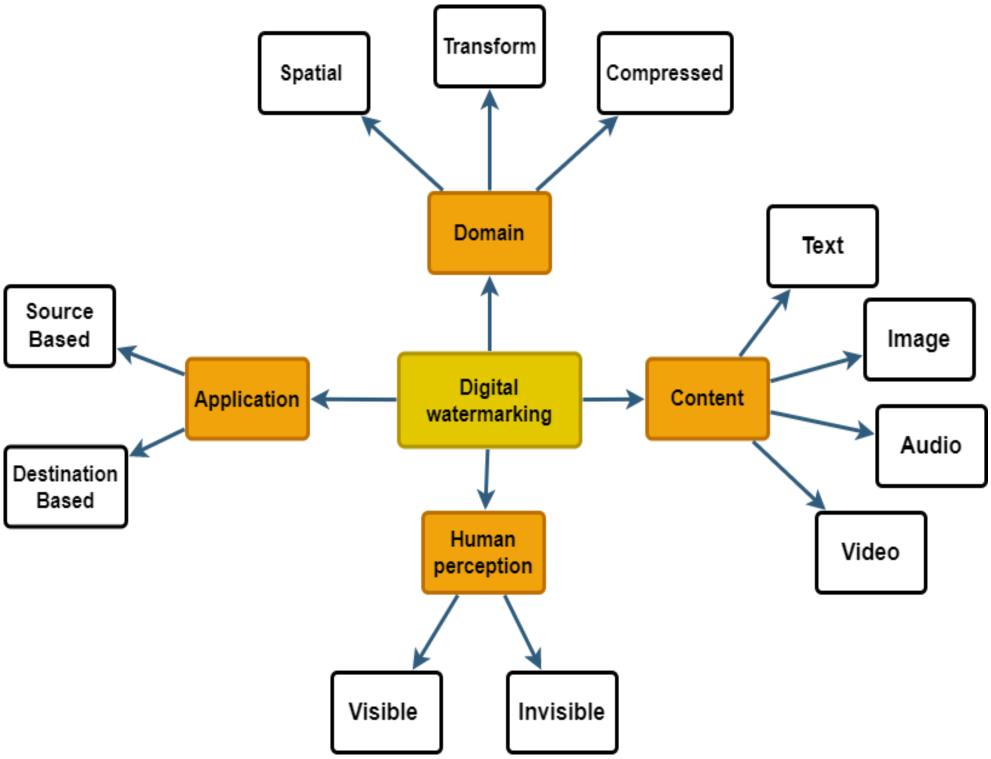


Figure 2.10 Classification of watermarking schemes

Digital watermarking is classified according to content, human perception, application, and working domain. The working environment is further broken into transform, spatial and compressed approaches. Although the spatial domain is more straightforward than the transform domain, the transform domain still provides a high level of resistance [123], [124]. The content is available in text, audio, video, and image, protected through watermarking techniques. The human perception of security is categorized into visible and invisible watermarking. Visible watermarking deals with copyright protection of the image and video. The invisible watermark cannot differentiate the original and watermarked content. Additionally, it is classified as fragile, semi-fragile, and robust.

2.2.4.1.Content-based watermarking

Watermarking approaches are classified according to media content transmitted over the internet, encompassing image, text, audio, and video[122]. The details are as follows.

- ***Text watermarking*** includes the watermark information into the text file, preventing unauthorized modification or reproduction of authorized text documents. This technique of watermarking details is incorporated in text font forms between line and character spaces. However, the purpose of the text watermark is to prevent the illegitimate reproduction, re-distribution of copyright content, forgery or plagiarism, and other forms of copyright breaches in the text documents, including e-books, journals, legal papers, memoirs, newspapers, literature, and blogs. On the other hand, the content owner is oblivious of illegal downloads, examination, and update. As a result, text content ownership rights and integrity are critical in digital security.
- ***Image watermarking*** strategy hides the secret user information in the image or alters the co-efficient. This approach is leveraged to detect and extract the watermark information to provide ownership rights[8], [118].
- ***Video watermarking*** inserts the watermark into the video stream that controls the applications. This approach is an extension of the image watermark. Thus, it performs the extraction in real-time and the compression resilient [125].
- ***Audio watermarking*** is the most essential and hot favorite to restrict the illegal access of MP3 because of internet music.

2.2.4.2.Human perception

Human perception is listed as perceptible and imperceptible watermarking.

- ***Perceptible or visible watermarking*** embeds the owner’s information into the cover image. Visual watermarking solutions protect the images and videos against infringement[101].
- ***Imperceptible or invisible watermarking***, the cover image incorporates the watermark information. Thereafter, the human visual system cannot discriminate between the cover and watermarked images until the extraction operation is performed. Although, the invisible image watermarking is further classified as fragile, semi-fragile, and robust depending on the changes made during transmission and attacks. The ***fragile watermark*** quickly identifies the content loss or modifications.

After that, it cannot retrieve the watermark. However, the attack portion is impossible to identify and used in content integrity proof[105]. The ***semi-fragile watermarks*** sustain regular changes but not malicious ones. However, the watermark is safe to broadcast over the network unless any image-processing attack occurs. Thereafter, the watermark is unrecoverable. This method is employed in tamper detection[101].

- ***Robust watermarking*** is secure and resistant to attacks. As a result, the watermark may be recovered even after the attacks and employed for copyright protection[126].

2.2.4.3.Application

According to the application perspective, the watermarks are classified as a source and destination-based watermarking; the details are as follows.

- ***Source-based approaches*** are used to identify ownership or authentication. In this approach, the specific user identity is inserted into all the copies of particular images that are transmitted[92].
- ***Destination-based approaches*** receive the watermarked copy and verify the buyers' identification. This approach is used to trace the illegal distribution[98].

2.2.4.4. Domain

The watermark algorithms are categorized according to the embedded process, such as spatial and transform domain. These domains are further categorized as illustrated in Figure 2.11 and details as follows.

- **Spatial watermarking domain**

This method converts the digital data into pixel format and then alters the cover signal pixels to hide the watermark data. Although, the spatial watermarking domain is more versatile. Therefore, it is less sophisticated, permits more bits in the cover image, and consumes less computational and communication time. This approach is less immune to attacks such as lossy compression. The spatial domain watermarking techniques is as follows.

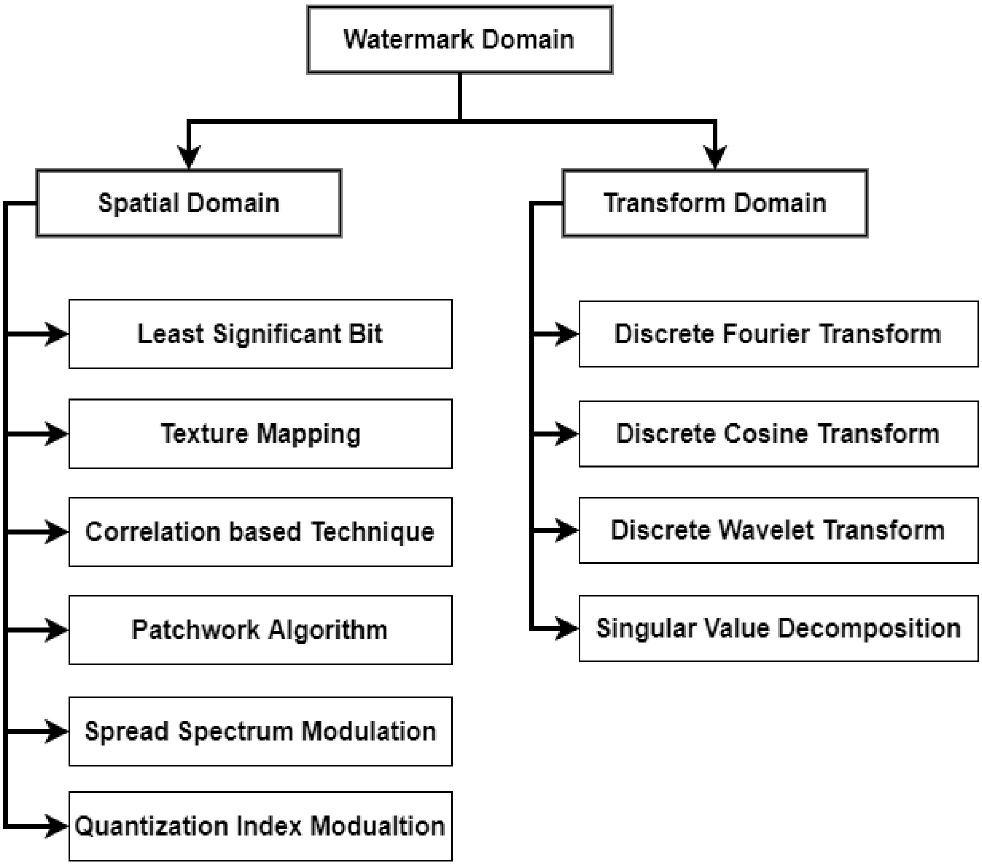

Watermark Domain
Spatial Domain
Transform Domain
Least Significant Bit
Texture Mapping
Correlation based Technique
Patchwork Algorithm
Spread Spectrum Modulation
Quantization Index Modualtion
Discrete Fourier Transform
Discrete Cosine Transform
Discrete Wavelet Transform
Singular Value Decomposition

Figure 2.11 Classification of watermark embedded domains

❖ ***Least significant bit (LSB)***

This strategy incorporates the watermark bits in the LSB of the cover image's specified pixel [121]. For instance, if the original image size is 256x256, the 150-pixel position is selected and encoded as 10010110 in the 8-bit sequence. While watermark information is 1100, and the resulting watermark pixel value is 156, shown in Table 2.5. However, this method is resilient to cropping attacks, but not noise and compression attacks. Moreover, since the passive attacker has done elementary operations, it rapidly recovers the altered bits by randomizing all LSB's.

Table 2.5 LSB digital watermarking model for 1-bit [127]

Selected pixel value	1	0	0	1	0	1	1	0
Watermark information					1	1	0	0
Watermarked Pixel value	1	0	0	1	1	1	0	0

❖ *Texture mapping*

This technique works well with images that include a variety of textures. Watermarking hides the secret information in the images' selected texture region. Indeed, this technique is not automated and works best in regions with a high density of random texture images. This method hides data inside the random texture information of an image[109].

❖ *Correlation-based technique*

The cover and watermark information images as $C_I(p,q)\ and\ W_I(p,q)$. The $W_I(p,q)$ is embedded into $C_I(p,q)$ through $M_I(p,q) = C_I(p,q) + \alpha * W_I(p,q)$. Here $M_I(ip,q)$ and α denotes the watermarked image and gain factor. The robustness and imperceptibility enhancement of the watermark depends on the selection of the gain factor. However, the watermark restoration is accomplished through a Pseudo-Random Noise Generator (PSNG). While detecting the watermark, a single bit is set if correlation exceeds the pre-defined threshold T. Thus, it is accomplished for every image block[101].

❖ *Patchwork algorithm*

This scheme uses the pseudo-random statistical approach to achieve the invisibility embedding using Gaussian distribution. For instance, the patches are selected from two images using pseudo-random that are brightness and darkness. Then, the statistical patchwork approach is used to accomplish the redundant pattern encoding by embedding the information into the image.

❖ *Spread-spectrum modulation (SSM)*

The image's watermark embedded into undesirable regions are easily destructed by the signal and geometric attacks. Nevertheless, SSM selects the massive bandwidth to transmit the tiny gesture. As a result, watermark information is dispersed across several frequency sub-bands, rendering it almost invisible. This scheme embeds the watermark into perceptually important data regions, making them resistant to conventional watermark attacks. Additionally, this scheme involves a minor human visual system (HVS), but the extraction process still requires the original image. Moreover, the slight depreciation may result in watermark destruction because of the watermark fragility[128].

- ***Quantization index modulation (QIM)***

Brian Chen developed the first quantization approach for watermarking as QIM [129]. In this approach, the embedding parameter splits the watermark's value into discrete index intervals—the extraction parameter analyses the co-efficient index interval to select the appropriate watermark. The watermark is embedded and identified through QIM. The index intervals are recomputed to correspond to the embedding domains features. However, this approach has limited resistance to scaling attack because index interval remains constant throughout the embedding and extraction process. The quantized coefficients change with scaling and may fall into different intervals than the embedded coefficients during extraction. As a consequence, the extraction procedure produces inaccurate results.

- **Transform watermarking domain**

This approach, also known as a frequency domain, involves modifying the cover image data using transformation algorithms. Thereafter, depending on the watermarking information, the alteration is performed to the converted co-efficient. As a result, this approach is more robust and invisible than the spatial domain. Consequently, the following transform watermark domains are often employed to protect copyright.

- **Discrete Fourier transformation (DFT)**

In DFT, the watermark information is implanted by selecting the appropriate frequency components of the host image, and image coefficients are complex numbers such as magnitude and phase. The DFT provides robustness against geometric attacks. However, the dimensional image changes influence the rending degree but not the volume, or circular shifts demonstrate the transforms translation invariance. Moreover, the DFT is anti-cropping since cropping results in spectrum blurring. Since the watermarks are embedded in the magnitude of the images, then no need for synchronization between normalized coordinators[120], [130].

❖ Discrete cosine transformation(DCT)

DCT represents the information in the frequency domain rather than the magnitude or phase domain. DCT is accomplished by embedding the watermark information in the middle-frequency cover images, enhancing its resistance to lossy compression[121], [128], [131]. In contrast to the spatial domain, this approach is more dependable. However, DCT resists conventional image processing techniques such as low-pass filtering, contrast enhancement, blurring and brightness augmentation. While DCT is more computationally expensive, it is more susceptible to geometric attacks such as cropping, rotation and scaling.

❖ Discrete wavelet transformation(DWT)

The 2D-DWT is used to decompose the image into the four non-overlapping multi-frequency sub-bands. The sub-bands are Approximation (LL), Horizontal (LH), Vertical (HL) and Diagonal (HH). Further, recurrently applied the same procedure to yield multiple wavelet decomposition, as illustrated in Figure 2.12. However, the human visual system is more sensitive to the LL sub-band. Thus, it is recommended to include the watermark information in LL. Although, the embedded operation in the LL sub-hand improves the robustness significantly in contrast with the HH-sub band. Moreover, DWT offers better temporal resolution over the DFT and DCT. It stores the latitude and frequency information also[8], [9], [126], [132], [133].

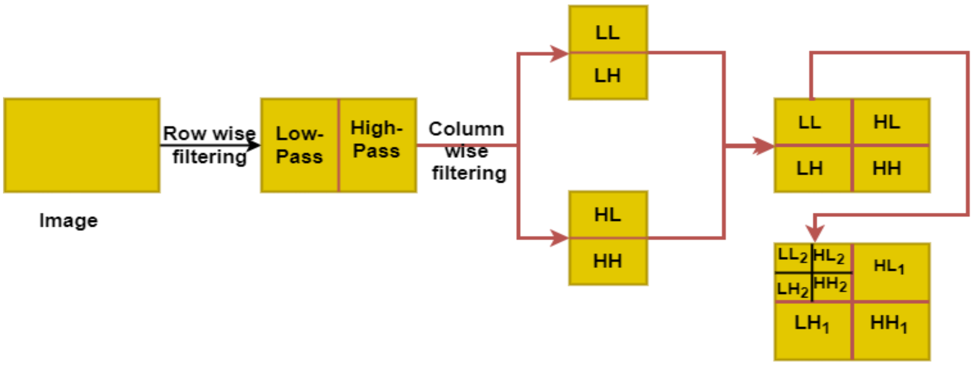


Figure 2.12 Level-2 decomposition

- **Singular value decomposition (SVD)**

SVD works on images represented in matrices with $'m'$ rows and $'n'$ columns as a size. The SVD's primary purpose is to resist geometric attacks [8], [118], [120]. Although, the SVD decompose the matrix into three matrices: *U, S, V*. Here U *and* V are orthogonal matrices of size $m \times m, n \times n$, and S is the diagonal matrix of size $m \times n$. The diagonal matrix contains the singular values of the matrix, which are unique values that offer the scale, rotation and translation affine. The *U, S, V* matrix properties are presented in Table 2.6.

Table 2.6 Properties of SVD

Type	U	S	V
Matrix type	Orthogonal	Diagonal	Orthogonal
Matrix values	Not unique	Unique	Not unique
Data type	Real	Real	Real
size	$m \times m$	$m \times n$	$n \times n$

Table 2.6 shows the SVD properties in watermarking approaches. Here *U* and *V* indicate the geometric image features and *S* denotes the image's brightness. As a result, tiny modifications to the image have a lower impact on the diagonal (*S*) matrix.

2.2.4.5.Comparison between spatial and transformation domains

The spatial and transformation parameters are compared, and the results are presented in Table 2.7

Table 2.7 Examines the spatial and transform domains

Category	Spatial domain	Transform domain
Watermarking Strategy	The host image pixel values are changed to meet the watermark image.	The host image's coefficients are adjusted to reflect the watermark image's coefficients.
complexity	Less	Impact the type of transform employed.

Protection against attacks	It reduces robustness and imperceptibility.	It enhances robustness and imperceptibility.
Watermark value distribution	Host image in regards to the discrete locations.	Across the host image, as a result of the change.

According to Table 2.7, the comparison shows that the transformation approach provides more imperceptibility and robustness over the spatial domain. The spatial domain watermarking approach changes the pixel values, reflecting on the cover image. In the transformation domain, the watermark information is adjusted in the cover image; hence the watermark information is invisible to the human visual system. Therefore, transformation domain watermarking is better than spatial domain watermarking.

2.2.5.Classification of watermark extraction methods

Watermark extraction methods are divided into three categories such as blind, semi-blind and non-blind techniques [134]. **Blind *watermark extraction*** is known as public watermarking and applied without using host and watermark images. However, the blind extraction methods are less resistant and complex to implement[135]. ***Semi-blind extraction*** requires information about the host image to extract the watermark[134]. ***Non-blind extraction*** techniques compare the extracted watermark with the original watermark information image. This approach provides more robustness.

2.2.6.State-of-the-art on 3D Anaglyph watermarking methods

Recently, the experts developed a novel concept named a stereogram [136]. A stereogram is a depth-perception visual distortion generated from 2D images. The most common stereogram images are 3D Anaglyph image [137], which appears as 3D stereoscopic. These images are viewed via two-color glasses that include red-cyan colors. However, the 3D Anaglyph images are composed of two color elements stacked with the impression’s depth. In general, the depth is at the center, and the foreground and background are displaced slightly in opposite directions. The 3D Anaglyph images consist of two unique filtered color images, one per eye viewed through anaglyph glasses. The visual frontal center converts the information into a 3D image. Moreover, these models offer a more precise color representation and rendering, challenging to accomplish.

In recent decades, 3D visualization has been significantly deployed in many areas, including visual arts, education, percussive motion, sculpting, and gaming. The study’s primary purpose is to protect 3D Anaglyph images transmitted over mobile networks. Therefore, the attackers easily copied the multimedia data, changed and reverted to the network. Consequently, a framework is required to protect the 3D Anaglyph images through watermarking approaches. Therefore, the survey of 3D Anaglyph image watermarking techniques works in the frequency domain. In this domain, the proprietors’ confidential information is incorporated into the original image frequency. Consequently, these techniques offer a high degree of resilience at the image quality trade-off. The present study examines several watermarking schemes applied to 3D anaglyph images, and videos are described below.

2.2.6.1.Watermarking techniques on 3D Anaglyph images

Bhatnagar et al. [120] established a system for protecting three-dimensional anaglyph images leveraging the Fractional Fourier Transform (FrFT) realm of secret color channels incorporated in SVD. The covert color channels are created by performing a reversible integer transformation on the RGB data. This method offers reasonable imperceptibility and robustness for malicious attacks. Nevertheless, since this technique does not use embedded watermarking, it suffers from a false positive rate and does not provide authentication. Therefore, users may argue ownership rights over digital objects. Zadokar et al. [133] proposed a DWT based 3D Anaglyph image watermarking scheme for copyright protection. This approach extracts the watermark effectively for various attacks except for noise attacks on a frontal image.

Prathap et al.[135] developed a blind robust algorithm using 3D-DWT and a Jacket matrix for 3D Anaglyph images. Indeed, the 3D-DWT is applied on a 3D Anaglyph image decomposed into several levels and jacket matrix applied to middle sub-band blocks. Beyond that, the watermark information is embedded by altering the diagonal component of each block with a 2x2 size. As a result, this scheme offers high imperceptibility to geometric and signal processing attacks because of the several-level decomposition contained in the middle sub-band. However, this approach requires more computation time.

Patel et al. [132] suggested a DWT technique for 3D anaglyph images. The watermark information is embedded in the left image by leveraging the DWT. Then, the watermarked image is merged with the right image that constructs the anaglyph image. The watermark information is retrieved from the left image through the inverse procedure. This approach demonstrates the critical nature of invisibility. However, it takes the extra time to rebuild the right image and has a low level of attack resistance. Munoz-Ramirez et al. [131] proposed a color image watermarking for 3D Anaglyph images using DCT and dither modulation with QIM (DM-QIM). In this scheme, the host and watermark images are RGB that transformed to YC_bC_r during the embedded process. The host image's luminance 'L' value is designated and decomposed into 8x8 blocks, thereafter applying the DCT. Moreover, the DM-QIM strategy changes the DCT's early 12-bits. Accordingly, the watermark image's brightness is selected after subsampling (4:2:0) to produce the watermark by performing DM-QIM implantation per block. This approach offers robustness and invisibility; still, the computation cost increases according to the size of the image. Wang et al. [128] devised watermarking schemes to protect the stereo images copyright through SSM. Another strategy involves adaptive dither modulation (ADM) with an enhanced Watson perception system. The watermark embedding process in the SSM approach selects the maximal frequency coefficients in the DCT domain. It then alters the frequency co-efficient to insert the watermark information without using PSRM. The extraction process is applying the blind watermark extraction. The watermark is inserted into the DCT domain's middle-frequency co-efficient in ADM with an enhanced Watson perception scheme. The extraction process employs a technique called minimum distance detection. While comparing the two approaches, it is clear that the ADM with an enhanced Watson perception scheme offers a high degree of invisibility and resistance to signal processing attacks. However, due to binary images, these approaches decrease the embedded capacity.

Rakesh et al. [130] performed the embedded operation in the blue channel, i.e. the right image of the 3D Anaglyph image through Fractional Fourier Transformation ($F_r FT$). Then, the marked image is merged with the left image that generates the 3D Anaglyph image. Although, it produces a low degree of invisibility. Devi et al. [126] scheme leverage the various approaches, including DWT, Genetic Algorithm (GA) and Advanced Encryption Standards that offer copyright protection for 3D red-cyan color Anaglyph images. This scheme applies the DWT on host images then uses the GA algorithm to optimize the DWT bits before they are sent into the Back Propagation Network (BPN). More performs the embedded procedure with the optimized bits after employing the AES encryption algorithm to the watermark information. Therefore, it offers high resilience. Nonetheless, the computational complexity of the training phase is high, and if the training phase fails, there is no obvious recovery method.

The other approach of Devi et al. [138] embeds and extracts a watermark using composition wavelet transformation and principal component analysis. Initially, watermark information is encrypted through the Arnold transformation and then performs the embedded operation using Principal Component Analysis (PCA) into a selected sub-band of composition wavelet transformation. Therefore, this scheme offers a high degree of invisibility. However, this scheme uses the binary marks as watermark information, requiring additional computational time.

Devi et al. [8] suggested employing DWT and SVD to preserve 3D anaglyph images against infringement. Primarily, the DWT is implemented over the blue component of an Anaglyph image. The vertical sub-band is elected, followed by the Fast wavelet Hadamard Transformation (FWHT) and SVD. Thereafter, the watermark information is distorted into 32×32 employing Arnold Transformation. The embedded procedure is carried out in accordance with the scaling factor. As a result, this framework offers resilience and imperceptibility with a watermark logo size of 32×32. Nevertheless, this strategy has a low resilience to rotation and filtering attacks.

Subhadeep Koley [118] framework employs the lifting wavelet transformation (LWT) and tensor-SVD (T-SVD) on 3D anaglyph images. On the 3D Anaglyph image, apply the LWT and elect the LL sub-band before performing the T-SVD. Thereafter, using Arnold cat map, scramble the watermark information before applying the embedded processing that yields the watermarked image. This framework offers invisibility and resilience to several attacks, excluding the rotation attacks.

2.2.6.2.Watermarking techniques on 3D Anaglyph videos

Waleed et al.[139] developed 3D Anaglyph video watermarking using DWT. In the embedded process, the DWT decomposes the blue channel of all the frames and selects HH sub-band applies 4-level decomposition on it. However, the attacker quickly destroys the watermark by attacking the blue component. Salih et al. [140] proposed a scheme based on the Waleed approach [139], where the watermark is embedded in the scene change frame. However, if the scene change in the video is limited to a small number or a single scene, then fragile watermarking can be accomplished. Dhaou et al. [141] proposed a group of pictures (GOP) based DWT scheme for the 3D red-cyan videos. The video is divided into a set of GOP's and each GOP is decomposed into red(R), blue (B) and reference or indirect (I) images. The embedded process applies the blue component of B, the red component of R, and the red, blue and depth component from I images through the DWT scheme, then combines the marked images. Therefore, this approach provides a high degree of invisibility and robustness but suffers from collusion attacks.

Dhaou et al. [121] proposed LSB, DCT and DWT based hybrid 3D video watermarking. The 3D video is segmented into frames, and the red-cyan images are extracted from each frame. The watermark information is then embedded into each red image through LSB and DCT scheme applied to each cyan image's middle sub-band. The 3D Anaglyph watermark is created by combining red and cyan watermarked images. Another mark is embedded using the 1-level DWT on 3D Anaglyph watermarked with the LL sub-band. Finally, it uses the inverse DWT (I-DWT) to reconstruct the 3D Anaglyph watermarked frames. This approach is robust and invisible. However, this scheme suffers from collusion attacks. Another method of Dhaou [142], [143] presented to handle collusion attacks through multi-sprite generation. In the first approach, the 3D Anaglyph video is segmented into various sets of 25 frames and generates a sprite for each group. The 3-level DWT is applied on each sprite then the watermark information is embedded through the middle significant bit algorithms on LL and LH sub-bands. Also, the watermark information is embedded in the HH and HL sub-bands through the DWT embedding process. Finally, the watermark is produced through a 3-level I-DWT. In the second approach, the embedded process applies on the LL sub-band with LSB, LH and HH sub-bands used with the DWT embedded process. However, the second approach [143] provides better resistance than the first approach [142]. Jabra [125] uses a 3D Anaglyph video that extracts the 3D cyan-red videos. Then, it creates the cyan mosaics from the cyan video and computes the krawtchouk moments' matrix. The watermark information is embedded in the matrix using DCT to produce the cyan video watermark. Finally, it combines the cyan video with the original red video with the watermarked video. Therefore, this scheme provides the resistance to type I and II collusion attacks but still requires improvement. Thus, the summary of the 3D Anaglyph images and videos watermarking scheme is outlined in Table 2.8.

Table 2.8 Comparative analysis of recent studies over 3D Anaglyph image and video watermarking schemes

Author	**Domain**							**Content**		**Findings**
	S	**Transformation**								
		F_r	D_f	D_c	D_w	L_W	S_V	I_m	V_e	
Bhatnagar et al. [120]	×	√	×	×	×	*X*	√	√	×	• This method uses grayscale images that provide reasonable robustness and imperceptibility for various attacks.

										• Suffers from the false positive rate.
Zadokar et al. [133]	×	×	×	×	√	×	×	√	×	• Suffering from Noise attacks and false-positive rate.
Ivy et al. [135]	×	×	×	×	√	×	×	√	×	• Provides the high imperceptibility for geometric and signal processing attacks. • Requires more computation time.
Patel et al. [132]	×	×	×	×	√	×	×	√	×	• The extraction process requires extra time to reconstruct the right image. • Less resistance to attacks.
Munoz-Ramirez et al.[131]	DM-QIM	×	×	√	×	×	×	√	×	• This approach offers robustness and imperceptibility. • Increases the computational cost that depends on the image size.
Wang et al. [128]	SSM, ADM	×	×	√	×	×	×	√	×	• This method suffers from lower-level imperceptibility. • High complexity.

Yadav et al. [130]	×	√	×	×	×	×	×	√	×	• Provides a low level of invisibility.
Devi et al. [126]	×	×	×	×	√	×	×	√	×	• The training phase provides high computation complexity. • If the training phase fails, there is no obvious recovery method.
Devi et al. [138]	PCA	×	×	×	√	×	×	√	×	• Provides a high degree of invisibility. • Uses binary marks that require additional computation time.
Devi et al. [8]	×	×	×	×	√	×	√	√	×	• The resistance against filtering and rotation attacks is less.
Koley [118]	×	×	×	×	×	√	√	√	×	• Requires improvement in rotation and histogram attacks
Waleed et al. [139]	×	×	×	×	√	×	×	×	√	• The attacker quickly destroys the watermark by applying the attack on the blue component.

										• Not robust against malicious attacks.
Salih et al. [140]	×	×	×	×	√	×	×	×	√	• The scene change detection is limited in the video as a single scene or a small number of scenes, and then fragile watermarking can be accomplished. • Not robust against malicious attacks
Dorra et al. [141]	×	×	×	×	√	×	×	×	√	• Suffering from collusion attack.
Dorra et al. [121]	LSB	×	×	√	√	×	×	×	√	• Suffering from collusion attack. • Requires additional time for reconstruction.
Dorra et al. [142]	MSB	×	×	×	√	×	×	×	√	• Less resistant to collusion attacks.
Dorra et al. [143]	LSB	×	×	×	√	×	×	×	√	• Resist the collusion attacks but requires improvement in it.
Jabra et al. [125]	×	×	×	√	×	×	×	×	√	• Provides the resistance to both type I and II collusion attacks but requires watermark information

										embedding in the cyan-red images.

S: Spatial domain,F_r: F_rFT,D_f: DFT, D_c: DCT,D_w: DWT,L_w: LWT,S_v: SVD,I_m: image,V_e: video

2.2.7.Critical analysis

The existing watermarking approaches are reviewed in Table 2.8, and it is noted that the critical challenges are mentioned below.

i. The copyright protection for color images is accomplished by converting RGB images into YC_bC_r or grayscale images and performing the embed process resulting in the information loss.

ii. The majority of existing schemes are oriented on the DCT and DWT domains resistant to the geometric and signal processing attacks over the 3D Anaglyph images but need computational, invisibility, and robustness improvements.

iii. The majority of the watermarking schemes are overlooked the False Positive Problem (FPP) and invest little effort in resolving it.

iv. The existing DWT schemes do not demonstrate how to select the embedded strength factor that determines the robustness and invisibility of the scheme against the various attacks.

v. None of the strategies is geared at copyright protection via variable watermark information sizes.

2.3. Summary

The current chapter describes the various P2P environment trust source of information, trust, and reputation models. The comparative analysis of different trust models that assess the certainty or uncertainty trust and the reputation trust models employed to determine the indirect trust in the P2P environment. Although, the comparative study of the taxonomy is provided based on the existing trust approaches in the P2P system and identified the critical challenges of the trust and reputation models. Therefore, most models are suffering from computational and communication overhead. However, less work is focused on uncertainty trust assessment.

Similarly, it presented the need for content protection techniques in a P2P environment and the existing strategies for digital image protection. Also, it showed the need for digital watermarking and a variety of threats, provisions, and usage. The digital watermarking taxonomy is used in embedding and extraction processes. Furthermore, it encompasses several distinct digital watermarking algorithms available for 3D Anaglyph images and videos, highlighting the essential aspects. As a result, most watermark systems suffer from invisibility, resilience, computational complexity. On the other hand, FPP receives less attention. The subsequent chapters of the thesis will provide the framework for our research lines based on this work.

CHAPTER 3

PROPOSED FRAMEWORK FOR TRUSTWORTHY PARTNER SELECTION SCHEME

This chapter develops an I-3VSL paradigm for assessing players' trust in MMOG. Designing such a paradigm is complex since trust is hard to comprehend in MMOG. Therefore, to manage trust effectively, the probability distribution with three distinct realms: belief, disbelief, and uncertainty. The trust states variations are examined over the trust propagation using 3VSL[61] and redesigning it. In I-3VSL, trust opinions are formed from the relationships between the players. Moreover, trust fusion is designed through combining operations. Hence, the direct and indirect trust between the players is computed using discounting and combining operations. Further, the Trustwalker algorithm is developed using I-3VSL to assess the trust in MMOG with arbitrary or bridge networks, and its experimental and evaluation details are included.

3.1. Theoretical Framework

To comprehend I-3VSL effectively, first examine the 3VSL[61] based on the interactions between players A and B. Thereafter, express the trustworthy opinion from A's perspective on B as

$$W_{AB} = (b_{AB}, d_{AB}, n_{AB}, e_{AB})|a_{AB} \qquad (3.1)$$

$$b_{AB} + d_{AB} + n_{AB} + e_{AB} = 1 \qquad (3.2)$$

Where b_{AB}, d_{AB}, n_{AB} represents the posterior probabilities from A's perspective on B is belief, disbelief, and posterior uncertainty, respectively as Eq. (3.1). The prior uncertainty opinion e_{AB} is 3 includes belief, distrust and uncertainty. The base rate a_{AB} is established based on the prior perception without substantial proof, e.g. preferences, partiality or gossip. For example, if ‘A’ persistent trust or distrust a member of a particular community to which 'B' belongs, thus a_{AB} will be less/greater than 0.5. Consequently, the players' have direct interaction from $A\ to\ B$ and their trust opinion is depicted as W_{AB} with four states such as

$$\begin{cases} b_{AB} = \dfrac{r_{AB}}{r_{AB} + s_{AB} + o_{AB} + 3} \\ d_{AB} = \dfrac{s_{AB}}{r_{AB} + s_{AB} + o_{AB} + 3} \\ n_{AB} = \dfrac{o_{AB}}{r_{AB} + s_{AB} + o_{AB} + 3} \\ e_{AB} = \dfrac{3}{r_{AB} + s_{AB} + o_{AB} + 3} \end{cases} \tag{3.3}$$

Here r_{AB}, s_{AB}, o_{AB} are quality and quantity of the interaction between players "A" and "$B.$" For instance, player "B" shares the 8 pieces of information with player "A." The player "A"'s opinion on received information as 4 pieces of information is trust($r_{AB} = 4$), 2 pieces of information are distrust($s_{AB} = 2$), and 2 pieces of information are neither trust nor dis-trust ($o_{AB} = 2$). The trust opinion is produced using Eq. (3.3) from $A\ to\ B$ based on the trust, distrust, and uncertainty states observation, the prior uncertainty opinion($e_{AB} = 3$). As a result, the trust opinion between players $A\ to\ B$ is <0.36, 0.182, 0.182, 0.27>. If player A never interacted with B, then the direct trust opinion r=0, s=0 and o=0 and the prior uncertain option is 1 is represented as $w_{AB} =< 0{,}0{,}0{,}1 >$. Although player $'A'$ wants to interact with the $'C'$, they never interacted earlier. Nonetheless, player $'A'$ establishes the interaction with $'C'$ through the recommendation of player 'B''. Therefore, 3VSL applies the indirect trust assessment through the discounting operation that propagation trust from A to C. Assume the trustworthiness between $A\ to\ B$ is $W_{AB} =< b_{AB}, d_{AB}, n_{AB}, e_{AB} >$ and $B\ to\ C$ as $W_{BC} =< b_{BC}, d_{BC}, n_{BC}, e_{BC} >$. Then, the trust from $A\ to\ C$ is computed as W_{AC} using Eq. (3.4) is as follows.

$$\begin{cases} b_{AC} = b_{AB} b_{BC} \\ d_{AC} = b_{AB} d_{BC} \\ n_{AC} = 1 - b_{AC} - d_{AC} - e_{BC} \\ e_{AC} = e_{BC} \end{cases} \tag{3.4}$$

3.2. Discounting Operation

The discounting operation is specified in 3VSL in the context of modern trust propagation literature [61], [63]. Thus, trust propagation refers to transferring a player's trust opinion to another player. In other terms, if A believes B, then B's perception of C is carried to A. Conversely, if A distrusts or is uncertain about B, then A is also uncertain on C since B's perspective influences C as distrust is represented in Figure 3.1.

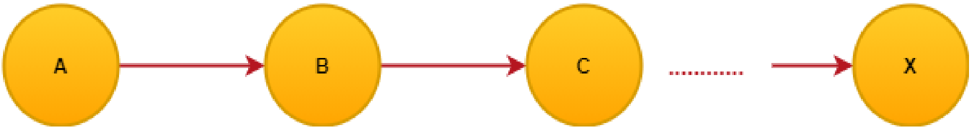


Figure 3.1 Serial topology for trust propagation

According to Figure 3.1, the trust evidence from A to B denotes $W_{AB} =< b_{AB}, d_{AB}, n_{AB}, e_{AB} >$ and $B\,to\,C$ denotes $W_{BC} =< b_{BC}, d_{BC}, n_{BC}, e_{BC} >$ then, the trust opinion from $A\ to\ C$ is measured using Eq. (3.4).

However, the finding in Eq. (3.4) is disregarded since only b_{AB}, b_{BC}, d_{BC} opinions are employed and d_{AB} is ignored in the evaluation of W_{AC}. Therefore, the changes of $d_{AB}, and\ \ n_{AB}$ have not influenced the trust evaluation of W_{AC}. Although, the trust opinion in 3VSL is composed of four states. Hence, the existing 3VSL discount operation required modification.

3.2.1.Improved discounting operation

The improved discounting operation substitutes the b_{AB} with the expected belief W_{AB}. Therefore, the effectiveness of the trust evaluation from $A\ to\ C$ is as follows.

$$W_{AC} = \begin{cases} b_{AC} = E(W_{AB})b_{BC} \\ d_{AC} = E(W_{AB})d_{BC} \\ n_{AC} = 1 - (E(W_{AB})(b_{AC} + d_{AC} + e_{BC})) \\ e_{AC} = e_{BC} \end{cases} \tag{3.5}$$

$$E(W_{AB}) = b_{AB} + a_{AB} * n_{AB} + e_{AB} * 0.5 \tag{3.6}$$

The expected belief $E(W_{AB})$ is computed through the belief, posterior, prior and base rate in Eq. (3.6). However, the base rate is determined employing probability theory, the default base rate at the center. As a result, the base rate is 0.5 since absolute belief equals 1 and complete distrust equals 0. The trust opinion derived from the recommendation is computed using Eq. (3.5).

Terminology 1 (Discounting Operation) *concerning the trustworthiness of three players A, B and C. The trust opinion from A's perspective on B is* $w_{AB} = < b_{AB}, d_{AB}, n_{AB}, e_{AB} >$ *and B's perspective on C is* $w_{AB} =< b_{BC}, d_{BC}, n_{BC}, e_{BC} >$*. The discounting operation computes the trustworthiness between A to C is through Eq. (3.5) and represented as*

$$W_{AC} = \Delta(W_{AB}, W_{BC}) =< b_{AC}, d_{AC}, n_{AC}, e_{AC} > \qquad (3.7)$$

Although, it is essential to realize that the discounting operation acquires the association property but not the cumulative property.

Corollary 3.1 Associative property: *concerning the trustworthiness of three pieces of evidence* W_{AB}, W_{BD}, W_{DE} *then the discounting operation acquires the results as* $\Delta(\Delta(W_{AB}, W_{BD})W_{DE}) \equiv \Delta(W_{AB}, \Delta(W_{BD}, W_{DE}))$.

Corollary 3.2 Commutative property: *concerning the trustworthiness of two pieces of evidence* W_{AB}, W_{BD} *then the discounting operation acquires the results as* $\Delta(W_{AB}, W_{BD}) \neq \Delta(W_{BD}, W_{AB}))$.

Proof: According to Eq. (3.5), the results are equal in the Associative but different in commutative.

Therefore, according to serial topology, the trust opinions are $W_{x_1x_2}, W_{x_2x_3}, W_{x_3x_4}, \dots W_{x_{n-1}x_n}$. Then, the discounting operation computes the results as $\Delta(\Delta(\Delta(W_{x_1x_2}, W_{x_2x_3}), W_{x_3x_4}), \dots W_{x_{n-1}x_n})$. According to associative property, it is streamlined as $\Delta(W_{x_1x_2}, W_{x_2x_3}, W_{x_3x_4}, \dots W_{x_{n-1}x_n})$.

3.3. Combining Operation

The combining operation is applied to merge the various trust perceptions by combining the evidence from diverse perspectives. The trust fusion can be evolved in the parallel topology, as illustrated in Figure 3.2.

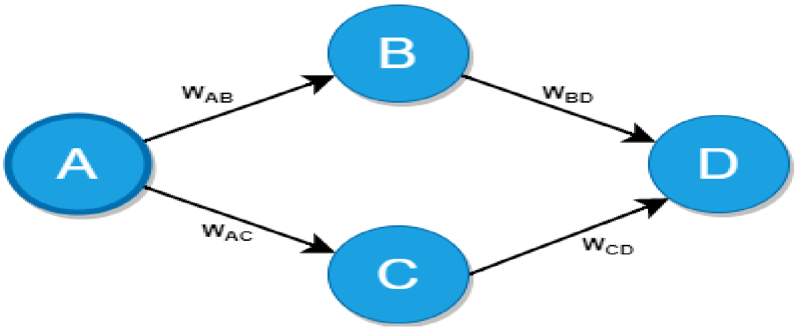


Figure 3.2 Parallel topologies for trust fusion

Figure 3.2 depicts the players as nodes, their communication as edges and the trust evidence as weights in MMOG. Let determine the degree of trust from A $to\ D$ by assessing the opinions of the different sources. In this case, $W_{AD} = \Delta(W_{AB}, W_{BD}) =< b_i, d_i, n_i, e_i >$ and $W_{AD} = \Delta(W_{AC}, W_{CD}) =< b_j, d_j, n_j, e_j >$ are employed to represent the trustworthiness from A's perspective to D.

$$\begin{cases} b_{ij} = \dfrac{e_j b_i + e_i b_j}{(e_i + e_j - e_i e_j)} \\ d_{ij} = \dfrac{e_j d_i + e_i d_j}{(e_i + e_j - e_i e_j)} \\ n_{ij} = \dfrac{e_j n_i + e_i n_j}{(e_i + e_j - e_i e_j)} \\ e_{ij} = \dfrac{e_i e_j}{(e_i + e_j - e_i e_j)} \end{cases} \qquad (3.8)$$

Thus, Eq. (3.8) produces the trust opinion from $A\ to\ D$ by combining the different opinions.

Terminology 2 (Combining Operation) *concerning the trustworthiness of the parallel paths from A to D as* $W_{A_1D_1} =< b_i, d_i, n_i, e_i >$ *and* $W_{A_2D_2} =< b_j, d_j, n_j, e_j >$ *then the combining operation is accomplished as* $W_{AD} = \Theta(W_{A_1D_1}, W_{A_2D_2})$.

$$W_{AD} = \Theta\left(W_{A_1D_1}, W_{A_2D_2}\right) =< b_{AD}, d_{AD}, n_{AD}, e_{AD} > \qquad (3.9)$$

Where $< b_{AD}, d_{AD}, n_{AD}, e_{AD} >$ evidence is obtained from Eq. (3.8), and Θ denotes the combining operation. Although, the combining operation acquires the following properties, which are essential to comprehend it.

Corollary 3.3 Associative property *concerning the trustworthiness of three independent evidence* $W_{A_iB_i}, W_{A_jB_j}\ and\ W_{A_kB_k}$ *then* $\Theta\left(W_{A_iB_i}\Theta\left(W_{A_jB_j}, W_{A_kB_k}\right)\right) \equiv \Theta\left(\Theta\left(W_{A_iB_i}, W_{A_jB_j}\right), W_{A_kB_k}\right)$

Corollary 3.4 Commutative property: *concerning the trustworthiness of two independent evidence* $W_{A_iB_i} and\ W_{A_jB_j}$ *then* $\Theta\left(W_{A_iB_i}, W_{A_jB_j}\right) \equiv \Theta\left(W_{A_jB_j}, W_{A_iB_i}\right)$

Proof: According to Eq. (3.8), the results are equal in the associative and commutative properties.

Therefore, according to parallel topology, the trust opinions are $W_{x_1y_1}, W_{x_2y_2}, W_{x_3y_3}, \dots W_{x_{n-1}y_{n-1},} W_{x_ny_n}$.Then, the combining operation computes the results as $\Theta(\Theta(\Theta(W_{x_1y_1}, W_{x_2y_2}), W_{x_3y_3}), \dots W_{x_ny_n})$. According to commutative and associative property, it is streamlined as $\Theta(W_{x_1y_1}, W_{x_2y_2}, W_{x_3y_3}, \dots W_{x_ny_n})$.

3.4. Expected Belief

The trust between two players is computed by leveraging the discounting and combining operations and resulting in four states opinions. However, a single number rather than a vector is recommended to represent the trust. Therefore, the expected belief opinion is computed using Eq. (3.6).

3.5. Design of Network Structure

The trust is evaluated by designing an arbitrary network with the I-3VSL model in MMOG. Among the challenges associated with the arbitrary network is implementing discounting and combing operations on serial-parallel topologies. With the massive size of the MMOG network, one-many interactions are essential. Thus, it is necessary to evaluate the performance with non-serial-parallel topologies. As a result, the problem with serial-parallel topology with trust propagation is distinguished by distorting and original opinion. For instance, consider Figure 3.3, the trust evidence from player A to B and B to C is propagated to produce the trust opinion from A to C. In this instance, trust evidence A to B is referred to be distortion. In contrast, trust evidence from B to C is referred to as original opinion that is established via trust fusion.

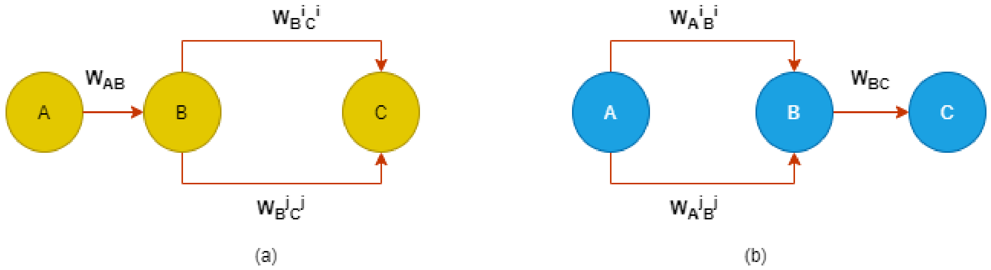


Figure 3.3 Distinguishing the distortion and original opinion

With the help of Figure 3.3, the distortion and original opinion using I-3VSL trust computation are expressed many times, but the actual evidence is represented only once.

Corollary 3.5 *concerning the trustworthiness of two independent opinions of parallel paths from B to C as* $W_{B^iC^i} =< b_{B^iC^i}, d_{B^iC^i}, n_{B^iC^i}, e_{B^iC^i} >$ *and* $W_{B^jC^j} =< b_{B^jC^j}, d_{B^jC^j}, n_{B^jC^j}, e_{B^jC^j} >$ *and the trustworthiness opinion from A to B as* $W_{AB} =< b_{AB}, d_{AB}, n_{AB}, e_{AB} >$*. Then the discounting and combining operations as* $\Theta\left(\Delta\left(W_{AB}, W_{B^iC^i}\right), \Delta\left(W_{AB}, W_{B^jC^j}\right)\right) \equiv \Delta(W_{AB}, \Theta(W_{B^iC^i}, W_{B^jC^j}))$

Proof: Let's assume trust opinions as W_{AB}=<0.78, 0.12, 0, 0.1>, $W_{B^iC^i}$=<0.31, 0.59, 0, 0.1> and $W_{B^jC^j}$=<0.67, 0.23, 0, 0.1>. Then apply the discounting and combining operations to the left side as $\Theta\left(\Delta\left(W_{AB}, W_{B^iC^i}\right), \Delta\left(W_{AB}, W_{B^jC^j}\right)\right)$. Therefore, the results are generated using Eq. (3.5) and (3.6).

$$W_{AC^i} = \Delta\left(W_{AB}, W_{B^iC^i}\right) =< 0.25, 0.48, .29, 0.1 > \qquad (3.10)$$

$$W_{AC^j} = \Delta\left(W_{AB}, W_{B^jC^j}\right) =< 0.55, 0.19, .29, 0.1 > \qquad (3.11)$$

Then apply the Eq. (3.8) that produces the result as

$$\Theta\left(\Delta\left(W_{AB}, W_{B^iC^i}\right), \Delta\left(W_{AB}, W_{B^jC^j}\right)\right) = \Theta\left(W_{AC^i}, W_{AC^j}\right) \quad (3.12)$$

$$W_{AC} = \Theta\left(W_{AC^i}, W_{AC^j}\right) = < 0.42, 0.35, 0.30, 0.05 > \qquad (3.13)$$

Similarly, apply the combining and discounting operations to the right side as $\Delta(W_{AB}, \Theta(W_{B^iC^i}, W_{B^jC^j}))$. Therefore, the generated values by applying Eq. (3.8) are as follows

$$W_{BC} = \Theta\left(W_{B^iC^i}, W_{B^jC^j}\right) = < 0.51, 0.43, 0, 0.05 > \qquad (3.14)$$

Then apply the Eq. (3.5) and (3.6) that produces the results as

$$W_{AC} = \Delta(W_{AB}, W_{BC}) = < 0.42, 0.35, 0.30, 0.05 > \qquad (3.15)$$

According to obtained values of the Eq. (3.13) and (3.15) are equivalent, i.e. $\Theta\left(\Delta\left(W_{AB}, W_{B^iC^i}\right), \Delta\left(W_{AB}, W_{B^jC^j}\right)\right) \equiv \Delta(W_{AB}, \Theta(W_{B^iC^i}, W_{B^jC^j}))$.

Corollary 3.6 *concerning the trustworthiness of two independent opinions of parallel paths from A to B as* $W_{A^iB^i} =< b_{A^iB^i}, d_{A^iB^i}, n_{A^iB^i}, e_{A^iB^i} >$ *and* $W_{A^jB^j} =< b_{A^jB^j}, d_{A^jB^j}, n_{A^jB^j}, e_{A^jB^j} >$ *and the trustworthiness opinion from B to C as* $W_{BC} =< b_{BC}, d_{BC}, n_{BC}, e_{BC} >$*. Then the discounting and combining operations as* $\Theta\left(\Delta(W_{A^iB^i}, W_{BC}), \Delta(W_{A^jB^j}, W_{BC})\right) \equiv \Delta(\Theta(W_{A^iB^i}, W_{A^jB^j}), W_{BC})$

Proof: Let's assume trust opinions as $W_{A^iB^i}$=<0.78, 0.12, 0, 0.1>, $W_{A^jB^j}$=<0.31, 0.59, 0, 0.1> and W_{BC}=<0.67, 0.23, 0, 0.1>.Then, apply the discounting and combine operation on left side $\Theta\left(\Delta(\mathrm{W}_{\mathrm{A^iB^i}}, \mathrm{W}_{\mathrm{BC}}), \Delta(\mathrm{W}_{\mathrm{A^jB^j}}, \mathrm{W}_{\mathrm{BC}})\right)$. Therefore, the generated values apply Eq. (3.5) and (3.6).

$$\Delta(\mathrm{W}_{\mathrm{A^iB^i}}, \mathrm{W}_{\mathrm{BC}}) =< 0.55{,}0.19{,}0.296{,}0.1 > \qquad (3.16)$$

$$\Delta(\mathrm{W}_{\mathrm{A^jB^j}}, \mathrm{W}_{\mathrm{BC}}) =< 0.24{,}0.08{,}0.84{,}0.1 > \qquad (3.17)$$

Thereafter, perform the combining operation among Eq. (3.16) and (3.17) through Eq. (3.8).

$$W_{AC} = \Theta\left(\Delta(\mathrm{W}_{\mathrm{A^iB^i}}, \mathrm{W}_{\mathrm{BC}}), \Delta(\mathrm{W}_{\mathrm{A^jB^j}}, \mathrm{W}_{\mathrm{BC}})\right) =< 0.41{,}0.14{,}0.60{,}0 > \quad (3.18)$$

Similarly, apply the combining and discounting operations to the right side as $\Delta(\Theta(W_{A^iB^i}, W_{A^jB^j}), W_{BC})$. Therefore the generated values by applying Eq. (3.8)

$$W_{AB} = \Theta(W_{A^iB^i}, W_{A^jB^j}) =< 0.57{,}0.37{,}0{,}0.05 > \qquad (3.19)$$

Thereafter, apply the discounting operation in between $\Delta(W_{AB}, W_{BC})$ using Eq. (3.5) and (3.6)

$$W_{AC} = \Delta(W_{AB}, W_{BC}) =< 0.40{,}0.13{,}0.61{,}0.1 > \qquad (3.20)$$

According to obtained results of Eq. (3.18) and (3.20) are not equal, i.e. $\Theta\left(\Delta(W_{A^iB^i}, W_{BC}), \Delta(W_{A^jB^j}, W_{BC})\right) \neq \Delta(\Theta(W_{A^iB^i}, W_{A^jB^j}), W_{BC})$.

The associative property supports the I-3VSL operations but not the commutative property according to corollary 3.5 and 3.6. In contrast to that W_{AB} and W_{BC}, the W_{BC} is actual evidence and W_{AB} is distortion evidence. Hence, the actual evidence is combined only once, whereas the distorted evidence is multiple times in trust evaluation.

3.5.1.Arbitrary network topology

The I-3VSL operations: discounting and combing operations for an arbitrary network with serial-parallel topology problem is explained in the above section. Hence, a non-series-parallel arbitrary network is constructed as Figure 3.4 and examined I-3VSL operations.

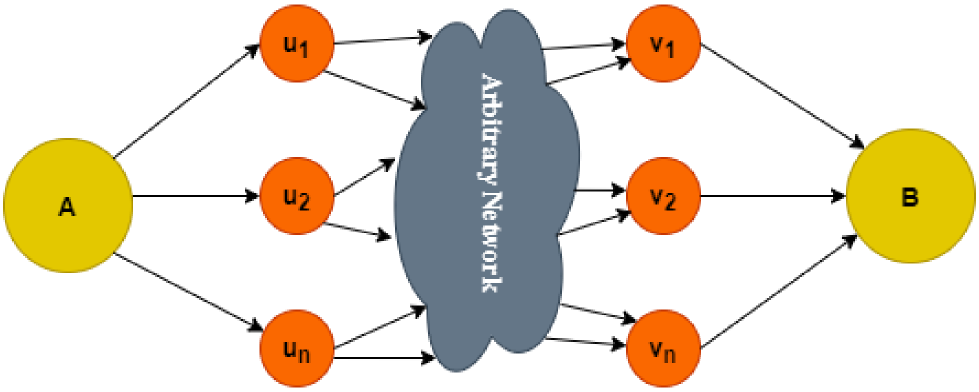


Figure 3.4 Arbitrary networks with non-series-parallel topology

The arbitrary network is represented as a directed graph *G= (V, E)* where source and destinations are denoted as A *and* B, as shown in Figure 3.4. The source node '*A*' is connected to n-nodes $(u_1, u_2, u_3 \dots u_n)$ and $(v_1, v_2, v_3 \dots v_n)$ are connected to target, i.e. $E\,(A, u_i)$ and $E\,(v_i, B)$. Therefore, the discounting and combining operations generate the trust evidence as W_{AB}. In this case, the problem is decomposed into subproblems until the base case is solvable and acquires a different solution.

Decomposition Rule:

1. The target node's in-degree is 1, then $W_{AB} = \Delta(W_{Au_1}, W_{u_1B})$
2. The target node's in-degree is > 1, then $W_{AB} = \Theta(\Delta(W_{Au_1}, W_{u_1B}), \Delta(W_{Au_2}, W_{u_2B}), \dots \Delta(W_{Au_n}, W_{u_nB}))$. Therefore, the corresponding sub-graph $G' = G - \sum E(v_i, B) - B$ is solvable and distinct to W_{Av_i}.

Hence, in each iteration, it generates the sub-graph that encompasses one edge from $A\ to\ a_n$, where $n \in [1, n]$. As a result, W_{Au_n} is obtained from actual graph G then apply the decomposition rule 1 and 2 repeatedly until it reaches the base case i.e. $|E| = 1\ and\ |V| = 2$

3.6. Design of TrustWalker (TW) Algorithm

The MMOG provides high scalability due to the number of players joining and leaving the network, creating one-to-many interactions. Therefore, to handle interactions effectively, the TW algorithm is designed. Primarily, the arbitrary network for the MMOG is established as a graph, i.e. $G = (V, E, W)$. In this graph, "G", the players represented as vertices "V", edges "E" denotes the interactions between the players, and "W" indicates the trust evidence of the interaction. Therefore, the "G" is represented as a trusted opinion matrix "M_O"which consist of the direct trust opinion of all the players with other players in the network denoted as W_{ij} illustrated as

$$\Omega_{ij}^{d} = \begin{cases} W_{ij} & The\ trust\ opinion\ from\ \text{i}\ to\ j \\ \cup & The\ uncertain\ trust\ opinion\ from\ i\ to\ j \end{cases} \qquad (3.21)$$

Where Ω_{ij}^{d} signifies the player "i" individual trust opinion with player "j". The W_{ij} represents the trust opinion between player *"i" to "j".* However, there is no interaction between *"i" to "j";* it is denoted as $\cup \triangleq < 0,0,0,1 >$. According to Eq. (3.21), the M_O illustrated with "n" players with trust opinions as

$$M_O = \begin{bmatrix} W_{11} & W_{12} & \cdots & W_{1n} \\ W_{21} & W_{22} & \cdots & W_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ W_{n1} & W_{n2} & \cdots & W_{nn} \end{bmatrix} \qquad (3.22)$$

From the M_O matrix, the specific players trust opinion vector is extracted as $''V''$ that consists of the column vector of $''n''$ opinions illustrated as

$$V^{d}{}_{i} = [\Omega_{i1}, \Omega_{i2} \dots \dots \dots \dots \Omega_{in}] \qquad (3.23)$$

Here d is a hop, and the specific player "i" is contacts all other players and their corresponding evidence as $\Omega^{d}{}_{ij}$. Further, the player "i" is an individual opinion on "j" is updated by applying the I-3VSL operations such as discounting and combining. However, the TW Algorithm follows the depth-limited BFS technique that updates the trust opinion in each iteration by travelling specific depth from trustor to trustee. The updated trust opinions are stored in ${V^d}_i$ as

$$V_i^d \ = (M_O)^T \odot V_i^{(d-1)} \qquad (3.24)$$

Here intuition of operator 'Θ' performs the matrix multiplication. In ordinary matrix multiplication, summation and multiplication operations are employed, whereas these operations are replaced with I-3VSL operations.

Terminology 3 (intuition of operator 'Θ') *concerning the trust opinion matrix and individual vector opinion are applied with Θ operator then the generated result as follows.*

$$\triangleq \begin{bmatrix} \Theta(\Delta(\Omega_{i1}^{(d-1)}, W_{11})) & \Theta(\Delta(\Omega_{i2}^{(d-1)}, W_{21})) & \cdots & \Theta(\Delta(\Omega_{in}^{(d-1)}, W_{n1})) \\ \Theta(\Delta(\Omega_{i1}^{(d-1)}, W_{12})) & \Theta(\Delta(\Omega_{i2}^{(d-1)}, W_{22})) & \cdots & \Theta(\Delta(\Omega_{i1}^{(d-1)}, W_{n2})) \\ \vdots & \vdots & \vdots & \vdots \\ \Theta(\Delta(\Omega_{i1}^{(d-1)}, W_{1n})) & \Theta(\Delta(\Omega_{i2}^{(d-1)}, W_{2n})) & \cdots & \Theta(\Delta(\Omega_{i1}^{(d-1)}, W_{nn})) \end{bmatrix}$$

$$\triangleq \begin{bmatrix} \Omega_{i1}^d & \Omega_{i2}^d & \cdots & \Omega_{ij}^d & \Omega_{in}^d \end{bmatrix} \qquad (3.25)$$

Correspondingly, the M_O is fabricated leveraging direct trust opinions, and the pseudo-code is as follows.

Algorithm 1: The $M_O$generation

Input: Digraph $G$and set of nodes S

Output: Opinion Matrix M_O

Goal: Generating M_O for Algorithm 2

Opinion_Matrix (G, S)

```
for $x$ ←1 to r do
    for y← 1 $to\ c\ do$
        if $x == y$ then
            $M_O[x][y] = \ I$
        else if   $edge(x, y) \in \ E$
            $OM[x][y] = W_{xy}$
        else
            $OM[x][y]$ =∪
```

```
9.          end if
10.       end for loop
11.   end for loop
```

Algorithm 1 describes the opinion matrix initialization from player "x" to all other players in the network. Hence, $n \times n$ matrix is created. Line 1 to 9 expresses the trust opinion between the players. Line 3-4 indicates trust opinion is an absolute trust because the interaction is self-player. Line 4-9, if the players have the direct connection with another player, then represents the direct trust opinion value as w_{xy}, else an uncertain opinion.

With the help of Algorithm 1, the TW algorithm is designed by incorporating I-3VSL discounting and combining operations that find the path from the trustor to trustee's and assess the trustworthiness of the trustee from the trustor perspective.

Algorithm 2: TrustWalker

Input: A directed Graph G, from the players, i.e., trustee, trustor, depth as a number of hops

Output: Assessing the trust evidence from trustor to selected trustee

Goal: To find the path from source to destination based on trust opinions

TrustWalker (G, trustor, trustee, depth)

```
1.  $M_O$=Direct_ Trust (G, S), Initialize $V^{(1)}{}_x$ based on $M_O$
2.  Initialize the hop count $d \leftarrow 1$
3.  While $d < D\ do$
4.      $d \leftarrow d + 1$
5.      for all columns $C_y \in M_O$ where $y \neq x$ do
6.          $\Omega^{(d)}{}_{xy} \leftarrow \cup$
7.          for all direct opinion $W_{sy} \in C_y$ where $W_{sy} \neq \cup$
8.              $\Omega^{(d-1)}{}_{xs} \leftarrow V^{(d-1)}{}_x\ [s]$
9.              if $\Omega^{(d-1)}{}_{xs} \neq \cup$ then
10.                 if $\Omega^{(d)}{}_{xs} = \cup$ then
11.                     $\Omega^{d}{}_{xy} \leftarrow \Delta(\Omega^{(d)}{}_{xs}, w_{sy})$
```

```
12.                 else
13.                     if $E\ (w_{xs}) \leq\ (b_{xs})$ then
14.                         $\Omega^{d}{}_{xy} \leftarrow\ \Theta(\Omega^{d}{}_{xy}, \Delta(\Omega^{(d-1)}{}_{xs}, w_{sy})$
15.                     end if
16.                  end if
17.              end if
18.         end for loop
19.         $V^{d}{}_{x}\ [y]\ \leftarrow\ \Omega^{d}{}_{xy}$
20.     end for loop
21. end while loop
22. return $V^{d}{}_{x}$
```

Algorithm 2 depicts the TW algorithms pseudocode. Line 3 of the algorithm is employed to restrict the network searching depth. Line 5-19 leverages discount and combining operations of I-3VSL that revise the indirect trust assessment opinions. Line 6 represents the trust evidence of all network users' excluding the trustor node "x." Line 7-18 implements the trust fusion of all the derived evidence from $W_{sy} \neq \cup$. Line 8 acquires "x's" the indirect trust at $d-1$ hop neighbor "s." Line 9 to 11 verifies the trust opinion before performing the discount operation $\Delta(\Omega^{(d)}{}_{xs}, w_{sy})$ and updating the value $\Omega^{d}{}_{xy}$. Meanwhile, Line 13 determines if several opinions are accessible and then filters the recommendations depending on the predicted belief. If the nodes have a higher belief value, it is appropriate for the recommendation; otherwise, the transfer path is invalid. Line 14 aggregates all opinions to $\Omega^{d}{}_{xy}$ which is subsequently assigned to the individual opinion vector at Line 19. Finally, it incorporates the trustworthiness opinions of all other players with "x".

3.6.1.Analysis of time complexity

The time complexity of the TW algorithm described as the “for” loop from lines 7-18 is $n.c_1$ and lines from 5-20, another "for" loop is running then $n.(n.c_1 + c_2)$. The "while" loop runs based on the depth from lines 3-21, and the complexity becomes $d.n.(n.c_1 + c_2)$ where "d" is constant (number of hops). Therefore, the time complexity is $O(dn^2)$.

Further, the complexity of the "for" loop from lines 7-18 determines the in-degree of the trustee. The in-degree of the trustee ranges from 0 $to\ n$, where n indicates the maximum number of players in the network or virtual world. For instance, the in-degree of the trustee is one, then the complexity is determined by using Eq. (3.26).

$$T(n) = d.n.(c_1 + c_2) = O(n) \qquad (3.26)$$

Since the in-degree of the trustee node increases slowly because the number of players joins and leaves the game in real-time, then the trustees' in-degree is increasing to utmost "n". Thus the complexity is assessed through Eq. (3.27).

$$T(n) = d.n.(n.c_1 + c_2) = O(n^2) \qquad (3.27)$$

However, the TW algorithm leverages the iteration procedure. It offers a faster running time than the recursive approach because it mitigates the stack operations and applies even with the extensive network size.

3.7. Summary

This chapter describes the uncertainty trust assessment framework for trustworthy partner selection using I-3VSL. Further, the associative and commutative properties are evaluated using I-3VSL with discounting and combining operations. The distortion and original trust opinions are distinguished with the mathematical proof. Moreover, a non-series parallel network is designed, i.e. arbitrary network. Subsequently, the trustworthiness of all the trustees is computed based on the trustors' perspective by creating the M_O and TW Algorithm. Later, the time complexity of The TW algorithm is analyzed based on the in-degree of the trustee node. Therefore, the TW provides the optimized time complexity compared to AT, i.e. $O(n^2)$ where in-degree is > 1; else, it is $O(n)$.

CHAPTER 4

PROPOSED FRAMEWORK FOR ROBUST WATERMARKING SCHEME

This chapter presents a content protection technique for Anaglyph 3D images in the transform domain that relies on the images' frequency. The transform domain inserts the content owner's secret message into the frequency of the host image. The host image is represented in the spatial domain transformed into DWT's frequency domain. The DWT divides the image into frequency sub-bands and then selects the appropriate sub-band for the embedding to enhance the watermark robustness. However, the DWT is sensitive to the geometric attacks that can mitigate through using decomposition strategies. As a result, SVD and HD are leveraged. However, the embedded process depends entirely on the embedding strength factor that differs between images; thus, PSO determines the embedded strength factor. Therefore, the experiment is carried out for variable watermark sizes under different attacks and evaluation details are provided.

4.1. 3D Anaglyph Image

At present, academicians primarily concentrate on a subset of 3D images termed stereograms. The stereograms are depth perceptions derived from 2D images viewed using thin mobile devices. The most prevalent type of stereogram is 3D Anaglyph images formed by leveraging separate color filters for each eye's perspective, such as red-cyan 3D Anaglyph images, as illustrated in Figure 4.1. Thus, the two stereo images are obtained from slightly different angles to generate the 3D Anaglyph image. Then, extract the color channels from each eye's left and right images, merge them to form a single image as a red-cyan Anaglyph 3D image. These images are viewed through red-cyan Anaglyph glasses.

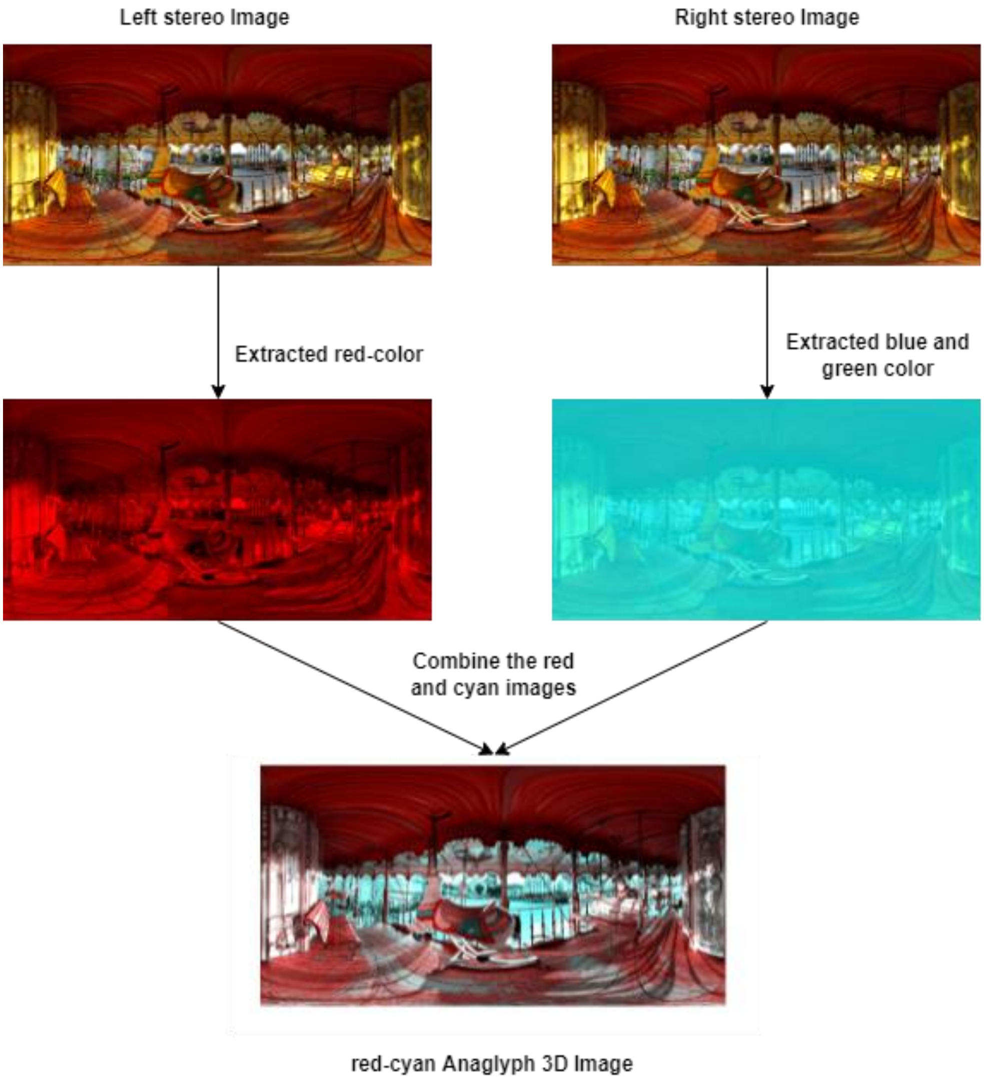

Left stereo Image
Right stereo Image
Extracted red-color
Extracted blue and green color
Combine the red and cyan images
red-cyan Anaglyph 3D Image

Figure 4.1 Red-cyan Anaglyph 3D image construction

Similarly, Anaglyph 3D images are also classified as true, color, mono, optimized-color and half-color. The numerous varieties of Anaglyph 3D images are created by extracting RGB color values from the left and right stereo views and combining them to obtain such images. For instance, the true color Anaglyph image is constructed using Eq. (4.1).

$$\begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} R_L \\ G_L \\ B_L \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0.299 & 0.587 & 0.114 \end{bmatrix} \begin{bmatrix} R_R \\ G_R \\ B_R \end{bmatrix} \qquad (4.1)$$

Although, the Anaglyph 3D visuals have recently witnessed a rejuvenation primarily to the exhibition of images and movies through the internet, portable devices and blue-ray discs. These images and videos are viewed through inexpensive plastic glasses with realistic color filters for all three primary colors. Therefore, the red-cyan color images are used in a variety of applications such as Mars Rover images and STEREO solar research that employs two orbiting spacecraft to acquire 3D sun images, geological surveys, museum artefacts and virtual online games. Further, recent healthcare applications, such as 3D ultrasonic heart images, are created through red-cyan Anaglyph images. The most significant benefit of Anaglyph technology is comfortable with both modern and old vintage Cathode Ray Tubes (CRT)[144].

Conversely, like 2D images, Anaglyph 3D images are also effortlessly replicated and disseminated without compromising the quality. Thus, this illegitimate activity violates the content ownership rights and results in monetary losses for the industry. As a result, a robust content protection scheme is essential for Anaglyph 3D images. Hence, a robust watermarking scheme for Anaglyph 3D image is presented in the subsequent section.

4.2. Theoretical Framework

This section outlines the mathematical concepts employed in the proposed watermarking scheme.

4.2.1.3D Discrete wavelet transformation

The 3D DWT is an extension of the 2D DWT, and the 3D DWT decomposes the 2D wavelet in the z-direction, resulting in the 3D wavelet decomposition sub-bands. The specifications of 2D wavelet decomposition are described in chapter 2. Figure 4.2 shows the 3D decomposition process [145].

According to Figure 4.2, level-1 2D-DWT decomposition has four sub-bands: LL, LH, HL, and HH. These sub-bands are further decomposed in the Z-direction using Eq. (4.2) and (4.3).

$$CI^{(x,y,z)} = (L^x \oplus H^x) \otimes (L^y \oplus H^y) \otimes (L^z \oplus H^z) \tag{4.2}$$

$$\begin{aligned} CI^{(x,y,z)} = {} & L^xL^yL^z \oplus L^xL^yH^z \oplus L^xH^yL^z \oplus L^xH^yH^z \oplus H^xL^yL^z \oplus H^xL^yH^z \\ & \oplus H^xH^yL^z \oplus H^xH^yH^z \end{aligned} \tag{4.3}$$

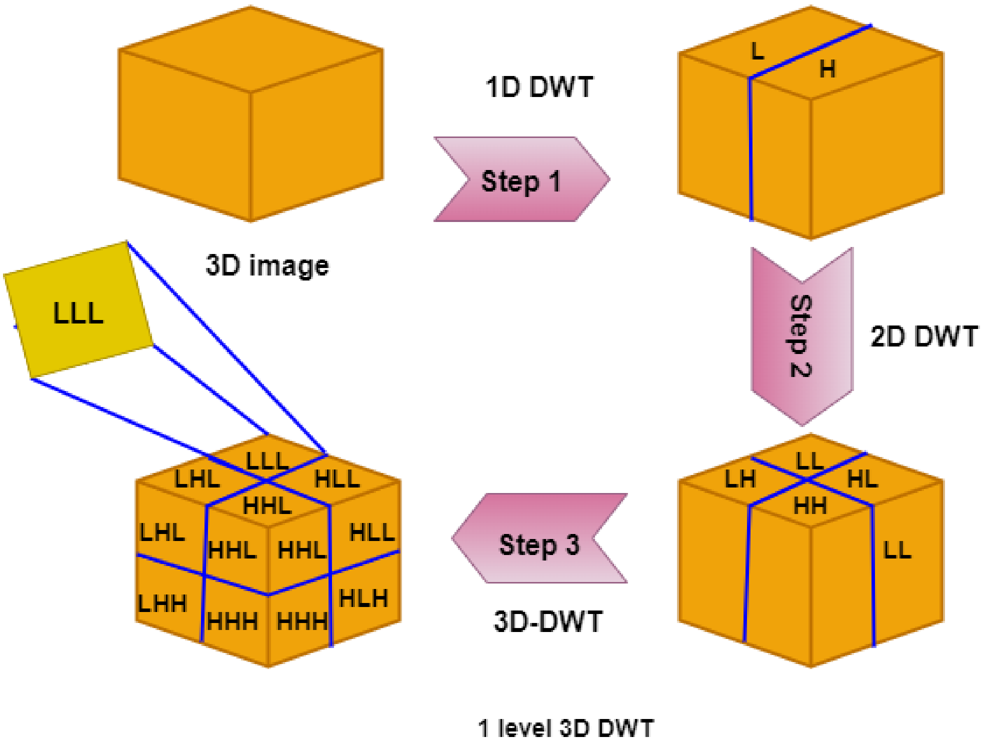


Figure 4.2 Level-1 decomposition flow of 3D DWT

Here, CI denotes the Anaglyph 3D image, $\oplus$ *and* $\otimes$ signifies the sum and product. Therefore, 1-level 3D-DWT generates the 8-subbands by applying low and high filters on the 2D image sub-bands such as LLL, LHL, LHH, LLH, HLL, HLH, HHL, and HHH. Then, Select a particular sub-band and apply 3D DWT for the next level decomposition, as illustrated in Figure 4.3.

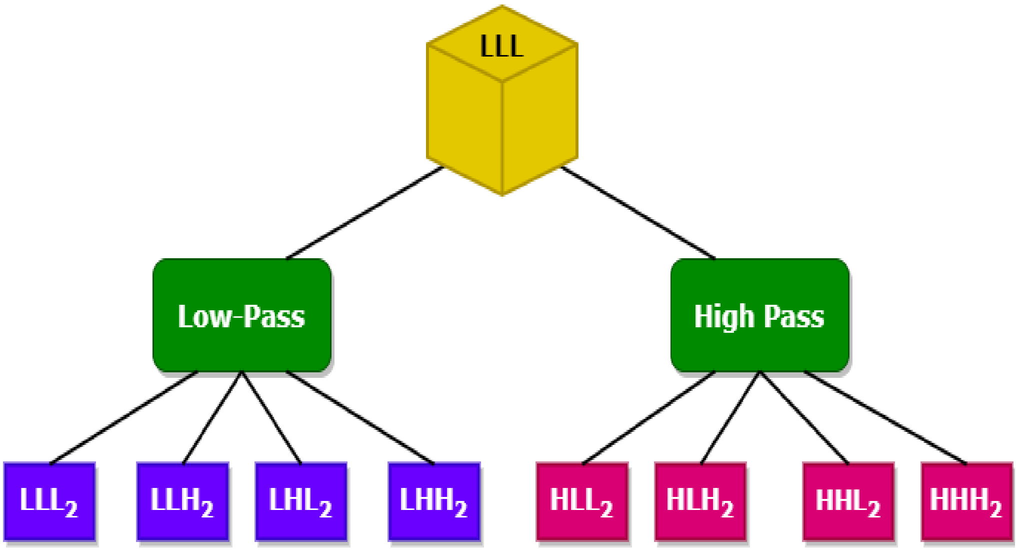


Figure 4.3 Level-2 3D DWT decomposition

Figure 4.3 represents the 2-level 3D DWT decomposition, and it consists of the 16 sub-bands. However, the 3D DWT essential elements are scaling and translation. Thus the scaling and wavelet translation functions are given in Eq. (4.4) and (4.5), respectively.

$$\phi_{i,p,q,r}(x,y,z) = 2^{i/2}\phi\left(2^{i}x - p, 2^{i}y - q, 2^{i}z - r\right) \qquad (4.4)$$

$$\psi^{j}_{i,p,q,r}(x,y,z) = 2^{i/2}\psi\left(2^{i}x - p, 2^{i}y - q, 2^{i}z - r\right) \qquad (4.5)$$

Here, p, q, r denotes the sizes of the 3D image, j denotes the direction, i denotes filters and (x, y, z) are coordinators. Therefore, the wavelet decomposition directions of each sub-band are represented through Eq. (4.6)

$$\begin{aligned} LLL &= \phi(x,y,z) = \phi(x)\phi(y)\phi(z) \\ LLH &= \psi(x,y,z) = \phi(x)\phi(y)\psi(z) \\ LHL &= \psi(x,y,z) = \phi(x)\psi(y)\phi(z) \\ LHH &= \psi(x,y,z) = \phi(x)\psi(y)\psi(z) \\ HLL &= \psi(x,y,z) = \psi(x)\phi(y)\phi(z) \\ HLH &= \psi(x,y,z) = \psi(x)\phi(y)\psi(z) \\ HHL &= \psi(x,y,z) = \psi(x)\psi(y)\phi(z) \\ HHH &= \psi(x,y,z) = \psi(x)\psi(y)\psi(z) \qquad (4.6) \end{aligned}$$

Therefore, Eq. (4.7) and (4.8) represent the discrete wavelet decomposition scaling and transition functions with size $p \times q \times r$.

$$W_{\phi}(i_0,p,q,r) = \frac{1}{\sqrt{pqr}}\sum_{x=0}^{p-1}\sum_{y=0}^{q-1}\sum_{z=0}^{r-1} C_I(x,y,z)\phi_{i_0,p,q,r}(x,y,z) \qquad (4.7)$$

$$W^{j}_{\psi}(i,p,q,r) = \frac{1}{\sqrt{pqr}}\sum_{x=0}^{p-1}\sum_{y=0}^{q-1}\sum_{z=0}^{r-1} C_I(x,y,z)\psi^{j}_{i,p,q,r}(x,y,z) \qquad (4.8)$$

From Eq. (4.7) and (4.8), the inverse DWT signal is generated for $C_{I(x,y,z)}$ in Eq. (4.9)

$$C_I(x,y,z)$$

$$= \frac{1}{\sqrt{pqr}}\sum_{p}\sum_{q}\sum_{r} W_{\phi}(i_0,p,q,r)\phi_{i_0,p,q,r}(x,y,z)$$

$$+\frac{1}{\sqrt{pqr}}\sum_{j=H,VD}\sum_{j=j\_0}^{\infty}\sum_{x=0}^{p-1}\sum_{y=0}^{q-1}\sum_{z=0}^{r-1} C_I(x,y,z)\psi^{j}_{i,p,q,r}(x,y,z) \qquad (4.9)$$

4.2.2. Hessenberg decomposition

The HD is a unique scaled or square matrix that divides the matrix "X" into unitary and Hessenberg matrices as represented in Eq. (4.10).

$$P\ H\ P^T = X \qquad (4.10)$$

Where P is an orthogonal matrix, H is Hessenberg upper triangular matrix and P^T is the conjugate transpose.

Terminology 1 (upper Hessenberg matrix) *A matrix "X" with* $n \times n$ *dimensions, then the upper Hessenberg matrix is represented as if* $X_{ij} = 0, \forall$ *i, j with* $i > j + 1$ *. However, the upper Hessenberg matrix is reduced with all the sub-diagonal entries with non-zero as if* $X_{i+1,i} \neq 0\ \forall i \in \{1,2,3 \ldots \ldots . n - 1\}$

Terminology 2 (lower Hessenberg matrix) *A matrix "X" with* $n \times n$ *dimensions, then the lower Hessenberg matrix is represented as if* $X_{ij} = 0, \forall$ *i, j with* $j > i + 1$ *. However, the upper Hessenberg matrix is reduced with all the super diagonal entries with non-zero as if* $X_{i,i+1} \neq 0\ \forall i \in \{1,2,3 \ldots \ldots . n - 1\}$

Generally, the HD estimates the householder matrix P, which is an orthogonal matrix using the Eq. (4.11)

$$P = \left(\frac{I_n}{\mu^T\mu}\right) - 2 \qquad (4.11)$$

Here $\mu\ and\ I_n$are R^n non-zero vector and identity matrix. Thus the HD is represented in Eq. (4.12)

$$H = (p_1, p_2 \ldots \ldots . p_{n-2})^T X (p_1, p_2 \ldots \ldots . p_{n-2}) \qquad (4.12)$$

$$H = \ P\ X\ P^T \qquad (4.13)$$

$$X = P\ H\ P^T \qquad (4.14)$$

Here P denotes the$(p_1, p_2 \ldots \ldots . p_{n-2})$.

4.2.3.Singular value decomposition

The SVD is a most potent decomposition technique that divides the real and complex matrix "X" into three decomposition matrices such as left orthogonal matrix (U), diagonal matrix (S) and right orthogonal matrix (V).

$$X = USV^T \tag{4.15}$$

Let "X" be an image with $p \times q$ size then $U\ and\ V$ orthogonal matrices are represented with $p \times p\ and\ q \times q$ sizes, S is a diagonal matrix with $p \times q$ size with non-negative singular values in decreasing order i.e. $s_1 \geq s_2 \ldots s_n$. Thus, the S diagonal as a matrix, $U\ and\ V$ are denoted as vectors in Eq. (4.16), Eq. (4.17) and Eq. (4.18).

$$S = \begin{bmatrix} S_1 & 0 & 0 & \ldots. & 0 \\ 0 & S_2 & 0 & \ldots. & 0 \\ 0 & 0 & S_3 & \ldots. & 0 \\ : & : & : & \ddots & : \\ 0 & 0 & \cdots & \cdots & S_q \end{bmatrix} \tag{4.16}$$

$$U = [u_1, u_2, \ldots \ldots .. u_p] \tag{4.17}$$

$$V = [v_1, v_2, \ldots \ldots .. v_q] \tag{4.18}$$

Conversely, the geometric interpretation of SVD is designed based on rotation and scaling. $U\ and\ V$ performs the rotation operation, and S performs the scaling process. Initially, V^T performs the rotation according to the axes, then S performs the scaling operation by stretching in the direction of the axes to form the eclipse shape. The final position is arranged by the rotation operation by U, as illustrated in Eq. (4.19).

$$Xv_j = S_j u_j \tag{4.19}$$

Here $X$is an image, which is rotated by v_j in the direction of "j" and S_j is scaling factor then rotated by u_j in the "j" direction.

4.2.4.Particle swarm optimization

The PSO provides the optimized solution established on the size of the population. The PSO works on the principle of movement and behavior of birds' demonstrate a significant social behavior. Every bird has its optimal solution and determines the optimum global position in this process. Therefore, the watermarking scheme incorporates this behavior while selecting the embedded strength factor. The PSO optimization problem is designed with various parameters such as population size, fitness function, termination criteria and other variables. Initially, the population is initialized using random numbers, and the fitness function validates the optimal solution in each iteration. Thus, it provides the global best solution based on the present population and updates accordingly all the solutions. However, the growth in the population size produces a new set of solutions that are compared with the existing solution; if the new solution is better, it replaces the current solution.

The PSO algorithm for the watermarking scheme is determined by initializing the population size as "m" and the *ith* particle best solution (Pb_i) is determined in search space, i.e. *(Pb1, Pb2 ... PbD)* and the global best position (G_{best}) is distinguished from all the particles best solution, i.e. Pb_i. Therefore, the *ith* particle velocity and position are determined using Eq. (4.20) and (4.21), respectively.

$$V_{i+1}^{m} = I_W * V_i^m + c_1 * r_1 * (Pb_i - X_i^m) + c_2 * r_2 * (G_{best} - X_i^m) \tag{4.20}$$

$$X_{i+1} = X_i + V_{i+1} \tag{4.21}$$

Here c_1, c_2 denotes the acceleration parameters, r_1, r_2 signifies the random numbers that are standardized to [0, 1] and I_W is inertia weight that controls the speed of the particles.

4.3. Proposed Watermarking Scheme

A robust watermarking scheme is presented to protect the Anaglyph 3D images from geometric attacks. The host and watermark logos are Anaglyph 3D color images, extract the blue channels from both the images named as $C_I^b\, and\, W_I^b$. The decomposition level (R) is computed using $C_I^b\, and\, W_I^b$ sizes. On C_I^b, the decomposition is performed using 3D DWT with Haar transformation. Further, the Lower level sub-band is selected and applies HD decomposition. The upper Hessenberg matrix (H) and W_I^b are selected and applies the SVD decomposition. The embedding process is carried out by choosing the singular diagonal values and embedding the strength factor. The PSO algorithm is employed to determine the embedding factor. Further, apply the inverse SVD and DWT to construct the watermark image. The watermark image is then combined with the host images remaining channels. The functional block diagram for the proposed watermark scheme is illustrated in Figures 4.4 and 4.5.

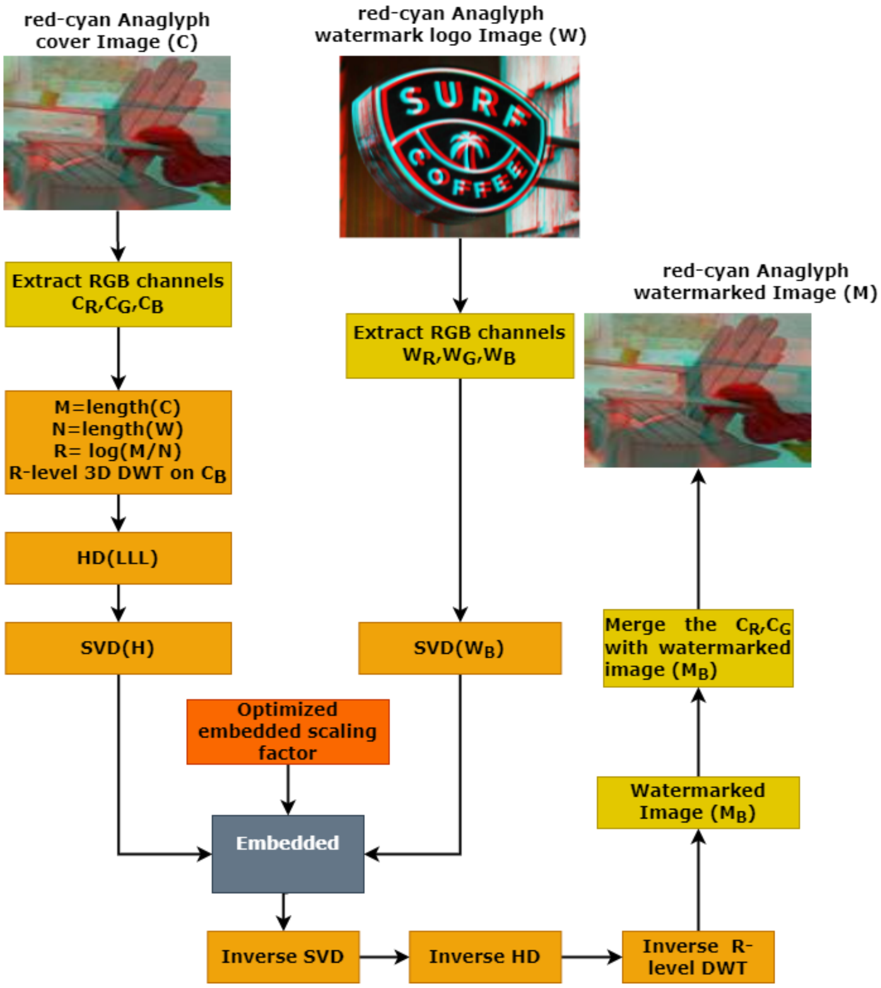

red-cyan Anaglyph cover Image (C)
red-cyan Anaglyph watermark logo Image (W)
red-cyan Anaglyph watermarked Image (M)
Extract RGB channels C_R,C_G,C_B
Extract RGB channels W_R,W_G,W_B
M=length(C)
N=length(W)
R= log(M/N)
R-level 3D DWT on C_B
HD(LLL)
SVD(H)
SVD(W_B)
Merge the C_R,C_G with watermarked image (M_B)
Optimized embedded scaling factor
Watermarked Image (M_B)
Embedded
Inverse SVD
Inverse HD
Inverse R-level DWT

Figure 4.4 Functional flow of watermark embedding

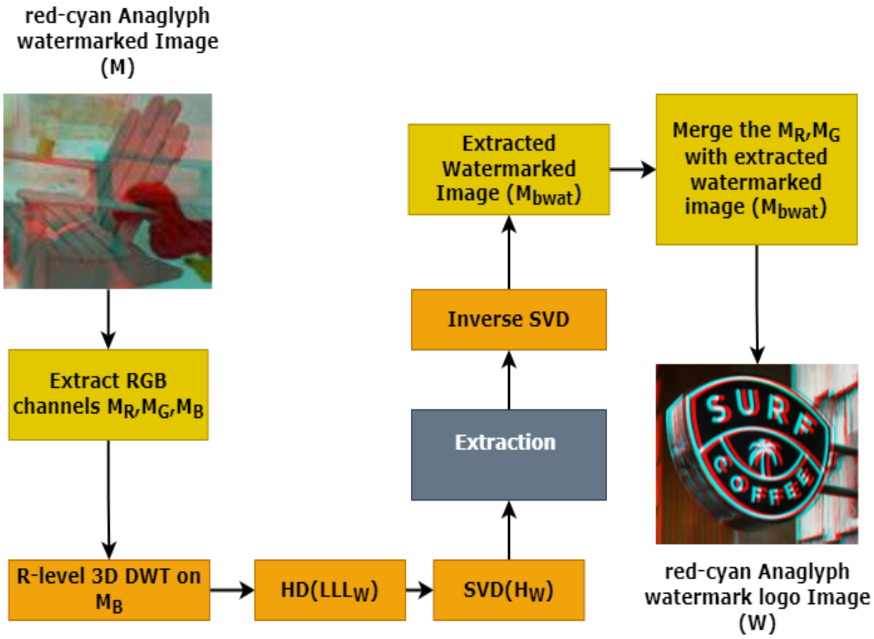

red-cyan Anaglyph watermarked Image (M)
Extracted Watermarked Image (M_{bwat})
Merge the M_R,M_G with extracted watermarked image (M_{bwat})
Inverse SVD
Extract RGB channels M_R,M_G,M_B
Extraction
red-cyan Anaglyph watermark logo Image (W)
R-level 3D DWT on M_B
HD(LLL_W)
SVD(H_W)

Figure 4.5 Function flow of watermark extraction

4.3.1.Watermarking embedded procedure

The proposed watermark embedded algorithm is divided into preprocessing, watermark embedding and post-processing.

Input: the cover image ($\boldsymbol{C_I}$) and watermark logo ($\boldsymbol{W_I}$)

Output: watermarked image ($\boldsymbol{M_I^{RGB}}$)

Goal: performing the embedded process for variable sizes of watermarks

Algorithm 1: Watermarking embedded ($\boldsymbol{C_I}$,$\boldsymbol{W_I}$)

Pre-processing

1. Extract the color channels from C_I and W_I such as C_I^R, C_I^G, C_I^B and W_I^R, W_I^G, W_I^B.
2. Select the $\boldsymbol{C_I}$'s the blue channel (C_I^B)
3. Compute the decomposition level (R) based on the sizes of C_I and W_I. $\mathrm{R} = \log_2 (M/N)$Where M=length ($C_I$) and N= length ($W_I$).
4. Apply the R-level DWT with Haar transformation on C_I^B that produces eight sub-bands
$$[\mathrm{LLL, LHL, LHH, LLH, HLL, HLH, HHL, HHH}] = dwt(C_I^B, "haar")$$
5. Apply the HD decomposition on the LLL sub-band
$$[P, H] = HD(LLL)$$
6. Apply the SVD decomposition on H and W_I^B
$$[U_{CI}, S_{CI}, V_{CI}] = SVD(H)$$
$$[U_{WI}, S_{WI}, V_{WI}] = SVD(W_I^B)$$

Embedding

7. Perform the embedding process by selecting the diagonal matrices of SVD
$$C_W = S_{CI} + \alpha * S_{WI}$$

Post-processing

8. Apply the inverse SVD and HD
$$C_{wat} = U_{CI} * C_W * V'_{CI}$$
$$LLL_{wat} = P * C_{wat} * P'$$

9. Apply the inverse R-level DWT on LLL_{wat}.It results in the watermarked image.

$$Watermarked = idwt(LLL_{wat}, LHL, LHH, LLH, HLL, HLH, HHL, HHH)$$

10. Combine the remaining channels such as $C_I^R, and\ C_I^G$ with watermarked resulting in the RGB watermarked image (M_I^{RGB}).

4.3.2.Watermarking extraction procedure

The proposed watermark extraction algorithm is divided into preprocessing, watermark extraction and post-processing.

Input: the watermarked cover image ($\boldsymbol{M_I^{RGB}}$)

Output: extracted watermark image ($\boldsymbol{M_I^{ext}}$)

Goal: Perform the extraction process on the watermarked image of variable sizes.

Algorithm 2: Watermarking extraction (M_I^{RGB})

Preprocess

1. Color channels (R, G, B) are extracted from M_I^{RGB} named as M_I^R, M_I^G, M_I^B
2. Select the M_I^B and apply the R-level DWT on it.

$$[LLL_w, LHL_w, LHH_w, LLH_w, HLL_w, HLH_w, HHL_w, HHH_w] = dwt(M_I^B)$$

3. Apply the HD decomposition on LLL_W

$$[P_W H_W] = HD(LLL_w)$$

4. Perform the SVD decomposition on H_W

$$[U_{wat}, S_{wat}, V_{wat}] = SVD(H_W)$$

Extraction

5. Perform the extraction in between $S_{wat} and\ S_{WI}$, the result is divisible by α

$$S_{bwat} = \frac{S_{wat} - S_{WI}}{\alpha}$$

Post-process

6. Apply the inverse SVD using $U_{WI}, S_{bwat} and\, V_{WI}$ resulting in the extracted watermark(M_I^{bext})

$$M_I^{bext} = U_{WI} * S_{bwat} * V_{WI}'$$

7. The extracted watermark M_I^{bext} is merged with M_I^R, M_I^G, resulting in the RGB-extracted watermark (M_I^{ext})

4.3.3 Optimization of scaling factor using PSO

The scaling factor plays a vital role in the watermarking scheme since it determines the robustness and imperceptibility. A slight improvement in the scaling factor enhances the effectiveness of the watermarked images despite having an impact on the extracted watermarked image. On the other hand, a high scaling factor provides significant robustness and moderate imperceptibility. Therefore, the scaling element leveraged must balance imperceptibility and robustness. However, the scaling factor value is determined manually by the existing watermarking schemes for Anaglyph 3D images. The scaling value varies depending on the image to provide the best robustness and imperceptibility. Therefore, determining the appropriate scaling factor can resolve the conflict between robustness and imperceptibility accomplished through optimization techniques. Thus, the proposed watermarking scheme employs the PSO to determine the scaling factor automatically to embed the watermark in the cover images SVD decomposition. The proposed optimization approach is based on the single objective PSO that computes the scaling factor. The scaling factor value is evaluated by employing the different attacks in each iteration to identify the optimum scaling factor. The flow of the optimal scaling factor is depicted in Figure 4.6.

According to Figure 4.6, the optimization strategy begins by randomly initializing the parameters such as velocity and position of all the particles, and the particles constantly move inside search space. The watermark scheme robustness and imperceptibility is assessed through the fitness function as Eq. (4.22)

$$f = \frac{n}{(\sum_{j=1}^{n} NCC_i + PSNR)} \qquad (4.22)$$

Here f represents the fitness function, and n indicates the number of various operations performed on the watermarked image throughout the optimization. NCC_i is used to assess the robustness under different attacks, while PSNR quantifies the watermark scheme's imperceptibility. Thus, to experiment, PSO uses various initial parameters listed in Table 4.1.

Table 4.1 Initial parameter for PSO optimization

Parameter	Value
Acceleration values (c_1, c_2)	2
Inertia weight (I_W)	0.8
Number of iterations	100
Population Size (m)	50

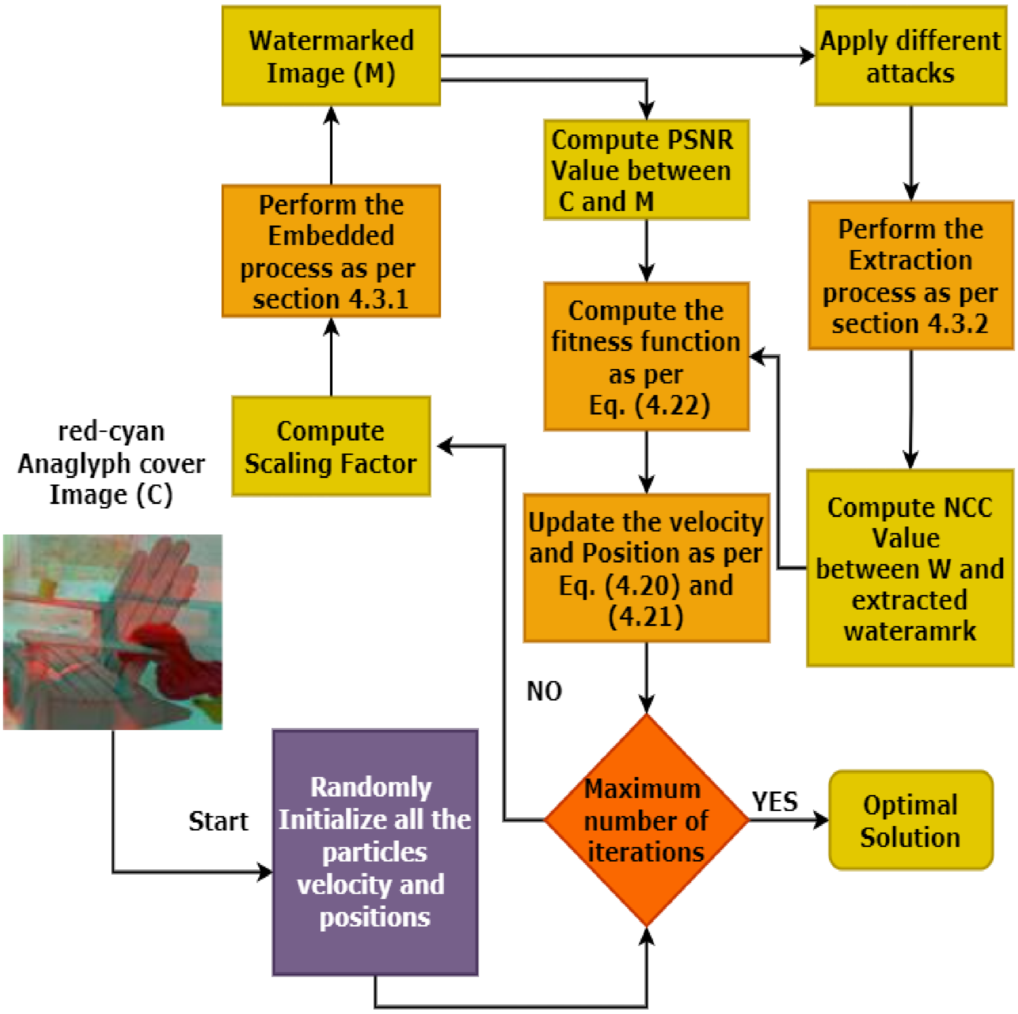

Watermarked Image (M)
Apply different attacks
Compute PSNR Value between C and M
Perform the Embedded process as per section 4.3.1
Perform the Extraction process as per section 4.3.2
Compute the fitness function as per Eq. (4.22)
red-cyan Anaglyph cover Image (C)
Compute Scaling Factor
Update the velocity and Position as per Eq. (4.20) and (4.21)
Compute NCC Value between W and extracted wateramrk
NO
Start
Randomly Initialize all the particles velocity and positions
Maximum number of iterations
YES
Optimal Solution

Figure 4.6 Flow of the optimization of scaling factor

4.4. Summary

This chapter describes the proposed framework for the robust watermarking scheme for the red-cyan and other forms of Anaglyph 3D images content protection. Initially, it provides information about Anaglyph 3D image generation. The theoretical framework's comprehension includes DWT, HD, SVD and PSO. Further, it presents the proposed framework of robust watermarking scheme operations such as watermarking embedding and extraction procedure is exemplified. Moreover, it provides the optimal scaling factor determination using the fitness function and its system.

CHAPTER 5
RESULTS AND DISCUSSIONS

This chapter provides the performance of the trustworthy partner selection and robust content protection scheme. The performance of the trustworthy partner selection is validated by conducting the simulation, and performance is assessed through MAE, RMSE, and accuracy. Further, the performance is compared with the existing approach. Similarly, the proposed watermarking scheme performance is validated through the MSE, PSNR, SSIM and NCC. Primarily, the PSO algorithm is leveraged to determine the optimized scaling factor under various geometric and non-geometric attacks. Thereafter, the robustness and imperceptibility are computed under various attacks for different sizes of watermark logos. The performance is examined over the existing approach.

5.1 Simulation Setup for Trust Assessment

The simulation environment is capable of replicating the wireless networks' VE circumstances. Thus, many simulators are available such as MATLAB, NS2 or NS3, Open Simulator, PeerfactSim, Socnetv, Networkx, etc. The networkx is an open-source python language for network analysis is used to conduct the simulation work [83], [146]. However, this package provides various graphs or network representations, including directed, self-loop, parallel and simple graphs. Also, many graph algorithms are created to quantify the clustering, degree distribution and shortest path. The networkx also enables the read, write and exchange of the several data formats used in many traditional graph models. Thus, the thesis leverages networkx with many prerequisites to validate the performance of both the proposed and existing approaches. A VE is established with 100 players, and these players are arranged in $1000 \times 1000\, m^2$ range. The MAC protocol of the IEEE 802.11 standards' is used, and the communication between the participants is formed within $5m$ range. Further, the graph interactions are divided into communities within the community (30%) and outside the community (2%). The graph layout is illustrated as a spring, and the random mobility model is leveraged to move the players'. After removing self-loops, the total number of interactions or edges between players is 1182. The simulation work is carried out with the initial setup, and the same settings are employed in the literature. The parameters details are depicted in Table 5.1

Table 5.1 Parameter for simulation

Parameter	**Value**
Name of the simulator	Network Analysis in Python
Network type	Wireless
MAC protocol	IEEE 802.11
Virtual world area	$1000 \times 1000 \text{ m}^2$
Number of nodes	100
Number of edges	1182
Communication range	5 m
Mobility model	Random model
Number of communities	3
Communication inside the community	30%
Communication outside the community	2%
Graph layout	Spring

5.1.1.Dataset

The MMOGs are graphical 2D or 3D video games that permit players to interact with other network gamers. As a result, the most popular MMOG games, such as World of Warcraft[147], Sony Ever Quest [148], [149], Travian [150], [151], and others are browser-based. The Travian dataset is selected since it is a real-time strategy game with over 5 million participants. The data was collected from 3x servers with a 3.5-month play cycle from multi-institutional virtual organizations. The game aims to establish villages and protect them against invasions from neighboring villages. The Travian network dataset comprises three datasets: trades, messages, and attacks. The attacks dataset is composed of individual player raids to take resources. The message dataset includes the player interactions and message exchanges between the participants, and the trades are multi-stakeholder trades [150]. In this study, the message network dataset demonstrates disassortative mixing, whereas the attack and trades represent non-assortative mixing. It indicates that the communication network is constructed based on players who send more messages and fewer messages. On the other hand, the interaction messages stream from one community to another.

5.1.2.Trusted network design

The trusted network is established through the message dataset, and it consists of the three attributes: the source, target, and timestamps. Trust relationships are found among the players using the source and target attributes that form the network. From the network, self-loops and isolated nodes are removed then the alias names are assigned to each player as ID. Further, the players are moving freely in the network, and the updated player's position information is distributed to all other players in the network. As a result, the use of network bandwidth is increasing. Hence, the network is sub-divided into small regions using community detection algorithms to minimize network bandwidth usage.

Nonetheless, several existing community detection schemes require prior knowledge, such as community density and duration. As a result, the players lack that specific knowledge. Hence, the asynchronous label propagation algorithm (LPA) is leveraged because of the linear time and no prior information about the community [152]. The LPA algorithm sub-divides the network into communities, with each community consisting of 40, 30, 30 nodes. The interaction between the players are established within the community is 30% and outside community 2%. Therefore, a community network is established and depicted in Figure 5.1.

As shown in Figure 5.1, the relations among the players with different communities are non-serial parallel connections. Therefore, based on the relationships between players, trust opinions are generated by leveraging the normal or Gaussian distribution function.

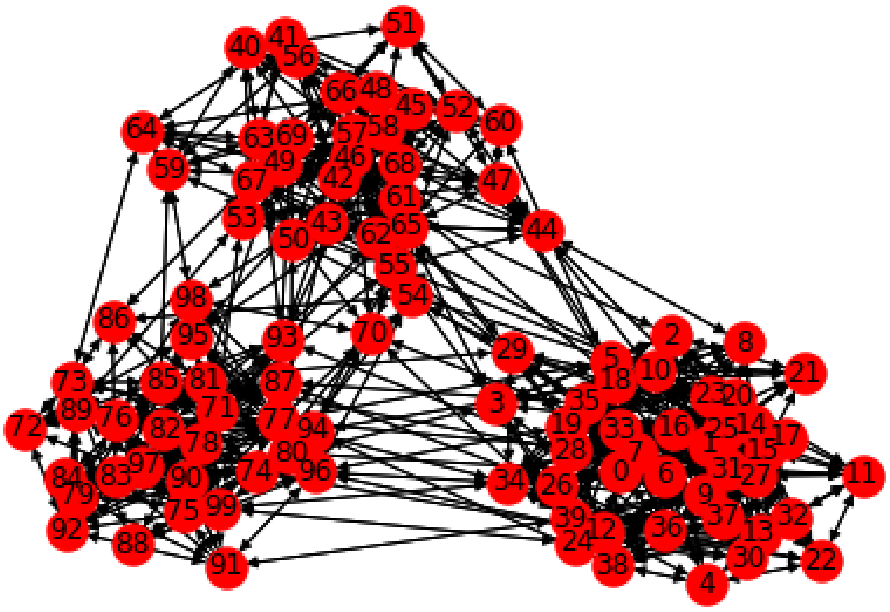


Figure 5.1 Sample trusted network

The Gaussian distribution function uses the mean and standard deviation as $\mu = 0.9, \sigma^2 = 0.1$. The trust opinions are standardized to [0,1], and the trust opinion is > 1 then recomputed the trust opinion of those nodes by modifying the $\mu = 0.3, and\ \sigma^2 = 0.0001$ respectively. Hence, the trusted network is created. However, the players move freely within the trusted network, changing the network topology. Accordingly, the players can change their positions by every 400 seconds.

5.1.3.Evaluation parameters

The proposed I-3VSL with TW is validated by comparing the existing framework 3VSL with AT using various parameters such as MAE, Accuracy and RMSE.

5.1.3.1 Computation of MAE

The MAE is computed by random selection of a trustor and its associated trustees. The trust of all the trustees' trust is assessed using I-3VSL with TW and their expected beliefs. Thus, the error is measured using Eq. (5.1).

$$MAE = \frac{\sum_{i=1}^{n} |T_{u,v} - E_{u,v}|}{N} \qquad (5.1)$$

5.1.3.2 Computation of RMSE

The RMSE is a non-linear assessment technique that quantifies the degree of the error by computing the difference between expected and actual trust opinion values is squared and then averaged over the sample. Then, it measures the average square root, as depicted in Eq. (5.2).

$$RMSE = \sqrt{\frac{\sum_{u,v}(T_{u,v} - E_{u,v})^2}{N}} \qquad (5.2)$$

In contrast, the MAE and RMSE are employed to analyze the error variance. Once the variance surpasses the disparity between them, it implies poor performance. If the RMSE matches MAE, they are of the same degree.

5.1.3.3 Accuracy

The accuracy is computed using the error rate. Both the error rate and accuracy are balanced. As a result, Eq. (5.3) is used to calculate the proposed and existing algorithms accuracy.

$$Accracy = 1 - Error\ rate \qquad (5.3)$$

5.1.4.Results and discussion

The proposed I-3VSL with TW framework performance is compared to the existing 3VSL with AT approach [60]. The performance of these approaches is determined by using MAE, RMSE and accuracy. The proposed method showed a significant improvement in all the evaluation parameters, and the results are explained as follows.

5.1.4.1 Evaluating MAE

The MAE is computed using Eq. (5.1), which assesses all the trustees' trust with trustor perspective using 3VSL and I-3VSL operations. Further, the trust path finds from trustor to trustee in-depth restricted BFS manner using TW and AT algorithms. Then, computes the trust between trustor to the trustee and expected belief using Eq. (3.5), (3.6) and (3.8). The results are depicted in Figure 5.2

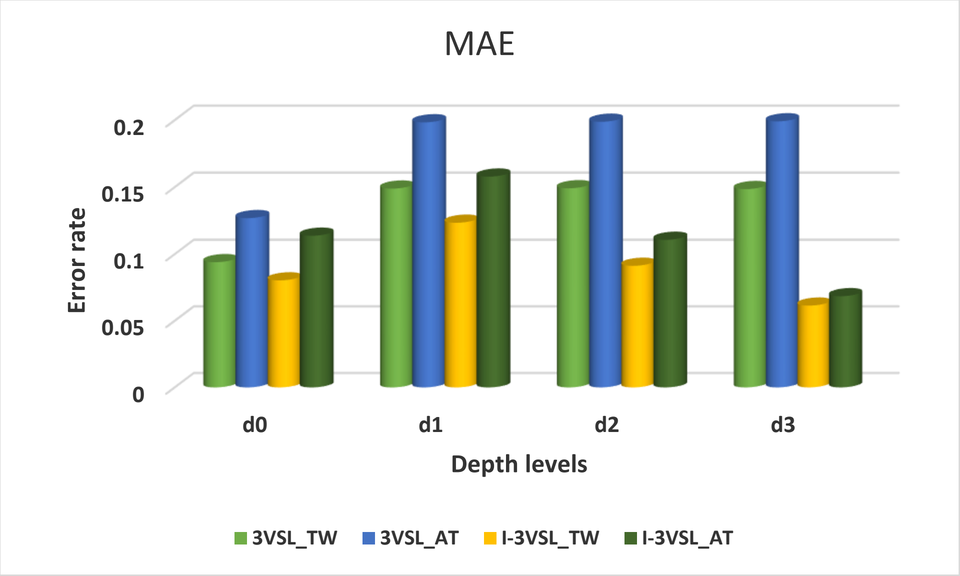


Figure 5.2 MAE optimization

According to Figure 5.2, the proposed algorithm minimizes the errors compared to 3VSL. The 5% error rate optimized with the I-3VSL_TW over 3VSL_TW, 7% error rate is optimized with I-3VSL_AT over 3VSL_AT, and 9% error rate is optimized with 3VSL_AT.

5.1.4.2 Evaluating the RMSE

The RMSE is computed through Eq. (5.2), and the results are depicted in Figure 5.3.

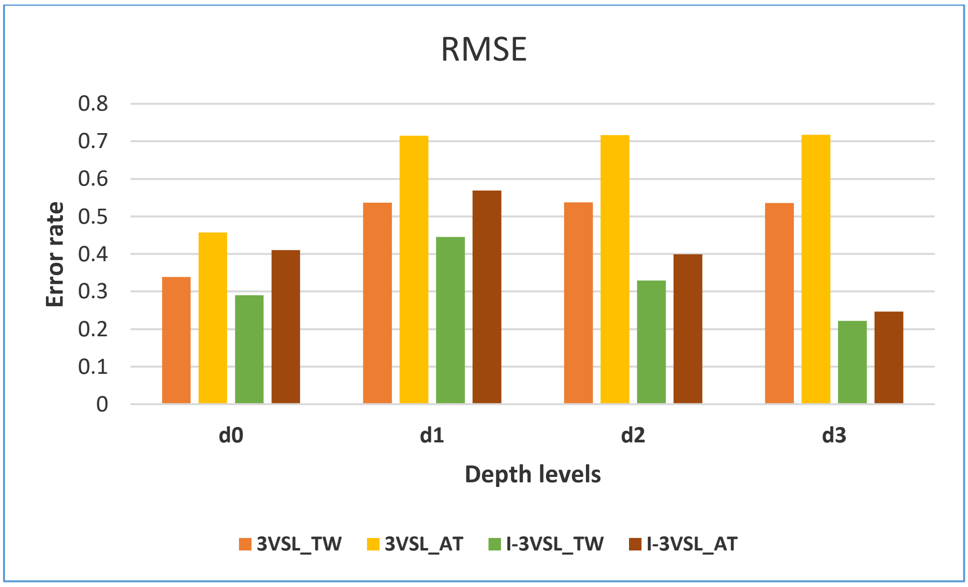


Figure 5.3RMSE optimization

According to Figure 5.3, the proposed algorithm minimizes the errors compared to 3VSL. The RMSE error is optimized 7% with I-3VSL_TW over 3VSL_TW. The 9% error rate is optimized with I-3VSL_AT over 3VSL_AT, and 5% is minimized with I-3VSL_TW over 3VSL_AT. Thus, the proposed approach provides the optimized error rate compared to all the combinations.

5.1.4.3 Evaluating the accuracy

The accuracy of the proposed and existing algorithms are assessed through Eq. (5.3), and the obtained results are depicted in Figure 5.4.

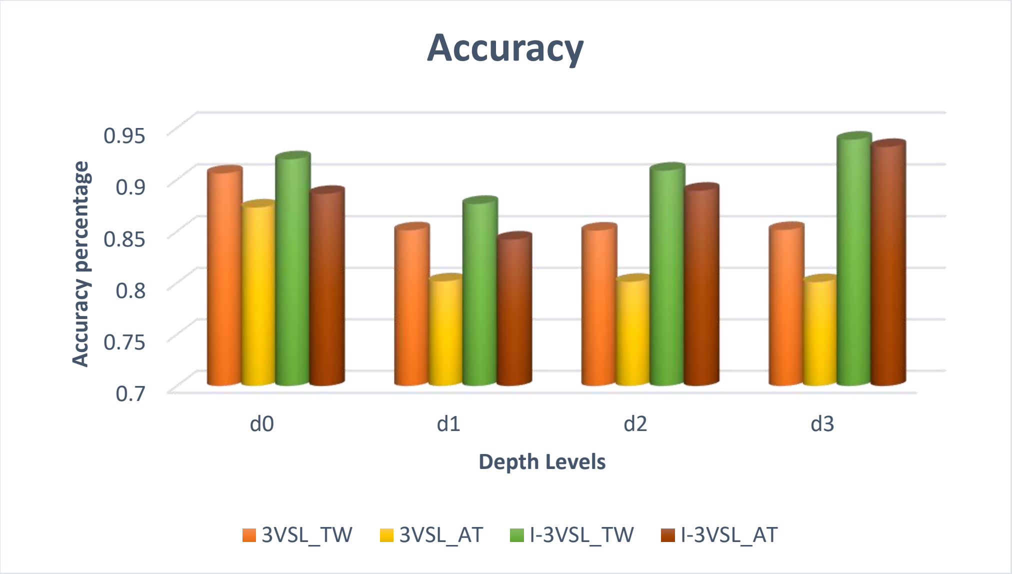


Figure 5.4 The accuracy comparison between I-3VSL_TW with 3VSL_AT [61]

According to Figure 5.4, the performance of the TW algorithm improves 5% in comparison to AT over 3VSL. The 3% improvement with I-3VSL over TW and AT Algorithms. Comparing the proposed approach I-3VSL_TW with the existing approach 3VSL_AT [61] obtains the 10% enhancement in terms of accuracy.

5.1.4.4 Evaluating the trust assessment

The trust is assessed using 3VSL and I-3VSL based on the trustors' perspective computed all the trustees' trust. Thus, I-3VSL provides an improvement in trust assessment. Hence, the trustor is selected randomly as 5, and the trustees are selected based on the in-degree of the trustor. The generated trust assessment results are depicted in Figure 5.5.

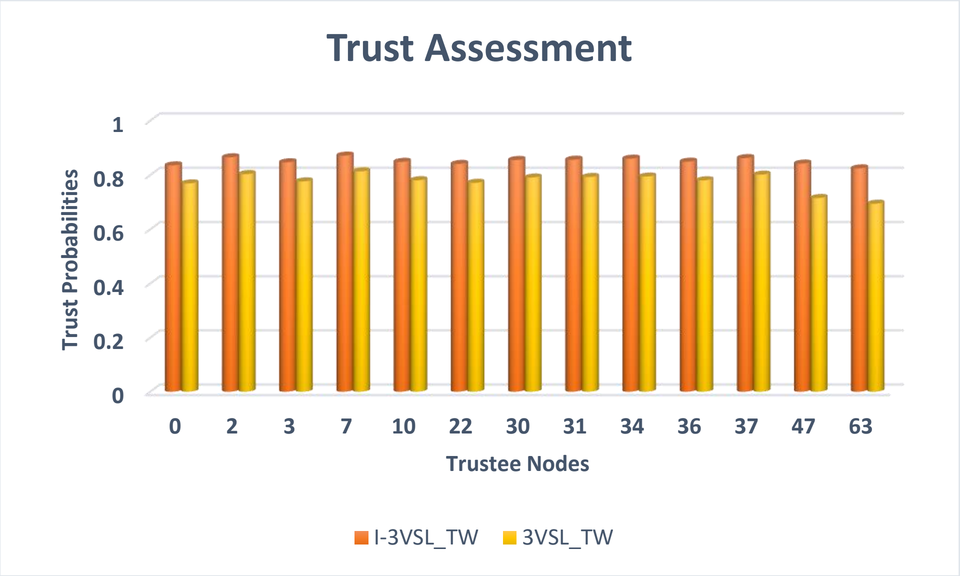


Figure 5.5 Trust probabilities of the trustees

According to Figure 5.5, the trust assessment according to I-3VSL operations provides 10% improvement compared to 3VSL for various trustees. The I-3VSL operation computes the trust by considering trust, distrust and posterior uncertainty. Consequently, the generated results are influenced by all the elements, whereas in 3VSL, only finds the trust. As a result, any changes in distrust or uncertainty are not affected in the development. Therefore, the obtained results provide a 10% improvement over the I-3VSL.

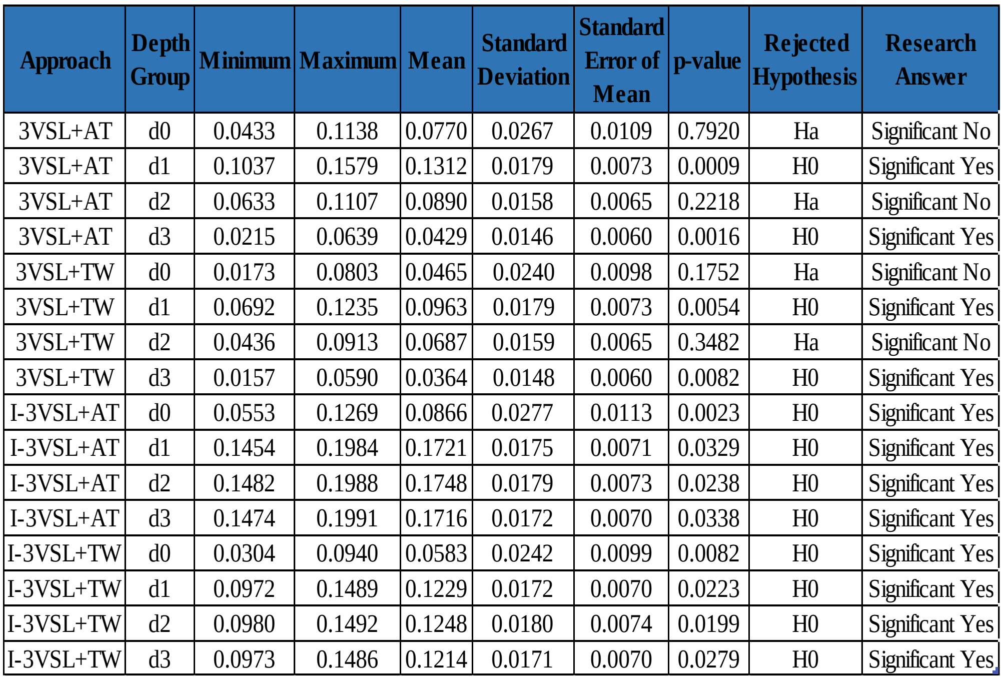
5.1.5.Statistical analysis

The statistical analysis of the MAE and trust assessment is determined by applying the hypothesis test. Generally, the practice states a null hypothesis, then determines whether the data allows the hypothesis's rejection. A P_{value} represents the probability that the null hypothesis is actual. The P_{value} is a measure of simulated data. If $P_{value} \leq$ 0.05 rejects the null hypothesis[153].

5.1.5.1 Statistical analysis for MAE

Table 5.2 presents the detailed result analysis of the one-tailed t-test with a significance level of 5% w.r.t the MAE along with the existing algorithm. The I-3VSLwith TW algorithm requires the minimum MAE for various depths.

Table 5.2 Statistical analysis of MAE

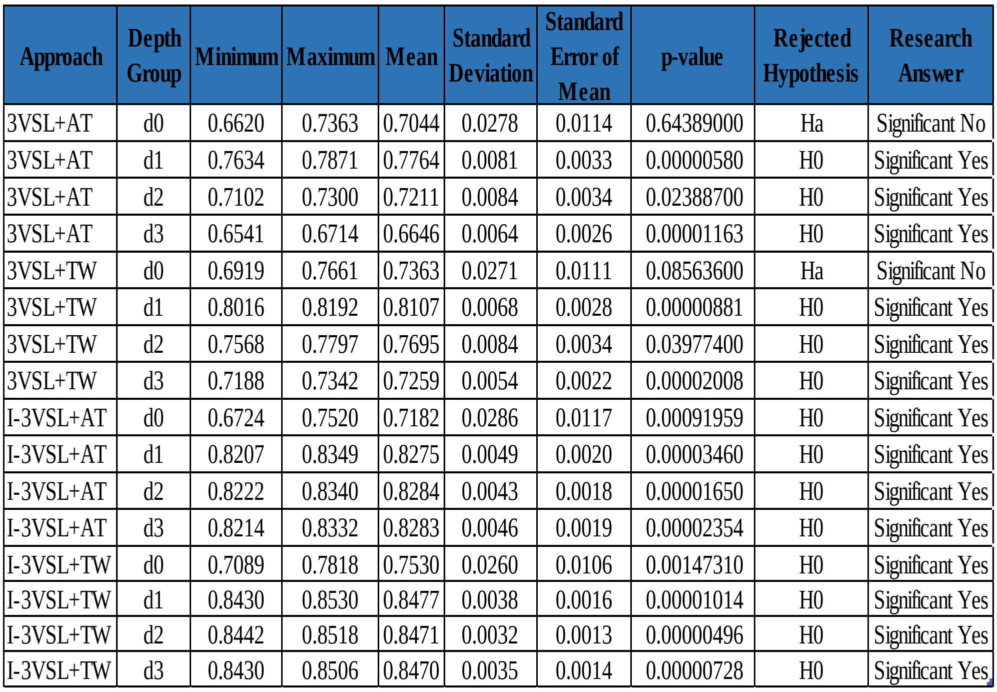


Approach	Depth Group	Minimum	Maximum	Mean	Standard Deviation	Standard Error of Mean	p-value	Rejected Hypothesis	Research Answer
3VSL+AT	d0	0.0433	0.1138	0.0770	0.0267	0.0109	0.7920	Ha	Significant No
3VSL+AT	d1	0.1037	0.1579	0.1312	0.0179	0.0073	0.0009	H0	Significant Yes
3VSL+AT	d2	0.0633	0.1107	0.0890	0.0158	0.0065	0.2218	Ha	Significant No
3VSL+AT	d3	0.0215	0.0639	0.0429	0.0146	0.0060	0.0016	H0	Significant Yes
3VSL+TW	d0	0.0173	0.0803	0.0465	0.0240	0.0098	0.1752	Ha	Significant No
3VSL+TW	d1	0.0692	0.1235	0.0963	0.0179	0.0073	0.0054	H0	Significant Yes
3VSL+TW	d2	0.0436	0.0913	0.0687	0.0159	0.0065	0.3482	Ha	Significant No
3VSL+TW	d3	0.0157	0.0590	0.0364	0.0148	0.0060	0.0082	H0	Significant Yes
I-3VSL+AT	d0	0.0553	0.1269	0.0866	0.0277	0.0113	0.0023	H0	Significant Yes
I-3VSL+AT	d1	0.1454	0.1984	0.1721	0.0175	0.0071	0.0329	H0	Significant Yes
I-3VSL+AT	d2	0.1482	0.1988	0.1748	0.0179	0.0073	0.0238	H0	Significant Yes
I-3VSL+AT	d3	0.1474	0.1991	0.1716	0.0172	0.0070	0.0338	H0	Significant Yes
I-3VSL+TW	d0	0.0304	0.0940	0.0583	0.0242	0.0099	0.0082	H0	Significant Yes
I-3VSL+TW	d1	0.0972	0.1489	0.1229	0.0172	0.0070	0.0223	H0	Significant Yes
I-3VSL+TW	d2	0.0980	0.1492	0.1248	0.0180	0.0074	0.0199	H0	Significant Yes
I-3VSL+TW	d3	0.0973	0.1486	0.1214	0.0171	0.0070	0.0279	H0	Significant Yes

5.1.5.2 Statistical analysis for trust assessment (TA)

Table 5.3 presents the detailed result analysis of the one-tailed t-test with a significance level of 5% w.r.t the TA along with existing algorithms. The I-3VSLwith TW algorithm requires the maximum TA for various depths.

Table 5.3 Statistical analysis of trust assessment



Approach	Depth Group	Minimum	Maximum	Mean	Standard Deviation	Standard Error of Mean	p-value	Rejected Hypothesis	Research Answer
3VSL+AT	d0	0.6620	0.7363	0.7044	0.0278	0.0114	0.64389000	Ha	Significant No
3VSL+AT	d1	0.7634	0.7871	0.7764	0.0081	0.0033	0.00000580	H0	Significant Yes
3VSL+AT	d2	0.7102	0.7300	0.7211	0.0084	0.0034	0.02388700	H0	Significant Yes
3VSL+AT	d3	0.6541	0.6714	0.6646	0.0064	0.0026	0.00001163	H0	Significant Yes
3VSL+TW	d0	0.6919	0.7661	0.7363	0.0271	0.0111	0.08563600	Ha	Significant No
3VSL+TW	d1	0.8016	0.8192	0.8107	0.0068	0.0028	0.00000881	H0	Significant Yes
3VSL+TW	d2	0.7568	0.7797	0.7695	0.0084	0.0034	0.03977400	H0	Significant Yes
3VSL+TW	d3	0.7188	0.7342	0.7259	0.0054	0.0022	0.00002008	H0	Significant Yes
I-3VSL+AT	d0	0.6724	0.7520	0.7182	0.0286	0.0117	0.00091959	H0	Significant Yes
I-3VSL+AT	d1	0.8207	0.8349	0.8275	0.0049	0.0020	0.00003460	H0	Significant Yes
I-3VSL+AT	d2	0.8222	0.8340	0.8284	0.0043	0.0018	0.00001650	H0	Significant Yes
I-3VSL+AT	d3	0.8214	0.8332	0.8283	0.0046	0.0019	0.00002354	H0	Significant Yes
I-3VSL+TW	d0	0.7089	0.7818	0.7530	0.0260	0.0106	0.00147310	H0	Significant Yes
I-3VSL+TW	d1	0.8430	0.8530	0.8477	0.0038	0.0016	0.00001014	H0	Significant Yes
I-3VSL+TW	d2	0.8442	0.8518	0.8471	0.0032	0.0013	0.00000496	H0	Significant Yes
I-3VSL+TW	d3	0.8430	0.8506	0.8470	0.0035	0.0014	0.00000728	H0	Significant Yes

According to Table 5.2 and 5.3, the CI with0.95, the significance value (∞) is fixed with 0.05. The significance value (∞) is above the P_{value}, the null hypothesis is accepted, and no considerable difference is noticed in the various depths based on the in-degree of the trustor, which means no significant gain is achieved on this evaluation. Nonetheless, our simulation table results show that the P_{value} is less than or equal to 0.05, which means that the I-3VSL_TW achieved considerable gain on traditional protocols with the 30 samples of records for various depths. The I-3VSL_TW accepts the null hypothesis for different depths. However, the 3VSL_AT trust assessment is carried a null hypothesis in the case of $d_1 and\ d_2$, remaining cases it accepts the alternative hypothesis.

5.2 An Experiment of Content Protection

In general, the effectiveness of the proposed watermarking scheme is determined through robustness and imperceptibility. The proposed watermarking scheme focused on the RGB Anaglyph 3D images. It is critical to compare it to other comparable schemes [8], [118] to illustrate the proposed watermark scheme's superiority in terms of invisibility and robustness. Thus, the experiment is conducted on Microsoft Windows-10 with 64-bit core i3-7100U CPU 2.4 GHz and 4GB RAM. The proposed watermarking scheme efficacy is demonstrated leveraging the red-cyan and other forms of Anaglyph 3Dimages.

5.2.1 Experimental setup

The proposed watermark scheme performance is assessed using different standard and customized RGB Anaglyph 3D images. The red-cyan images such as Adirondack, Aloe, Art, Baby and many others are collected from the Middlebury Stereo datasets[154]. The true, color, mono, optimized-color and half-color Anaglyph 3D images are created using a saliency map [155]. The red-cyan cover image sizes as $512 \times 512 \times 512 \times 3$ and watermark logs are variable sizes such as $256 \times 256 \times 256 \times 3, 128 \times 128 \times 128 \times 3,\ 64 \times 64 \times 64 \times 3$. For instance, the cover and watermark logos of red-cyan

Anaglyph 3D images and other forms of Anaglyph 3D images are depicted in Figures 5.6 and 5.7.

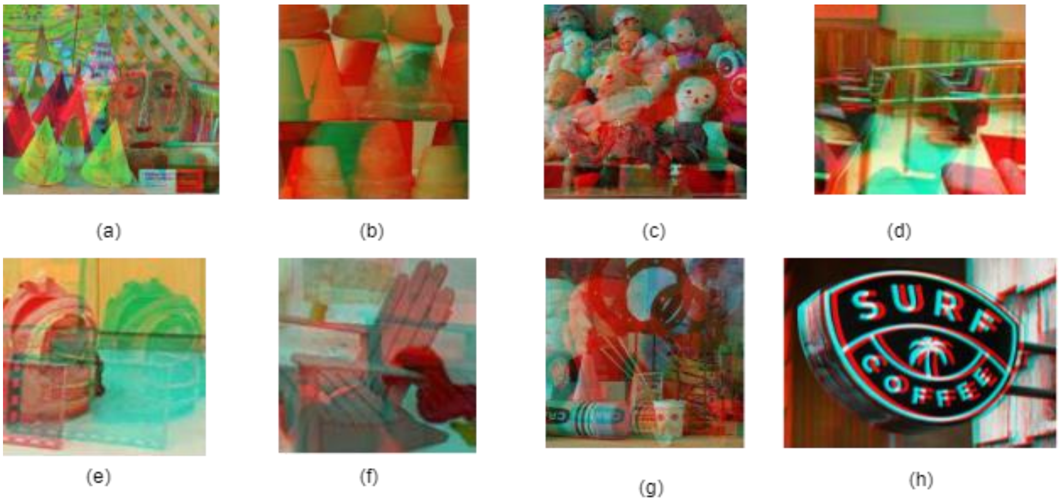


Figure 5.6 **Cover images:** (a) cones (b) flowerpots (c) dolls (d) classroom (e) backpack (f) Adirondack (g) art **Watermark logo:** (h) Surf Coffee

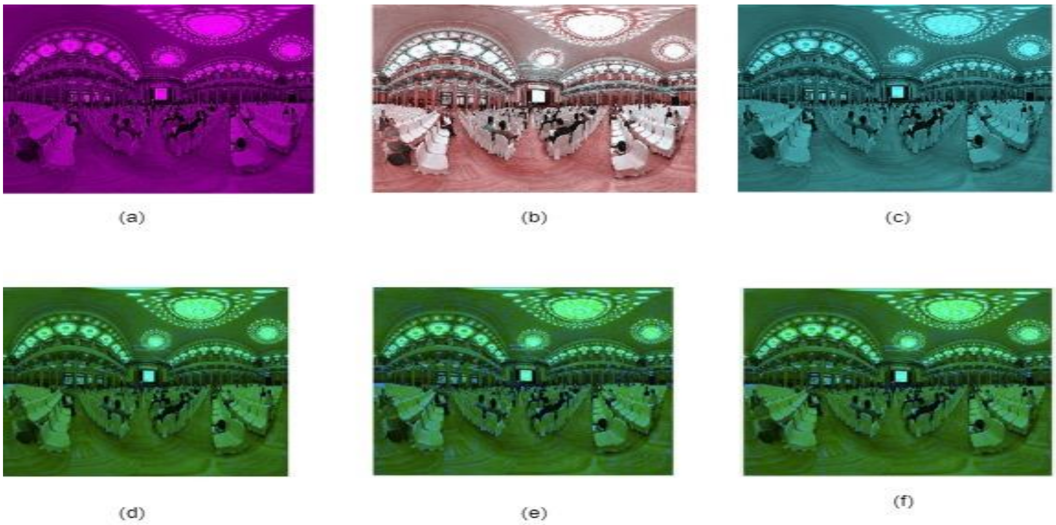


Figure 5.7 **Cover images:** (a) True Anaglyph (b) Red-cyan Anaglyph (c) Mono Anaglyph **watermark logos:** (d) Color Anaglyph (e) Half-color Anaglyph (f) optimized-color Anaglyph 3D images

5.2.2 Performance metrics

The performance of the proposed watermark framework is assessed through MSE, SSIM, PSNR, and NCC. The MSE and PSNR are used to determine the watermark quality through Eq. (5.4) and (5.5).

$$MSE = \frac{1}{(p * q * r)} \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} \sum_{k=0}^{r-1} \left(C_I(i,j,k) - M_I(i,j,k) \right)^2 \qquad (5.4)$$

$$PSNR = 10 \ \log_{10} \frac{k_{max}^2}{MSE} \qquad (5.5)$$

Here p, q, r are the dimensions of the Anaglyph host image, $C_I and\ M_I$ are host and watermarked images. In Eq.(5.5), k_{max} signifies the host images max dimension value. However, the MSE and PSNR are inversely proportional to each other, the PSNR value is higher, and MSE is low, then the watermarked image quality is high. The imperceptibility capacity is assessed through SSIM based on the luminance (l), contrast (cont) and structure (struct), which is represented in Eq. (5.6).

$$SSIM = l(C_I, M_I) * cont(C_I, M_I) * struc(C_I, M_I) \qquad (5.6)$$

$$l(C_I, M_I) = \frac{2\mu_{CI}\mu_{MI} + C_1}{\mu_{CI}^2 + \mu_{MI}^2 + C_1} \qquad (5.7)$$

$$cont(C_I, M_I) = \frac{2\sigma_{CI}\sigma_{MI} + C_2}{\sigma_{CI}^2 + \sigma_{MI}^2 + C_2} \qquad (5.8)$$

$$struct(C_I, M_I) = \frac{\sigma_{CIMI} + C_3}{\sigma_{CI}\sigma_{MI} + C_3} \qquad (5.9)$$

Here, C_1, C_2, C_3 are constants, $\mu\ and\ \sigma$ are mean and standard deviation. The l computes the average luminance of cover and watermarked images through Eq. (5.7). The $cont$ is calculating the contrast of cover and watermarked images the standard deviation using Eq. (5.8). The $struct$ computes the correlation between the cover and watermarked Eq. (5.9). The correlation value normalized to [0, 1], 0 represents the different images, and 1 means similar. Therefore, PSNR, SSIM values are specifically used to denote the imperceptibility of watermarked images. Moreover, the robustness of the proposed watermarking scheme is assessed through NCC or NC is represented in Eq. (5.10).

$$NCC = \frac{\sum_{i=0}^{p-1} \sum_{j=0}^{q-1} \sum_{k=0}^{r-1} W_I^{RGB}(i,j,k) \times M_I^{ext}(i,j,k)}{\sqrt{\sum_{i=0}^{p-1} \sum_{j=0}^{q-1} \sum_{k=0}^{r-1} (W_I^{RGB})^2} \sqrt{\sum_{i=0}^{p-1} \sum_{j=0}^{q-1} \sum_{k=0}^{r-1} (M_I^{ext})^2}} \qquad (5.10)$$

Here, $W_I^{RGB} and\ M_I^{ext}$ are denotes the watermark logo and extracted watermark. The NCC value ranges from 0 to 1, with 1indicating the improved robustness to different attacks on watermarked images.

5.2.3 Experimental results

The proposed watermarking scheme's experimental results are determined by examining the optimal scaling factor over the MSE, PSNR, SSIM and NC under varied size watermark logos. Further, based on the red-cyan and true Anaglyph images with varying sizes of watermark logos, the imperceptibility and robustness of the proposed watermarked scheme are examined. Additionally, evaluate the robustness and imperceptibility of the various attacks under different parameters. Finally, the proposed watermarked scheme is compared against the current work under multiple attacks.

5.2.3.1 Analyzing the optimal scaling factor

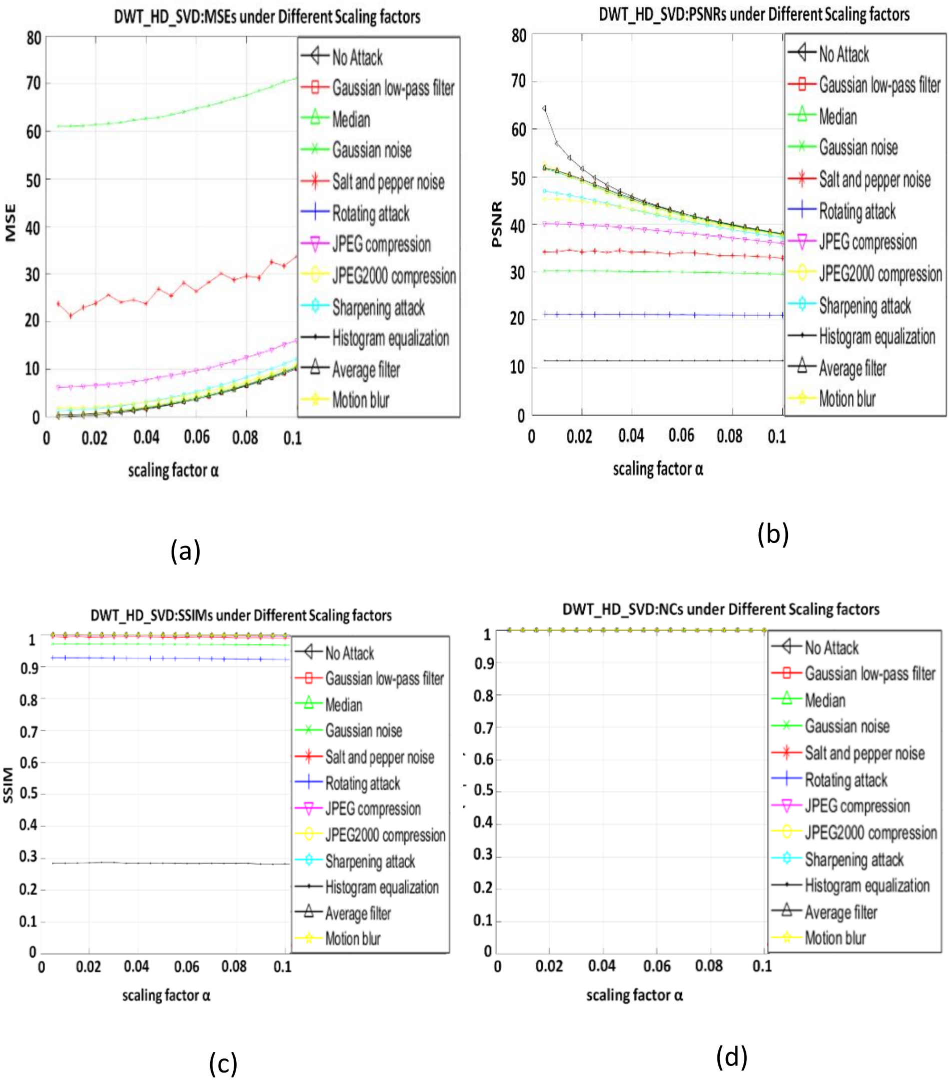
The performance of the proposed watermarking scheme is analyzed under various attacks to determine the optimal scaling factor. Figure 5.6 depicts the flow to compute the optimal scaling factor (α) under multiple attacks. Then, the appropriate scaling factor for varied watermark logo sizes is determined. For instance, the red-cyan is considered to cover and watermark logs that find the relevant scaling factor through the performance metrics. The red-cyan Anaglyph 3D images are depicted in Figures 5. 6, and 5.7, and the attacks are listed in Table 5.4.

Table 5. 4 Types of attacks with specifications

Name of the attack	Attack category	Value
Average filter	Filtering attack	–
Gaussian low-pass filter	Filtering attack	3×3
Median filter	Filtering attack	3×3
Gaussian noise	Noise attack	0.001
Salt and Pepper noise	Noise attack	–
Rotation attack	Geometric attack	2°
JPEG compression	Lossy compression	50

JPEG2000 compression	Lossy compression	12
Sharpening attack	Sharpening attack	0.8
Histogram attack	Contrast enhancement	–
Motion blur	Blurring attack	–

Therefore, the performance metric values of MSE, PSNR, SSIM and NCC are obtained by varying the scaling factor from 0 to 0.1 under different attacks. The results are depicted in Figures 5.8 (a)-(d).



(a)

(b)

(c)

(d)

Figure 5. 8 Performance under various attacks with different scaling factors

According to Figures 5.8 (a)-(d), the MSE for different attacks with the scaling factors ranging from [0, 0.1] and the values are increasing steadily as the scaling factors increase. However, the salt and pepper and Gaussian noise attack yield higher values than other attacks—the PSNR for different attacks under scale factors with a range of [0, 0.1]. Thus, the PSNR value negatively correlates with the scaling range [0, 0.1]. Therefore, the initial scaling factor for PSNR is $\alpha_1 = 0.005$. The SSIM for different attacks under various scaling factors with a range of [0, 0.1] provides stabilized results. Thus, the default scaling factor for SSIM is $\alpha_1 = 0.005$. The NCC provides consistent results for different attacks under various scaling factors. Thus, the baseline scaling factor is $\alpha_2 = 0.005$. As a result, the optimized scaling factor (α) is determined by using Eq. (4.22).

5.2.3.2 Imperceptibility assessment

The visibility quality or imperceptibility means the embedded information in the cover image is not visible to the human eyes. The embedded information is not affected by the visual appearance. Therefore, the imperceptibility of the watermark embedding is validated through the various red-cyan as depicted in Figure 5.7 and other Anaglyph 3D images shown in Figure 5.8 as the cover images, watermark logos. The watermarked images' performance under no attack is considered a baseline because the watermarked images do not suffer from the attacks. Therefore, the watermarked images and extracted watermark logos with different sizes such as $256 \ \times 256 \times 256, 128 \times 128 \times \ and\ 64 \times 64 \times 64$ are shown in, Fig 5.9, Table 5.5 and Table 5.6.

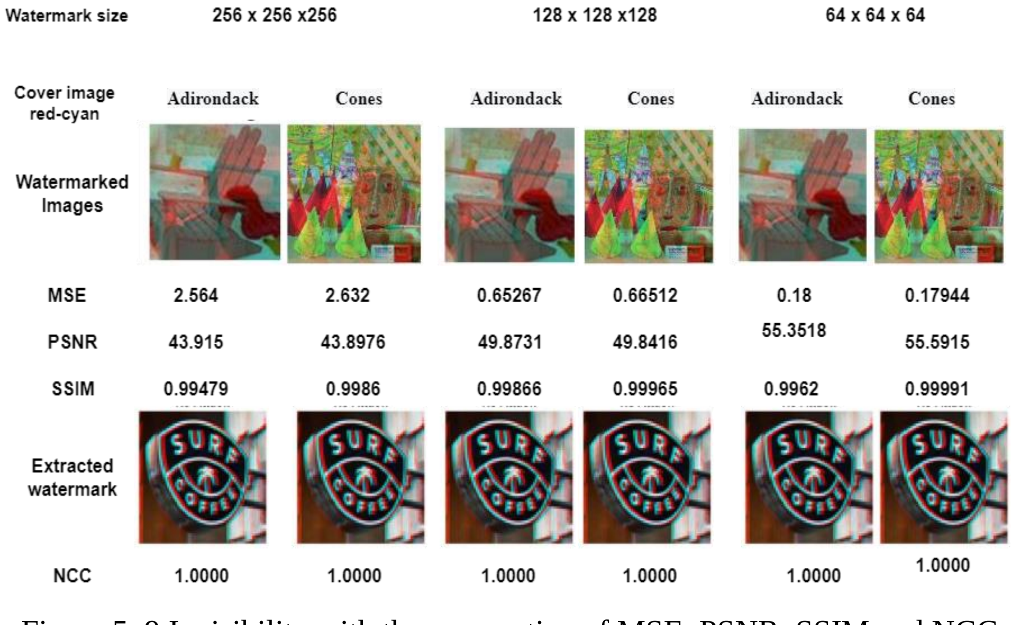


Figure 5. 9 Invisibility with the perspective of MSE, PSNR, SSIM and NCC

Table 5.5 PSNR values for various red-cyan Anaglyph images with different sizes

PSNR	Adirondack	Aloe	Art	Baby	Backpack	Classroom	Cones	Dolls2
256x256	43.915	49.847	43.898	43.893	43.899	43.906	43.898	43.906
128x128	49.842	49.847	49.914	49.687	49.762	49.944	49.873	49.889
64x64	55.352	49.847	55.753	54.972	49.762	55.989	55.592	55.756

Table 5.6 Imperceptibility performance based on MSE, PSNR, SSIM and NCC

			Perfomance metrics			
Cover image	Watermark logo	Watermark size	MSE	PSNR	SSIM	NCC
True Anaglyph	Half-Color Anaglyph	256x256x256	0.6968	49.6200	0.9999	1
Red-cyan Anaglyph	Half-Color Anaglyph	256x256x256	0.6716	49.7703	0.9992	1
Mono Anaglyph	Half-Color Anaglyph	256x256x256	0.6871	49.6811	0.9998	1
True Anaglyph	Color Anaglyph	256x256x256	0.6948	49.6321	0.9999	1
Red-cyan Anaglyph	Color Anaglyph	256x256x256	0.6696	49.7820	0.9992	1
Mono Anaglyph	Color Anaglyph	256x256x256	0.6853	49.6918	0.9998	1
True Anaglyph	Half-Color Anaglyph	128x128x128	0.2138	54.7867	0.9999	1
Red-cyan Anaglyph	Half-Color Anaglyph	128x128x128	0.1914	55.2751	0.9997	1
Mono Anaglyph	Half-Color Anaglyph	128x128x128	0.2125	54.8135	0.9999	1
True Anaglyph	Color Anaglyph	128x128x128	0.2131	54.8012	0.9999	1
Red-cyan Anaglyph	Color Anaglyph	128x128x128	0.1905	55.2935	0.9997	1
Mono Anaglyph	Color Anaglyph	128x128x128	0.2118	54.8287	0.9999	1
True Anaglyph	Half-Color Anaglyph	64x64x64	0.0391	62.2039	1.0000	1
Red-cyan Anaglyph	Half-Color Anaglyph	64x64x64	0.0462	61.4839	0.9999	1
Mono Anaglyph	Half-Color Anaglyph	64x64x64	0.0391	62.2040	1.0000	1
True Anaglyph	Color Anaglyph	64x64x64	0.0389	62.2298	1.0000	1
Red-cyan Anaglyph	Color Anaglyph	64x64x64	0.0462	61.4839	0.9999	1
Mono Anaglyph	Color Anaglyph	64x64x64	0.0391	62.2040	1.0000	1

According to Figure 5.9, Table 5.5, and Table 5.6, The default PSNR value for under no attack of the watermarked image is determined for red-cyan Anaglyph with different sizes are $> 43\ dB, > 49\ dB\ and > 54dB$ and for other Anaglyph images $> 49dB, > 54dB\ and\ 61dB$. Further, the SSIM value for red-cyan and other Anaglyph images is > 998. The watermark logo size is smaller than the PSNR, and SSIM values for red-cyan Anaglyph are 55 dB and 0.9991, respectively, as shown in Figure 5.9. As shown in Table 5.6, the values 61 dB and 1 are observed respectively for other Anaglyph images. The NCC value for all the Anaglyph 3D extracted watermark images is 1.0000. Therefore, the proposed watermarking scheme provides excellent imperceptibility.

5.2.3.3 Robustness assessment

The images robustness emphasizes the capacity to sustain alterations without affecting the original structure. In digital watermarking schemes, the robustness is assessed between the extracted watermark and original watermark logo under the different attacks. As a result, validating the robustness of the proposed watermarking scheme is crucial. The effectiveness of the watermark extraction algorithm is assessed by applying various attacks on the watermarked image, as illustrated in Figure 5.10. The performance of the extracted watermarked logos is examined, whether they are resistant to attacks. Further, an extraction algorithm is performed under various attacks on the different sizes of watermarked images. Later, the recovered watermark images and their associated NCC values are shown in Table 5.6.

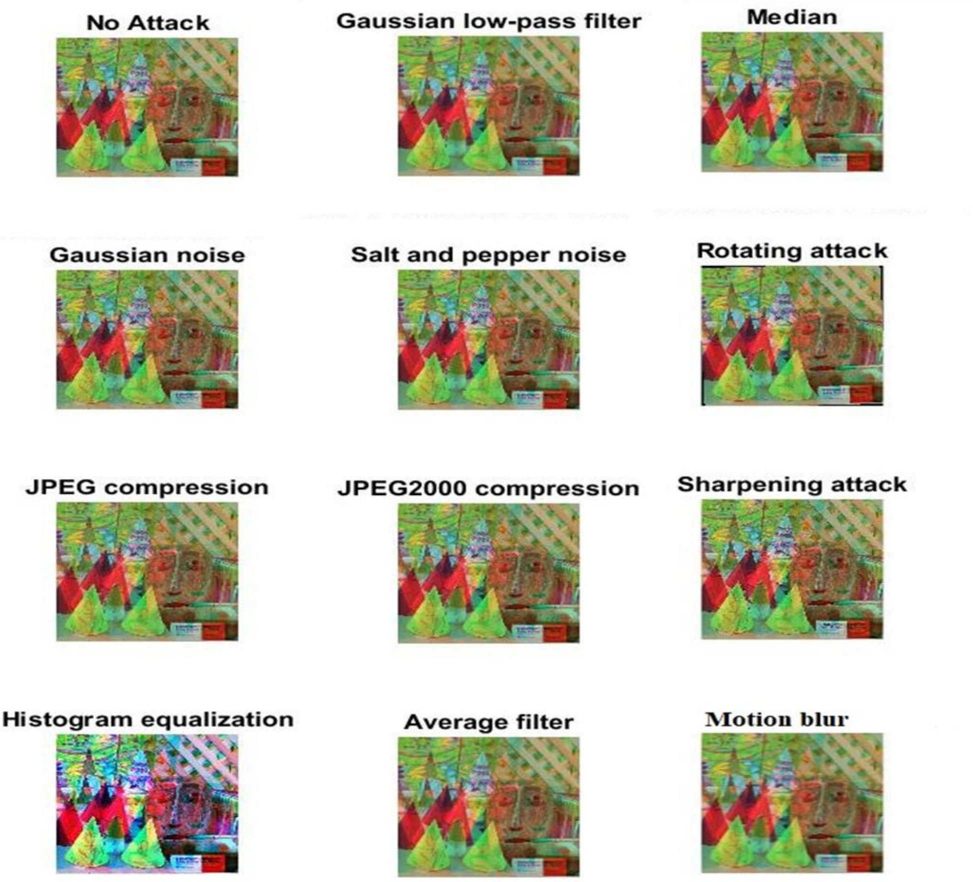


Figure 5.10 Attacked watermarked Cone red-cyan color Anaglyph images

According to Table 5.7, the extracted watermarks robustness is acceptable for all the sizes of red-cyan Anaglyph images. Significantly, NCC's of all attacks except for the HE attack, the value decreases while the watermark logos' sizes decrease.

Table 5.7 Recovered watermark logos with NCC values

Attacks	256 x 256 x 256	128 x 128 x 128	64 x 64 x 64
No Attack	1	1	1
Gaussian low-pass filter	1	1	1
Median	1	1	1
Gaussian noise	1	1	1
Salt and pepper noise	1	1	1
Rotating attack	1	1	1
JPEG compression	1	1	1
JPEG2000 compression	1	1	1
Sharpening attack	1	1	1
Histogram equalization	0.9924	0.9913	0.9877
Average filter	1	1	1
Motion blur	0.9322	0.9569	0.9147

Further, the NCC values of all the attacks ≥ 0.99 of different sizes of watermark logos except motion blur attack. The extracted watermarks differ in the case of motion blur, but the preliminary information is identical. The extracted watermarking algorithm is validated under three filtering attacks, two noise attacks, two compression attacks, rotation, and sharpening attacks, providing high robustness as 1 for all sizes of watermark logos. Therefore, the proposed scheme offers high robustness for filtering, noise, compression, rotation and sharpening attacks. However, the proposed watermarking scheme is validated under static parameters, and then the results provide acceptable robustness.

Therefore, the performance of the proposed method validated under dynamic parameters and results are depicted in Figure 5.11.

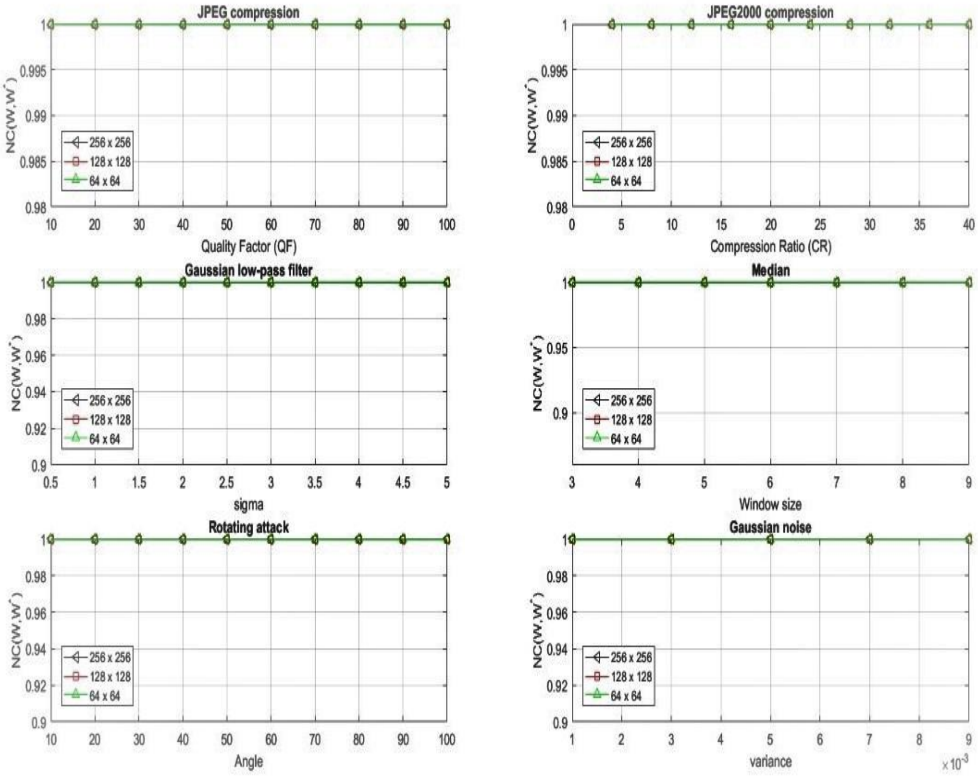


Figure 5.11 Different attacks for dynamic parameters

According to Figure 5.11, the JPEG compression attack validated with Quality factor (QF) ranges from [10,100]. The NCC value for all the sizes is≥ 0.99. The JPEG2000 compression is evaluated with Compression Ratio (CR) varying from [0, 40], then obtained NCC value is equal to 1. Similarly, two filtering attacks such as Gaussian low-pass filter with sigma ranges from [0.5, 5] and median filter with window sizes [3x3, 9x9] then obtained results provides the high robustness. The rotation attack is applied to vary the rotation angle from [10,100] with a 10 step increment and gives high robustness to all the sizes. The Gaussian noise attack is used based on the variance ranging of [0.001, 0.009] by incrementing with 0.001 that provides high robustness for all the sizes. Therefore, the proposed watermarking scheme is more robust and imperceptible for all sizes of watermark logos.

5.2.4 Comparative Analysis

The proposed watermarking scheme is validated in terms of robustness and imperceptibility by comparing it with the existing watermark approaches.[118]. Thus, the robustness is compared with two types of attacks: geometric and non-geometric attacks. The non-geometric attacks are intended to extract the watermark logos from watermarked images without compromising the integrity of the watermarking algorithm [156]. The non-geometric attacks include filtering, noise, compression, motion blur, sharpening, and HE attacks [119]. The geometric attacks include rotation, translation, cropping, and scaling. The proposed watermarking scheme's performance is validated using various red-cyan Anaglyph 3D images against the geometric and non-geometric attacks with specific parameters, as shown in Table 5.4. The comparative analysis of the proposed watermarking scheme with Koley [118] is demonstrated in Table 5.8.

Table 5.8 Comparison of performance metrics between the proposed approach and the Koley approach

Attacks	Proposed approach (DWT_HD_SVD)				Koley Approach (LWT,T-SVD,ACM) [118]			
	MSE	PSNR	SSIM	NCC	MSE	PSNR	SSIM	NCC
No Attack	2.3979	43.4995	0.9942	1.0000	7.6958	39.9817	0.8976	0.9997
Gaussian low-pass filter	2.2874	47.0975	0.9964	1.0000	7.2157	43.9492	0.9863	0.9978
Median	2.3648	46.9303	0.9966	1.0000	6.1976	44.9776	0.9883	0.9997
Gaussian noise	13.9232	42.7215	0.9729	1.0000	20.1743	38.2505	0.8601	0.9970
Salt and pepper noise	1.9400	49.4835	0.9896	1.0000	7.7711	44.4324	0.9883	0.9999
Rotating attack	19.3678	28.0144	0.8496	1.0000	23.0693	26.0930	0.8106	0.9961
JPEG compression	4.3504	46.9281	0.9898	1.0000	17.4524	35.6062	0.8779	0.9947
JPEG2000 compression	1.8800	53.9253	0.9975	1.0000	7.2233	44.3621	0.9954	0.9990
Sharpening attack	1.7517	51.3949	0.9962	1.0000	6.6343	44.2925	0.9888	0.9948
Histogram equalization	65.1977	20.0189	0.6568	0.9924	67.1473	19.8494	0.5877	0.8761
Average filter	2.2757	47.0632	0.9916	1.0000	7.3442	43.7749	0.8873	0.9982
Motion blur	3.0191	43.1968	0.9909	0.9322	19.1428	28.8531	0.8612	0.8583

According to Table 5.8, the proposed watermarking scheme provides more robustness against all the attacks as ≥ 99 expect motion blur attacks. As a result, the proposed watermarking scheme offers 2% robustness over the Koley approach [118]. Similarly, the imperceptibility of the proposed approach is validated through MSE, PSNR and SSIM as the baseline is under no attack. Thus, the proposed scheme provides MSE, PSNR and SSIM as $2.39, 43.49, and\ 0.9941,$ whereas the existing approach provides $7.69, 39.98\ and\ 0.8975.$ Further, it applies the various attacks by assessing each attack's performance. The assessed value is lower than MSE and higher than the PSNR and SSIM's base value. Then the watermarking scheme provides high imperceptibility; otherwise, it is lower imperceptible. Therefore, the proposed watermarking scheme gives high invisibility to all the filtering attacks based on the MSE, PSNR and SSIM. The invisibility of noise attacks such as Gaussian noise is good, and salt and pepper is high. The compression attacks such as JPEG and JPEG2000 provides moderate and high imperceptibility. The sharpening attack also provides high invisibility, and the HE attack provides lower imperceptibility. The motion blur attack provides moderated imperceptibility. However, the proposed approach offers enhanced imperceptibility for all the attacks compared to the existing approach. Therefore, the proposed watermarking scheme enhances robustness and imperceptibility against all the attacks over the Koley method [118] for red-cyan Anaglyph 3D images.

5.3 Summary

This chapter presents an experimental setup for both trust assessment and content protection. The trust assessment simulation work is carried out using the network analysis in python by setting the various parameters. The experiment is conducted using the Travian dataset to establish the trusted network. The performance of the proposed I-3VSL with TW is evaluated through trust assessment, MSE, RMSE, and accuracy. The evaluation metrics provide better results than 3VSL with AT and assessed the data accuracy by conducting statistical hypothesis tests for various depths. Correspondingly, the experiment is performed for the proposed robust watermarking scheme. The performance of the proposed watermarking scheme is evaluated through the imperceptibility and robustness of different sizes of watermark logos. Thereafter, the robustness is assessed through dynamic parameters. Therefore, the proposed scheme provides better results compared to existing watermarking techniques.

CHAPTER 6
CONCLUSION

The proposed work includes the trusted partner selection scheme through the I-3VSL uncertainty model and content protection for the red-cyan Anaglyph 3D images. The trust partner selection is essential in MMOG that optimizes the risk, increases productivity and establishes strong relationships among the participant players in the network. Similarly, the content protection techniques provide the digital media's integrity and restrict the illegal distribution of the content over the internet. Therefore, the thesis focused on studying the trusted partner selection schemes in the P2P environment and content protection techniques. The proposed strategies provide the enhanced trustworthy partner selection scheme and content protection technique through a robust watermarking scheme that fulfils the requirements of both safety and privacy in the virtual environment. Hence, the objective of the proposed research is to "Design and Implement an algorithm to enhance the trustworthiness of partner selection and content protection in P2P 3D Streaming over thin mobile devices." Primarily, the thesis demonstrates a comprehensive introduction of P2P 3D streaming over thin mobile devices. Further, the chapter presents the research objective of the present research. Chapters 2 is devoted to a detailed literature review of the trust and recommendation models in the P2P environment and content protection with digital watermarking techniques. We noticed that most of the existing trust assessment models focused on absolute trust in the survey—the lack of uncertainty models available to assess the trust also requires improvement in the uncertainty models. Similarly, the current content protection through watermarking techniques for red-cyan Anaglyph 3D images is focused on the DWT that also requires enhancement in terms of robustness and imperceptibility. Chapters 3,4 and 5 focus on the trust computation of all the trustees from the trustor perspective in arbitrary network, the content protection through a robust watermarking scheme that enhances the robustness and imperceptibility of the red-cyan Anaglyph 3D images with different watermark logos and followed by experimental results. The detailed contributions are presented in the following subsection. Finally, an illustration of the research program concludes by proposing future research directions.

6.1 Contributions

The significant contributions of the thesis are outlined below,

Contribution 1: Formulate a trustworthy partner selection scheme through an uncertainty trust model

The proposed I-3VSL uncertainty trust assessment paradigm is to manage the trust effectively with the help of direct and indirect trust assessments. The direct trust is evaluated based on the interaction among the players. The trust opinion of interactions is represented as positive, negative, prior and posterior uncertainties based on the trust opinion between the players computed. The indirect trust is assessed through trust propagation and fusion, performed using improved discounting and combining operations. The direct and indirect trust assessments are formulated and represented in chapter 3.

Contribution 2: Design an effective trustworthiness computing algorithm

An effective trustworthiness computing algorithm is proposed to assess all the trustees' trust from the trustors' perspectives through the TW algorithm. The TW algorithm was designed by incorporating the improved discounting and combining operations. This algorithm works in depth limited BFS fashion, and it executes faster compared to the existing AT, i.e. $O(n^2)$. The performance of the proposed algorithm is validated by establishing the trusted network through the Travian dataset. The performance is assessed through computing the error and accuracy that shows the 10% improvement in the accuracy of trust assessment over the existing approach. The proposed TW algorithm and comparison details are presented in Chapters 3 and 5.

Contribution 3: Design the 3D content /copyright protection scheme

A robust watermarking scheme is proposed to protect the digital content over thin mobile devices. The watermarking scheme algorithm is designed by leveraging the DWT, HD and SVD to perform the embedded and extraction operations. Further, an optimized scaling factor is determined through PSO. The performance of the proposed watermarking scheme is examined by using red-cyan Anaglyph 3D images. The cover and watermark logos are RGB color channels, and variable size watermark logos are leveraged in this study. The optimized scaling factor is primarily determined by selecting the scaling element ranging from [0, 0.1] then measuring the scaling factor.

Further, the embedded and extraction operations are directed based on the optimized scaling factor. Thereafter, the baseline of the performance metrics is determined under a no attack scenario—the performance metrics used as MSE, PSNR, SSIM and NCC. The proposed watermarking scheme is examined under different geometric and non-geometric attacks that show resistance. The proposed approach enhances the 2% robustness and 10% imperceptibility over the existing watermarking scheme, and the details are presented in chapters 4 and 5.

6.2 Future research directions

Trust assessment and content protection are fundamental security aspects in the virtual environment. The present trust assessment research program can be extended towards the optimization aspect that further enhances this topic. Firstly, research can be developed by incorporating the Monte Carlo principles into the I-3VSL operations, such as discounting and combining. Additionally, the trust computing algorithm is optimized through meta-heuristic algorithms. Similarly, the watermarking scheme is extended by using artificial intelligence and machine learning techniques to protect the content against various geometric and non-geometric attacks effectively. However, the existing watermarking schemes store their watermark information in the centralized server, creating leakage and alteration. Hence, it requires decentralized storage that can enhance content protection.

The thin mobile device applications are still evolving to cater to their actual purpose, and a lot of research is in progress. The growth of virtual environment applications such as virtual online video games, healthcare, and medical applications has given security researchers a lot of scopes. Concerning trusted partner selection strategies in MMOG, digital content protection is further extended by employing the benefits of the recent developments in Deep Learning and Blockchain technology that have opened up new research areas in privacy-preserving communications. Additionally, evolving information and communication technology (ICT) like 6G has opened new virtual environment research horizons. Efficient security, privacy, and trusted routing remain open for the investigators.

REFERENCES

[1] T. El-Ganainy and M. Hefeeda, “Streaming Virtual Reality Content,” *ArXiv161208350 Cs*, vol. abs/1612.08350, pp. 1–8, Dec. 2016.

[2] Y. Sun, Z. Chen, M. Tao, and H. Liu, “Communications, Caching and Computing for Mobile Virtual Reality: Modeling and Tradeoff,” *ArXiv180608928 Cs Math*, vol. 67, no. 11, pp. 7573–7586, Jun. 2018.

[3] W. Zhang, B. Han, P. Hui, V. Gopalakrishnan, E. Zavesky, and F. Qian, “CARS: Collaborative Augmented Reality for Socialization,” in *Proceedings of the 19th International Workshop on Mobile Computing Systems & Applications*, Tempe Arizona USA, Feb. 2018, pp. 25–30. doi: 10.1145/3177102.3177107.

[4] L. V. Fernandes, C. D. Castanho, and R. P. Jacobi, “A Survey on Game Analytics in Massive Multiplayer Online Games,” in *2018 17th Brazilian Symposium on Computer Games and Digital Entertainment (SBGames)*, Oct. 2018, pp. 21–2109. doi: 10.1109/SBGAMES.2018.00012.

[5] H. R. Maamar, A. Boukerche, and E. Petriu, “Streaming 3D meshes over thin mobile devices,” *IEEE Wirel. Commun.*, vol. 20, no. 3, pp. 136–142, Jun. 2013, doi: 10.1109/MWC.2013.6549293.

[6] W.-L. Sung, S.-Y. Hu, and J.-R. Jiang, “Selection strategies for peer-to-peer 3D streaming,” Jan. 2008, pp. 15–20. doi: 10.1145/1496046.1496050.

[7] J. Yan and B. Randell, “An Investigation of Cheating in Online Games,” *IEEE Secur. Priv. Mag.*, vol. 7, no. 3, pp. 37–44, May 2009, doi: 10.1109/MSP.2009.60.

[8] H. Devi and K. Singh, “red-cyan anaglyph image watermarking using DWT, Hadamard transform and singular value decomposition for copyright protection,” *J. Inf. Secur. Appl.*, vol. 50, p. 102424, Feb. 2020, doi: 10.1016/j.jisa.2019.102424.

[9] J. Prather, R. Nix, and R. Jessup, “Trust management for cheating detection in distributed massively multiplayer online games,” in *2017 15th Annual Workshop on Network and Systems Support for Games (NetGames)*, Jun. 2017, pp. 1–3. doi: 10.1109/NetGames.2017.7991547.

[10] H. R. Maamar, A. Boukerche, and E. Petriu, “A multihop supplying partner protocol for 3D streaming systems over thin mobile devices,” in *Proceedings of the second ACM international symposium on Design and analysis of intelligent vehicular networks and applications*, New York, NY, USA, Oct. 2012, pp. 81–88. doi: 10.1145/2386958.2386971.

[11] S. A. Abdulazeez, A. El Rhalibi, and D. Al-Jumeily, “Evaluation of scalability and communication in MMOGs,” in *2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC)*, Jan. 2016, pp. 393–398. doi: 10.1109/CCNC.2016.7444812.

[12] “Second Life.” https://secondlife.com/ (accessed Nov. 11, 2021).

[13] H. R. Maamar, A. Boukerche, and E. M. Petriu, “3-D streaming supplying partner protocols for mobile collaborative exergaming for health,” *IEEE Trans. Inf. Technol. Biomed. Publ. IEEE Eng. Med. Biol. Soc.*, vol. 16, no. 6, pp. 1079–1095, Nov. 2012, doi: 10.1109/TITB.2012.2206116.

[14] M. Fleury, D. Kanellopoulos, and N. N. Qadri, “Video streaming over MANETs: An overview of techniques,” *Multimed. Tools Appl.*, vol. 78, no. 16, pp. 23749–23782, Aug. 2019, doi: 10.1007/s11042-019-7679-0.

[15] N. Kasenides and N. Paspallis, “A Systematic Mapping Study of MMOG Backend Architectures,” *Inf. Switz.*, vol. 10, p. 264, Aug. 2019, doi: 10.3390/info10090264.

[16] A. Qureshi, H. Rifa-Pous, and D. Megias, “State-of-the-art, challenges and open issues in integrating security and privacy in P2P content distribution systems,” in *2016 Eleventh International Conference on Digital Information Management (ICDIM)*, Sep. 2016, pp. 1–9. doi: 10.1109/ICDIM.2016.7829784.

[17] J.-H. Cho, A. Swami, and I.-R. Chen, “A Survey on Trust Management for Mobile Ad Hoc Networks,” *IEEE Commun. Surv. Tutor.*, vol. 13, no. 4, pp. 562–583, 2011, doi: 10.1109/SURV.2011.092110.00088.

[18] D. Gambetta, “Review of Trust: Making and Breaking Cooperative Relations,” *Econ. J.*, vol. 99, no. 394, pp. 201–203, 1989, doi: 10.2307/2234217.

[19] L. M. Lucas, “The impact of trust and reputation on the transfer of best practices,” *J Knowl Manag*, vol. 9, no. 4, pp. 87–101, 2005, doi: 10.1108/13673270510610350.

[20] A. Bhattacherjee, “Individual Trust in Online Firms: Scale Development and Initial Test,” *J. Manag. Inf. Syst.*, vol. 19, no. 1, pp. 211–241, Jul. 2002.

[21] K. Blomqvist and P. Ståhle, “Trust in technology partnerships,” in *Trust in knowledge management and systems in organizations*, USA: IGI Global, 2004, pp. 173–199.

[22] D. Rousseau, S. Sitkin, R. Burt, and C. Camerer, “Not So Different After All: A Cross-Discipline View Of Trust,” 1998, doi: 10.5465/AMR.1998.926617.

[23] “Trust Definition & Meaning - Merriam-Webster.” https://www.merriam-webster.com/dictionary/trust (accessed Dec. 25, 2021).

[24] “Reputation | Definition of Reputation by Merriam-Webster.” https://www.merriam-webster.com/dictionary/reputation (accessed Nov. 11, 2021).

[25] "Reputation," *Wikipedia*. Aug. 13, 2021. Accessed: Nov. 11, 2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Reputation&oldid=1038633499

[26] "What is reputation?" https://blog.reputationx.com/whats-reputation (accessed Nov. 11, 2021).

[27] A. Abdul-Rahman and S. Hailes, "Supporting trust in virtual communities," in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, Jan. 2000, p. 9 pp. vol.1-. doi: 10.1109/HICSS.2000.926814.

[28] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Comput. Surv.*, vol. 45, no. 4, pp. 1–33, Aug. 2013, doi: 10.1145/2501654.2501661.

[29] G. Wang and J. Wu, "Multi-dimensional evidence-based trust management with multi-trusted paths," *Future Gener. Comput. Syst.*, vol. 27, no. 5, pp. 529–538, May 2011, doi: 10.1016/j.future.2010.04.015.

[30] R. S. Miller, *Intimate relationships*, Seventh edition. New York, NY: McGraw-Hill, 2015.

[31] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and analysis of online social networks," in *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement - IMC '07*, San Diego, California, USA, 2007, pp. 29–42. doi: 10.1145/1298306.1298311.

[32] S. Song, K. Hwang, R. Zhou, and Y.-K. Kwok, "Trusted P2P Transactions with Fuzzy Reputation Aggregation," *Internet Comput. IEEE*, vol. 9, pp. 24–34, Dec. 2005, doi: 10.1109/MIC.2005.136.

[33] X. Tong, W. Zhang, Y. Long, and H. Huang, "Subjectivity and Objectivity of Trust," in *Agents and Data Mining Interaction*, Berlin,

Heidelberg, 2013, vol. 7607, pp. 105–114. doi: 10.1007/978-3-642-36288-0_10.

[34] S. Hamdi, A. Bouzeghoub, A. L. Gancarski, and S. B. Yahia, "Trust Inference Computation for Online Social Networks," in *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Jul. 2013, pp. 210–217. doi: 10.1109/TrustCom.2013.240.

[35] C. J. Fung, J. Zhang, I. Aib, R. Boutaba, and S. Member, "Dirichlet-based trust management for effective collaborative intrusion detection networks," *IEEE Trans Netw. Serv. Manag.*, vol. 8, no. 2, pp. 79–91, 2011.

[36] K. Mukherjee and N. Banerjee, "Effect of Social Networking Advertisements on Shaping Consumers' Attitude," *Glob. Bus. Rev.*, vol. 18, no. 5, pp. 1291–1306, Oct. 2017, doi: 10.1177/0972150917710153.

[37] M. Jiang, "Behavior Modeling in Social Networks," in *Encyclopedia of Social Network Analysis and Mining*, R. Alhajj and J. Rokne, Eds. New York, NY: Springer, 2017, pp. 1–11. doi: 10.1007/978-1-4614-7163-9_110203-1.

[38] G. Danezis and P. Mittal, "SybilInfer: Detecting Sybil Nodes using Social Networks."

[39] W. Wei, F. Xu, C. C. Tan, and Q. Li, "Sybildefender: Defend against sybil attacks in large social networks," in *In IEEE INFOCOM*, 2012, pp. 1951–1959.

[40] H. Yu, M. Kaminsky, P. B. Gibbons, and F. Xiao, "SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks," p. 15.

[41] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: defending against sybil attacks via social networks," in *Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications*, 2006, vol. 16, pp. 267–278.

[42] J. Golbeck and J. Hendler, “FilmTrust: movie recommendations using trust in web-based social networks,” in *CCNC 2006. 2006 3rd IEEE Consumer Communications and Networking Conference, 2006.*, Las Vegas, NV, USA, 2006, vol. 2006, pp. 282–286. doi: 10.1109/CCNC.2006.1593032.

[43] T. DuBois, J. Golbeck, and A. Srinivasan, “Rigorous Probabilistic Trust-Inference with Applications to Clustering,” in *2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology*, Milan, Italy, 2009, pp. 655–658. doi: 10.1109/WI-IAT.2009.109.

[44] H. Liu *et al.*, “Predicting Trusts among Users of Online Communities - An Epinions Case Study,” *ACM Conf. Electron. Commer.*, pp. 310–319, 2008.

[45] S. Nepal, W. Sherchan, and C. Paris, “STrust: A Trust Model for Social Networks,” in *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, Nov. 2011, pp. 841–846. doi: 10.1109/TrustCom.2011.112.

[46] S. Trifunovic, F. Legendre, and C. Anastasiades, “Social Trust in Opportunistic Networks,” in *2010 INFOCOM IEEE Conference on Computer Communications Workshops*, Mar. 2010, pp. 1–6. doi: 10.1109/INFCOMW.2010.5466696.

[47] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, “The EigenTrust Algorithm for Reputation Management in P2P Networks,” p. 12.

[48] Z. Gyöngyi, H. Garcia-Molina, and J. O. Pedersen, “Combating Web Spam with TrustRank,” 2004. doi: 10.1016/B978-012088469-8.50052-8.

[49] G. Vogiatzis, I. MacGillivray, and M. Chli, “A probabilistic model for trust and reputation,” p. 8.

[50] E. Elsalamouny, V. Sassone, and M. Nielsen, "HMM-based trust model," in *Formal Aspects in Security and Trust*, Berlin, Heidelberg, Nov. 2009, vol. 5983. doi: 10.1007/978-3-642-12459-4_3.

[51] X. Liu and A. Datta, "Modeling Context-Aware Dynamic Trust Using Hidden Markov Model," p. 7.

[52] A. Jøsang, "A LOGIC FOR UNCERTAIN PROBABILITIES," *World Sci. Publ. Co.*, vol. 9, no. 3, p. 33, 2001.

[53] W. T. L. Teacy, M. Luck, A. Rogers, and N. R. Jennings, "An efficient and versatile approach to trust and reputation using hierarchical Bayesian modelling," *Artif. Intell.*, vol. 193, pp. 149–185, Dec. 2012, doi: 10.1016/j.artint.2012.09.001.

[54] S. Tu, "The Dirichlet-Multinomial and Dirichlet-Categorical models for Bayesian inference," *Comput. Sci. Div.*, p. 6, 2014.

[55] G. Shafer, "A mathematical theory of evidence," in *BULLETIN OF THE AMERICAN MATHEMATICAL SOCIETY*, 1976, vol. 83, p. 06. doi: 10.2307/1268172.

[56] Y. Wang, C. Hang, and M. P. Singh, "A Probabilistic Approach for Maintaining Trust Based on Evidence," *J. Artif. Intell. Res.*, vol. 40, pp. 221–267, Jan. 2011, doi: 10.1613/jair.3108.

[57] A. Jøsang, S. Marsh, and S. Pope, "Exploring Different Types of Trust Propagation," 2006.

[58] A. Jøsang, "The Consensus Operator for Combining Beliefs," *Artif. Intell.*, vol. 141, pp. 157–170, Oct. 2002, doi: 10.1016/S0004-3702(02)00259-X.

[59] R. C. Cardoso, A. J. P. Gomes, and M. M. Freire, "A User Trust System for Online Games—Part I: An Activity Theory Approach for Trust Representation," *IEEE Trans. Comput. Intell. AI Games*, vol. 9, no. 3, pp. 305–320, Sep. 2017, doi: 10.1109/TCIAIG.2016.2592965.

[60] R. C. Cardoso, A. J. P. Gomes, and M. M. Freire, “A User Trust System for Online Games—Part II: A Subjective Logic Approach for Trust Inference,” *IEEE Trans. Comput. Intell. AI Games*, vol. 9, no. 4, pp. 354–368, Dec. 2017, doi: 10.1109/TCIAIG.2016.2593000.

[61] G. Liu, Q. Yang, H. Wang, and A. X. Liu, “Trust Assessment in Online Social Networks,” *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 2, pp. 994–1007, Mar. 2021, doi: 10.1109/TDSC.2019.2916366.

[62] G. Liu, C. Li, and Q. Yang, “NeuralWalk: Trust Assessment in Online Social Networks with Neural Networks,” in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, Paris, France, Apr. 2019, pp. 1999–2007. doi: 10.1109/INFOCOM.2019.8737469.

[63] T. Cheng, G. Liu, Q. Yang, and J. Sun, “Trust Assessment in Vehicular Social Network Based on Three-Valued Subjective Logic,” *IEEE Trans. Multimed.*, vol. 21, no. 3, pp. 652–663, Mar. 2019, doi: 10.1109/TMM.2019.2891417.

[64] G. Liu, Q. Chen, Q. Yang, B. Zhu, H. Wang, and W. Wang, “OpinionWalk: An efficient solution to massive trust assessment in online social networks,” in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, May 2017, pp. 1–9. doi: 10.1109/INFOCOM.2017.8057106.

[65] H. A. Kurdi, “HonestPeer: An enhanced EigenTrust algorithm for reputation management in P2P systems,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 27, no. 3, pp. 315–322, Jul. 2015, doi: 10.1016/j.jksuci.2014.10.002.

[66] S. Alkharji, H. Kurdi, R. Altamimi, and E. Aloboud, “AuthenticPeer++: A Trust Management System for P2P Networks,” in *2017 European Modelling Symposium (EMS)*, Nov. 2017, pp. 191–196. doi: 10.1109/EMS.2017.41.

[67] L. Xiong and L. Liu, “PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities,” *IEEE Trans. Knowl. Data Eng.*,

vol. 16, no. 7, pp. 843–857, Jul. 2004, doi: 10.1109/TKDE.2004.1318566.

[68] D. Kaur and J. SenGupta, "Proposed P2P Trust and Reputation-based Model to Secure Grid," *Int. Conf. Recent Adv. Future Trends Inf. Technol.*, p. 6, 2012.

[69] R. Chen, X. Zhao, L. Tang, J. Hu, and Z. Chen, "CuboidTrust: A Global Reputation-Based Trust Model in Peer-to-Peer Networks," in *Autonomic and Trusted Computing*, Berlin, Heidelberg, 2007, pp. 203–215. doi: 10.1007/978-3-540-73547-2_22.

[70] R. Zhou and K. Hwang, "PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 18, no. 4, pp. 460–473, Apr. 2007, doi: 10.1109/TPDS.2007.1021.

[71] R. Gupta and Y. N. Singh, "Reputation Aggregation in Peer-to-Peer Network Using Differential Gossip Algorithm," *IEEE Trans. Knowl. Data Eng.*, vol. 27, no. 10, pp. 2812–2823, Oct. 2015, doi: 10.1109/TKDE.2015.2427793.

[72] R. Gaeta and M. Grangetto, "Identification of Malicious Nodes in Peer-to-Peer Streaming: A Belief Propagation-Based Technique," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 10, pp. 1994–2003, Oct. 2013, doi: 10.1109/TPDS.2012.342.

[73] E. Ayday and F. Fekri, "BP-P2P: Belief propagation-based trust and reputation management for P2P networks," in *2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, Jun. 2012, pp. 578–586. doi: 10.1109/SECON.2012.6275830.

[74] H. Zhao and X. Li, "VectorTrust: Trust Vector Aggregation Scheme for Trust Management in Peer-to-Peer Networks," in *2009 Proceedings of 18th International Conference on Computer Communications and Networks*, Aug. 2009, pp. 1–6. doi: 10.1109/ICCCN.2009.5235290.

[75] H. Lin, X. Wu, and H. Lin, "Hierarchical fuzzy trust management for peer-to-peer network," in *2009 ISECS International Colloquium on Computing, Communication, Control, and Management*, Aug. 2009, vol. 4, pp. 377–380. doi: 10.1109/CCCM.2009.5270416.

[76] R. Andersen, F. Chung, and K. Lang, "Local Partitioning for Directed Graphs Using PageRank," in *Algorithms and Models for the Web-Graph*, Berlin, Heidelberg, 2007, pp. 166–178. doi: 10.1007/978-3-540-77004-6_13.

[77] A. Josang, R. Hayward, and S. Pope, "Trust network analysis with subjective logic," in *Conference Proceedings of the Twenty-Ninth Australasian Computer Science Conference (ACSW 2006)*, 2006, pp. 85–94.

[78] A. Jøsang and T. Bhuiyan, "Optimal Trust Network Analysis with Subjective Logic," in *International Conference on Emerging Security Information, Systems and Technologies*, Sep. 2008, pp. 179–184. doi: 10.1109/SECURWARE.2008.64.

[79] P. Massa and P. Avesani, "Controversial users demand local trust metrics: an experimental study on Epinions.com community," in *Proceedings of the 20th national conference on Artificial intelligence - Volume 1*, Pittsburgh, Pennsylvania, Jul. 2005, pp. 121–126.

[80] "Free and Open-Source Tool for Social Network Analysis," *Social Network Visualizer*. https://socnetv.org/ (accessed Nov. 11, 2021).

[81] "Network visualisation & analysis - CVCE Website," *Network visualization and analysis*. https://www.cvce.eu/en/digital-innovation/projects/netviz (accessed Nov. 11, 2021).

[82] "Graphviz," *Graphviz*. https://graphviz.org/ (accessed Nov. 11, 2021).

[83] "NetworkX — NetworkX documentation," *Network Analysis in Python*. https://networkx.org/ (accessed Nov. 11, 2021).

[84] "Security, Cloud Delivery, Performance | Akamai," *Akamai*, 1998. https://www.akamai.com/ (accessed Nov. 12, 2021).

[85] "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies - The Washington Post." https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html (accessed Nov. 12, 2021).

[86] "China blamed after ASIO blueprints stolen in the major cyber attack," *ABC News*, May 27, 2013. https://www.abc.net.au/news/2013-05-27/asio-blueprints-stolen-in-major-hacking-operation/4715960 (accessed Nov. 12, 2021).

[87] "In China, a Skyscraper-Sized Knock-Off | Studio 360," *WNYC*, 2013. https://www.wnyc.org/story/269375-in-china-a-skyscraper-sized-knock-off/ (accessed Nov. 12, 2021).

[88] A. Jolfaei, X.-W. Wu, and V. Muthukkumarasamy, "A 3D Object Encryption Scheme Which Maintains Dimensional and Spatial Stability," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 2, pp. 409–422, Feb. 2015, doi: 10.1109/TIFS.2014.2378146.

[89] E. E. García-Guerrero, E. Inzunza-González, O. R. López-Bonilla, J. R. Cárdenas-Valdez, and E. Tlelo-Cuautle, "Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channels," *Chaos Solitons Fractals*, vol. 133, p. 109646, Apr. 2020, doi: 10.1016/j.chaos.2020.109646.

[90] H. Liu, A. Kadir, and Y. Li, "Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys," *Optik*, vol. 127, no. 19, pp. 7431–7438, Oct. 2016, doi: 10.1016/j.ijleo.2016.05.073.

[91] "Real-time selective video encryption based on the chaos system in scalable HEVC extension - ScienceDirect." https://www.sciencedirect.com/science/article/pii/S0923596517301145?casa_token=n6K2ra2efkwAAAAA:d3ruPMqV0VZ7xhZ-8NaVO5PfRZ3uhOAK_SpG7fvlAeTHvMpp6gEucWeJeOI6D9K5ckT7SzMemcqK-Q (accessed Dec. 30, 2021).

[92] D. Megías, M. Kuribayashi, and A. Qureshi, "Survey on Decentralized Fingerprinting Solutions: Copyright Protection through Piracy Tracing," *Computers*, vol. 9, no. 2, Art. no. 2, Jun. 2020, doi: 10.3390/computers9020026.

[93] E. Diehl, "Digital Cinema," in *Securing Digital Video: Techniques for DRM and Content Protection*, E. Diehl, Ed. Berlin, Heidelberg: Springer, 2012, pp. 189–192. doi: 10.1007/978-3-642-17345-5_10.

[94] E. Chen and W.-C. Wu, "An anonymous DRM scheme for sharing multimedia files in P2P networks," *Multimed. Tools Appl.*, vol. 69, no. 3, pp. 1041–1065, Apr. 2014, doi: 10.1007/s11042-012-1166-1.

[95] S. PARUL SANJAY, JHAJHARIA, *CASES IN MANAGEMENT- Buy CASES IN MANAGEMENT Online at Best Prices in India - Phindia.com*. Prentice-Hall of India Ltd, 2011. Accessed: Nov. 12, 2021. [Online]. Available: https://www.phindia.com/Books/BookDetail/9788120341586/cases-in-management-srivastava-jhajharia

[96] M.-K. Sun, C.-S. Laih, H.-Y. Yen, and J.-R. Kuo, "A Ticket Based Digital Rights Management Model," in *2009 6th IEEE Consumer Communications and Networking Conference*, Jan. 2009, pp. 1–5. doi: 10.1109/CCNC.2009.4784774.

[97] Y. Sun, "Rightholder as the Center: The DRM System in Copyright after so Many Years," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2430424, Apr. 2014. doi: 10.2139/ssrn.2430424.

[98] D. Megías and A. Qureshi, "Collusion-resistant and privacy-preserving P2P multimedia distribution based on recombined fingerprinting," *Expert Syst. Appl.*, vol. 71, pp. 147–172, Apr. 2017, doi: 10.1016/j.eswa.2016.11.015.

[99] M. Kuribayashi and N. Funabiki, "Decentralized tracing protocol for the fingerprinting system," *APSIPA Trans. Signal Inf. Process.*, vol. 8, ed 2019, doi: 10.1017/ATSIP.2018.28.

[100] M. Sabir, T. M. Khan, M. Arshad, and S. Munawar, "Reducing computational complexity in fingerprint matching," vol. 28, no. 5, pp. 2538–2551, 2020.

[101] D. Dhaou, S. Ben Jabra, and E. Zagrouba, "A Review on Anaglyph 3D Image and Video Watermarking," *3D Res.*, vol. 10, no. 2, p. 13, Jun. 2019, doi: 10.1007/s13319-019-0223-1.

[102] L. Rzouga Haddada, B. Dorizzi, and N. Essoukri Ben Amara, "A combined watermarking approach for securing biometric data," *Signal Process. Image Commun.*, vol. 55, pp. 23–31, Jul. 2017, doi: 10.1016/j.image.2017.03.008.

[103] Amirtharajan R, Qin J, and Rayappan JB, "Random image steganography and steganalysis: Present status and future directions," *Inf. Technol J*, vol. 11, no. 5, p. 10, 2012.

[104] S. P. Mohanty, A. Sengupta, P. Guturu, and E. Kougianos, "Everything You Want to Know About Watermarking: From Paper Marks to Hardware Protection: From paper marks to hardware protection.," *IEEE Consum. Electron. Mag.*, vol. 6, no. 3, pp. 83–91, Jul. 2017, doi: 10.1109/MCE.2017.2684980.

[105] T.-S. Nguyen, C.-C. Chang, and X.-Q. Yang, "A reversible image authentication scheme based on fragile watermarking in the discrete wavelet transform domain," *AEU - Int. J. Electron. Commun.*, vol. 70, no. 8, pp. 1055–1061, Aug. 2016, doi: 10.1016/j.aeue.2016.05.003.

[106] R. Thanki and K. Borisagar, “Sparse Watermarking Technique for Improving Security of Biometric System,” *Procedia Comput. Sci.*, vol. 70, pp. 251–258, Jan. 2015, doi: 10.1016/j.procs.2015.10.083.

[107] H. Al-Otum, “Semi-fragile Watermarking for Grayscale Image Authentication and Tamper Detection Based on an Adjusted Expanded-Bit Multiscale Quantization-Based Technique,” *J. Vis. Commun. Image Represent.*, vol. 25, Jul. 2014, doi: 10.1016/j.jvcir.2013.12.017.

[108] I. A. Ansari and M. Pant, “Multipurpose image watermarking in the domain of DWT based on SVD and ABC,” *Pattern Recognit. Lett.*, vol. 94, pp. 228–236, Jul. 2017, doi: 10.1016/j.patrec.2016.12.010.

[109] Y. Wang, J. Liu, Y. Yang, D. Ma, and R. Liu, “3D model watermarking algorithm robust to geometric attacks,” *IET Image Process.*, vol. 11, no. 10, pp. 822–832, Oct. 2017, doi: 10.1049/iet-ipr.2016.0927.

[110] P. Singh, A. Agarwal, and J. Gupta, “Image Watermark Attacks: Classification & Implementation,” vol. 4, no. 2, p. 6, 2013.

[111] S. Rai, R. Boghey, D. Shahane, and P. Saxena, “Digital Image Watermarking Against Geometrical Attack,” in *Data, Engineering and Applications: Volume 2*, R. K. Shukla, J. Agrawal, S. Sharma, and G. Singh Tomer, Eds. Singapore: Springer, 2019, pp. 129–145. doi: 10.1007/978-981-13-6351-1_12.

[112] A. M. Cheema, S. M. Adnan, and Z. Mehmood, “A Novel Optimized Semi-Blind Scheme for Color Image Watermarking,” *IEEE Access*, vol. 8, pp. 169525–169547, 2020, doi: 10.1109/ACCESS.2020.3024181.

[113] A. E. Aydemir, A. Temizel, and T. T. Temizel, “The Effects of JPEG and JPEG2000 Compression on Attacks using Adversarial Examples,” p. 4.

[114] N. Hasan, M. S. Islam, W. Chen, M. A. Kabir, and S. Al-Ahmadi, “Encryption Based Image Watermarking Algorithm in 2DWT-DCT Domains,” *Sensors*, vol. 21, no. 16, p. 5540, Aug. 2021, doi: 10.3390/s21165540.

[115] M. Begum and M. S. Uddin, “Analysis of Digital Image Watermarking Techniques through Hybrid Methods,” *Adv. Multimed.*, vol. 2020, p. e7912690, Aug. 2020, doi: 10.1155/2020/7912690.

[116] M. Begum and M. S. Uddin, “Digital Image Watermarking Techniques: A Review,” *Information*, vol. 11, no. 2, Art. no. 2, Feb. 2020, doi: 10.3390/info11020110.

[117] A. F. Qasim, F. Meziane, and R. Aspin, “Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review,” *Comput. Sci. Rev.*, vol. 27, pp. 45–60, Feb. 2018, doi: 10.1016/j.cosrev.2017.11.003.

[118] S. Koley, “Hardware Implementation of a Fast 3D Anaglyph Image Watermarking Framework for Integration in Consumer Electronics Devices,” in *2020 Zooming Innovation in Consumer Technologies Conference (ZINC)*, May 2020, pp. 40–45. doi: 10.1109/ZINC50678.2020.9161783.

[119] N. Tarhouni, M. Charfeddine, and C. Ben Amar, “Novel and Robust Image Watermarking for Copyright Protection and Integrity Control,” *Circuits Syst. Signal Process.*, vol. 39, no. 10, pp. 5059–5103, Oct. 2020, doi: 10.1007/s00034-020-01401-1.

[120] G. Bhatnagar, J. Wu, and B. Raman, “A robust security framework for 3D images,” *J. Vis.*, vol. 14, no. 1, pp. 85–93, 2011.

[121] D. Dhaou, S. Ben Jabra, and E. Zagrouba, “An Efficient Anaglyph 3D Video Watermarking Approach Based on Hybrid Insertion,” in *Computer Analysis of Images and Patterns*, Cham, 2019, vol. 11679, pp. 96–107. doi: 10.1007/978-3-030-29891-3_9.

[122] R. Singh, D. Shaw, and M. Alam, “Experimental Studies of LSB Watermarking with Different Noise,” *Procedia Comput. Sci.*, vol. 54, pp. 612–620, Dec. 2015, doi: 10.1016/j.procs.2015.06.071.

[123] A. K. Singh, M. Dave, and A. Mohan, “Hybrid technique for robust and imperceptible multiple watermarking using medical images,” *Multimed. Tools Appl.*, vol. 75, no. 14, pp. 8381–8401, 2016.

[124] F. Y. Shih, X. Zhong, I.-C. Chang, and S. Satoh, “An adjustable-purpose image watermarking technique by particle swarm optimization,” *Multimed. Tools Appl.*, vol. 77, no. 2, pp. 1623–1642, 2018.

[125] S. Ben Jabra and E. Zagrouba, “Robust anaglyph 3D video watermarking based on the cyan mosaic generation and DCT insertion in Krawtchouk moments,” *Vis. Comput.*, Jun. 2021, doi: 10.1007/s00371-021-02191-6.

[126] H. Devi and K. Singh, “A robust and optimized 3D red-cyan anaglyph blind image watermarking in the DWT domain,” *Contemp. Eng. Sci.*, vol. 9, pp. 1575–1589, Jan. 2016, doi: 10.12988/ces.2016.69156.

[127] M. Abdullatif, A. M. Zeki, J. Chebil, and T. S. Gunawan, “Properties of digital image watermarking,” in *2013 IEEE 9th international colloquium on signal processing and its applications*, 2013, pp. 235–240.

[128] C. Wang, F. Han, and X. Zhuang, “Robust Digital Watermarking Scheme of Anaglyphic 3D for RGB Color Images,” *Int. J. Image Process.*, vol. 9, no. 3, p. 10, 2015.

[129] B. Chen and G. W. Wornell, “Quantization index modulation: A class of provably good methods for digital watermarking and information embedding,” *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1423–1443, 2001.

[130] SRKIT, R. Y, and K. S. R. Krishna, “Digital Watermarked Anaglyph 3D Images Using FrFT,” *Int. J. Comput. Trends Technol.*, vol. 41, no. 2, pp. 77–80, Nov. 2016, doi: 10.14445/22312803/IJCTT-V41P113.

[131] D. O. Muñoz-Ramírez, R. Reyes-Reyes, V. Ponomaryov, and C. Cruz-Ramos, “Invisible digital color watermarking technique in anaglyph 3D images,” in *2015 12th International Conference on Electrical*

Engineering, Computing Science and Automatic Control (CCE), 2015, pp. 1–6.

[132] R. Patel and P. Bhatt, “Robust Watermarking for Anaglyph 3D images Using DWT Techniques,” *Int. J. Eng. Tech. Res.*, vol. 3, no. 6, p. 4, 2015.

[133] S. R. Zadokar, V. B. Raskar, and S. V. Shinde, “A digital watermarking for anaglyph 3D images,” in *2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2013, pp. 483–488. doi: 10.1109/ICACCI.2013.6637219.

[134] G. Kasana and S. S. Kasana, “Reference-based semi-blind image watermarking scheme in the wavelet domain,” *Optik*, vol. 142, pp. 191–204, Aug. 2017, doi: 10.1016/j.ijleo.2017.05.027.

[135] I. Prathap and R. Anitha, “Robust and blind watermarking scheme for three-dimensional anaglyph images,” *Comput. Electr. Eng.*, vol. 40, no. 1, pp. 51–58, Jan. 2014, doi: 10.1016/j.compeleceng.2013.11.005.

[136] “Steven Pinker.” https://stevenpinker.com/publications/how-mind-works-19972009 (accessed Dec. 30, 2021).

[137] P. W. Stoffer, E. Phillips, and P. Messina, “Anaglyph image technology as a visualization tool for teaching geology of national parks,” in *AGU Fall Meeting Abstracts*, 2003, vol. 2003, pp. ED32B-1198.

[138] H. Devi and K. Singh, “A Novel, Efficient, Robust, and Blind Imperceptible 3D Anaglyph Image Watermarking,” *Arab. J. Sci. Eng.*, vol. 42, pp. 1–13, Apr. 2017, doi: 10.1007/s13369-017-2531-1.

[139] S. Abid, J. Waleed, H. Jun, H. Hatem, and R. Majeed, “Integral Algorithm to Embed Imperceptible Watermark into Anaglyph 3D Video,” *IJACT*, vol. 5, pp. 163–173, Sep. 2013.

[140] J. Waleed, S. Abid, and T. Hasan, “Imperceptible 3D Video Watermarking Technique Based on Scene Change Detection,” *Int. J.*

Adv. Sci. Technol., vol. 82, pp. 11–22, Sep. 2015, doi: 10.14257/ijast.2015.82.02.

[141] D. Dhaou, S. Ben Jabra, and E. Zagrouba, “An Efficient Group of Pictures Decomposition based Watermarking for Anaglyph 3D Video,” in *International Conference on Computer Vision Theory and Applications*, Jan. 2018, vol. 4, pp. 501–510. doi: 10.5220/0006619305010510.

[142] D. Dhaou, S. Ben Jabra, and E. Zagrouba, “A Multi-sprite Based Anaglyph 3D Video Watermarking Approach Robust Against Collusion,” *3D Res.*, vol. 10, no. 2, p. 21, May 2019, doi: 10.1007/s13319-019-0231-1.

[143] D. Dhaou, S. Ben Jabra, and E. Zagrouba, “A Robust Anaglyph 3D Video Watermarking based on Multi-sprite Generation:” in *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications*, Prague, Czech Republic, 2019, pp. 260–267. doi: 10.5220/0007930102600267.

[144] A. Ometov *et al.*, “A Survey on Wearable Technology: History, State-of-the-Art and Current Challenges,” *Comput. Netw.*, vol. 193, p. 108074, Jul. 2021, doi: 10.1016/j.comnet.2021.108074.

[145] R. Biswas, S. R. Malreddy, and S. Banerjee, “A High-Precision Low-Area Unified Architecture for Lossy and Lossless 3D Multi-Level Discrete Wavelet Transform,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 9, pp. 2386–2396, Sep. 2018, doi: 10.1109/TCSVT.2017.2721113.

[146] A. A. Hagberg, D. A. Schult, and P. J. Swart, “Exploring Network Structure, Dynamics, and Function using NetworkX,” *SciPy Conf.*, p. 5, 2008.

[147] C. Thurau and C. Bauckhage, “Analyzing the Evolution of Social Groups in World of Warcraft®,” in *Proceedings of the 2010 IEEE*

Conference on Computational Intelligence and Games, Aug. 2010, pp. 170–177. doi: 10.1109/ITW.2010.5593358.

[148] A. Roy, C. Sarkar, J. Srivastava, and J. Huh, "Trustingness amp; trustworthiness: A pair of complementary trust measures in a social network," in *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, Aug. 2016, pp. 549–554. doi: 10.1109/ASONAM.2016.7752289.

[149] Z. H. Borbora, M. A. Ahmad, J. Oh, K. Z. Haigh, J. Srivastava, and Z. Wen, "Robust features of trust in social networks," *Soc. Netw. Anal. Min.*, vol. 3, no. 4, pp. 981–999, Dec. 2013, doi: 10.1007/s13278-013-0136-6.

[150] A. Hajibagheri, G. Sukthankar, K. Lakkaraju, H. Alvari, R. T. Wigand, and N. Agarwal, "Using Massively Multiplayer Online Game Data to Analyze the Dynamics of Social Interactions," in *Social Interactions in Virtual Worlds: An Interdisciplinary Perspective*, G. Sukthankar, K. Lakkaraju, and R. T. Wigand, Eds. Cambridge: Cambridge University Press, 2018, pp. 375–416. doi: 10.1017/9781316422823.015.

[151] C.-Y. Huang and W. C. B. Chin, "Distinguishing Arc Types to Understand Complex Network Strength Structures and Hierarchical Connectivity Patterns," *IEEE Access*, vol. 8, pp. 71021–71040, 2020, doi: 10.1109/ACCESS.2020.2986017.

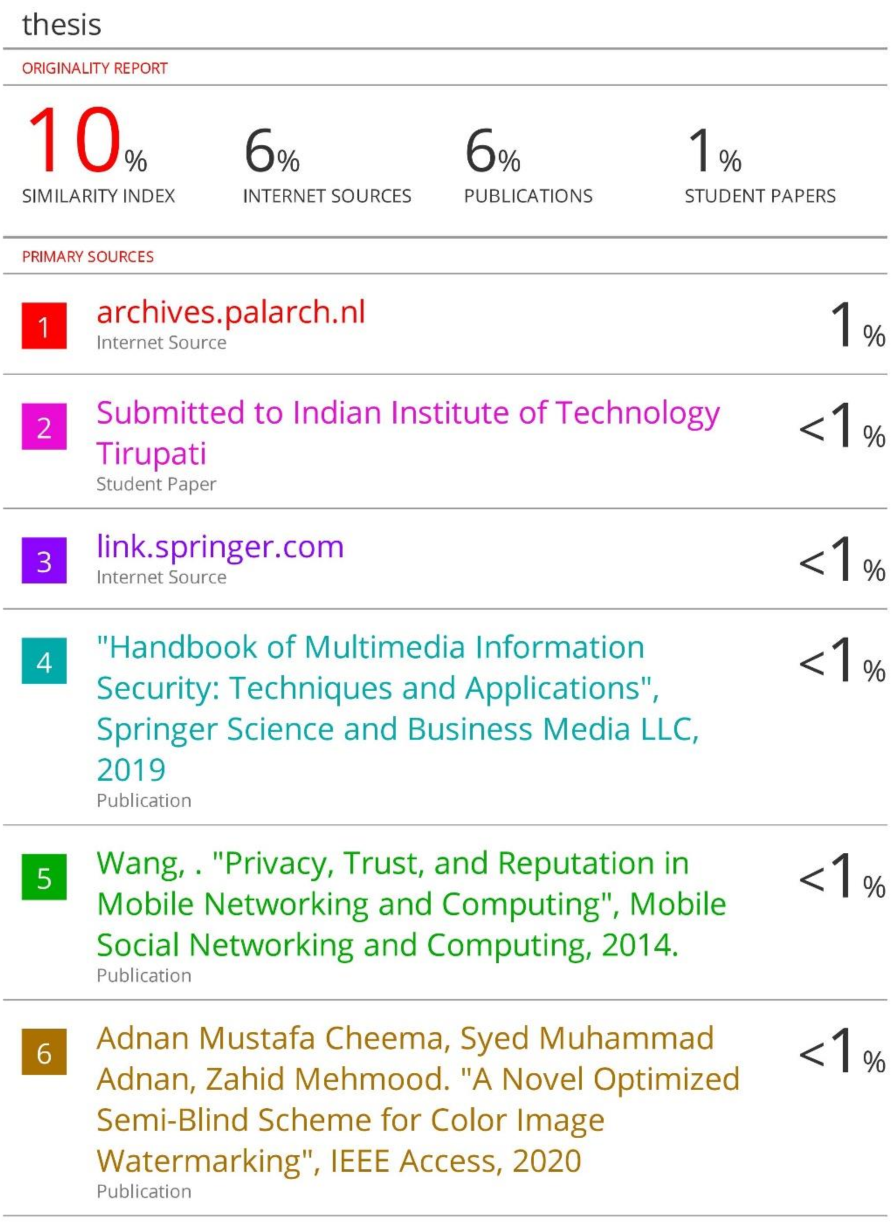
[152] U. N. Raghavan, R. Albert, and S. Kumara, "Near linear time algorithm to detect community structures in large-scale networks," *Phys. Rev. E*, vol. 76, no. 3, p. 036106, Sep. 2007, doi: 10.1103/PhysRevE.76.036106.

[153] W. J. Boone, "Rasch Analysis for Instrument Development: Why, When, and How?," *CBE—Life Sci. Educ.*, vol. 15, no. 4, p. rm4, Dec. 2016, doi: 10.1187/cbe.16-04-0148.

[154] "vision.middlebury.edu/stereo/data." https://vision.middlebury.edu/stereo/data/ (accessed Dec. 30, 2021).

[155] Y. Rai, J. Gutiérrez, and P. Le Callet, “A Dataset of Head and Eye Movements for 360 Degree Images,” in *Proceedings of the 8th ACM on Multimedia Systems Conference*, Taipei Taiwan, Jun. 2017, pp. 205–210. doi: 10.1145/3083187.3083218.

[156] E. Najafi, “A robust embedding and blind extraction of image watermarking based on discrete wavelet transform,” *Math. Sci.*, vol. 11, no. 4, pp. 307–318, Dec. 2017, doi: 10.1007/s40096-017-0233-1.



thesis

ORIGINALITY REPORT

10%	6%	6%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	archives.palarch.nl Internet Source	1%
2	Submitted to Indian Institute of Technology Tirupati Student Paper	<1%
3	link.springer.com Internet Source	<1%
4	"Handbook of Multimedia Information Security: Techniques and Applications", Springer Science and Business Media LLC, 2019 Publication	<1%
5	Wang, . "Privacy, Trust, and Reputation in Mobile Networking and Computing", Mobile Social Networking and Computing, 2014. Publication	<1%
6	Adnan Mustafa Cheema, Syed Muhammad Adnan, Zahid Mehmood. "A Novel Optimized Semi-Blind Scheme for Color Image Watermarking", IEEE Access, 2020 Publication	<1%