

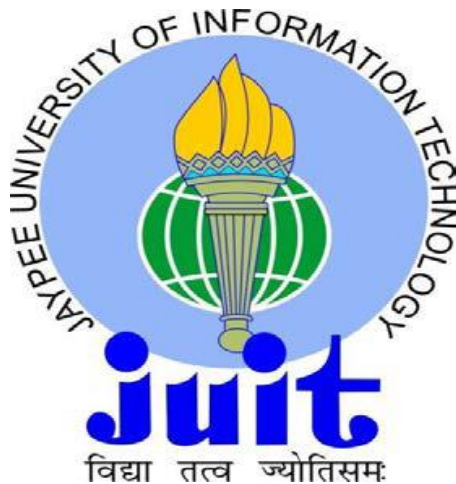
ROBUST & IMPERCEPTIBLE WATERMARKING TECHNIQUES FOR MULTIMEDIA DATA

*Thesis submitted in fulfillment of the requirements for the
Degree of*

DOCTOR OF PHILOSOPHY

By

NAMITA AGARWAL



Department of Computer Science Engineering and Information Technology

**JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY
WAKNAGHAT, SOLAN-173234, HIMACHAL PRADESH, INDIA**

January, 2022

**@ Copyright JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY
WAKNAGHAT**

January, 2022

ALL RIGHTS RESERVED

Table of Contents

DECLARATION BY THE SCHOLAR	i
SUPERVISOR’S CERTIFICATE	ii
ACKNOWLEDGEMENT	iii
LIST OF ACRONYMS & ABBREVIATIONS	iv-vi
LIST OF FIGURES	vii-viii
LIST OF TABLES	ix-x
ABSTRACT	xi

CHAPTER 1

INTRODUCTION	2-14
1.1 Characteristics of watermarking	2
1.2 Applications of watermarking	4
1.3 Watermarking embedding/extraction process	6
1.4 Classification of watermarking	7
1.4.1 Watermarking domain techniques	8
1.5 Watermarking performance metrics	9
1.6 Watermarking attacks	11
1.7 Research objectives and contributions	12
1.8 Thesis organization	14

CHAPTER 2

LITERATURE SURVEY	16-43
2.1 Review of related research	17
2.1.1 Domain-based watermarking.....	17
2.1.2 Encryption-based watermarking.....	27
2.1.3 Optimization-based watermarking	30
2.2 Comparative analysis transform domain watermarking	35
2.2.1 Structure of digital image watermarking	35
2.3 Preliminaries of transform domain watermarking	36
2.4 Experimental setup	41

CHAPTER 3

ROBUST AND SECURE COLOR IMAGE WATERMARKING WITH PAILLIER CRYPTOSYSTEM AND ARNOLD TRANSFORMATION	45-55
3.1 Introduction	45
3.2 Paillier homomorphic cryptosystem	47

3.2.1 Key generation steps.....	47
3.2.2 Encryption	47
3.2.3 Decryption	47
3.3 Arnold transformation	48
3.4 Proposed Paillier homomorphic cryptosystem-based watermarking	48
3.4.1 Steps for embedding	49
3.4.2 Steps for extraction.....	50
3.5 Experimental outcomes	51

CHAPTER 4

DCT AND GENETIC ALGORITHM BASED WATERMARKING METHOD FOR COLOR IMAGES.....57-77

4.1 Introduction	57
4.2 Watermarking with genetic algorithm	58
4.3 Designed method	60
4.3.1 Steps for embedding	62
4.3.2 Steps for extraction.....	62
4.4 Experimental study.....	63
4.4.1 YCbCr color space	69
4.4.2 YIQ color space	73

CHAPTER 5

AN EFFECTIVE MULTIPLE WATERMARKING USING TRANSFORM DOMAIN METHODS WITH WAVELET FUSION FOR DIGITAL MEDIA.....79-92

5.1 Introduction	79
5.2 Proposed method	81
5.2.1 With Wavelet Fusion Technique	81
5.2.2 Experimental analysis.....	84
5.2.3 Multiple watermarking with transform domain	87
5.2.4 Experimental analysis.....	89

CHAPTER 6

CONCLUSION AND FUTURE SCOPE.....94-95

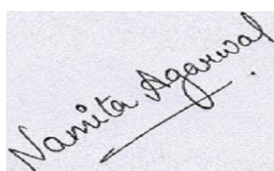
LIST OF PUBLICATIONS

REFERENCES.....99-112

APPENDIX-A..... 113

DECLARATION BY THE SCHOLAR

I hereby declare that the work reported in the Ph.D. thesis entitled “**Robust & Imperceptible Watermarking Techniques for Multimedia Data**” submitted at **Jaypee University of Information Technology, Wagnaghat, India**, is an authentic record of my work carried out under the supervision of **Dr. Amit Kumar and Dr. Pradeep Kumar Singh**. I have not submitted this work elsewhere for any other degree or diploma. I am fully responsible for the contents of my Ph.D. Thesis.

A photograph of a handwritten signature in black ink on a light-colored background. The signature reads "Namita Agarwal" in a cursive script, with a horizontal line drawn underneath the name.

Namita Agarwal

Enrollment No.: 176205

Department of Computer Science Engineering and Information Technology

Jaypee University of Information Technology,

Wagnaghat, Solan-173234, Himachal Pradesh, India

Date: 15-01-2022



JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY

(Established by H.P. State Legislative vide Act No. 14 of 2002)

P.O. Wagnaghat, Teh. Kandaghat, Distt. Solan - 173234 (H.P.) INDIA

Website: www.juit.ac.in

Phone No. (91) 01792-257999

Fax: +91-01792-245362

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the Ph.D. thesis entitled “**Robust & Imperceptible Watermarking Techniques for Multimedia Data**”, submitted by **Namita Agarwal** at **Jaypee University of Information Technology, Wagnaghat, India**, is a bonafide record of his original work carried out under our supervision. This work has not been submitted elsewhere for any other degree or diploma.

(Signature of Supervisor 1)

Dr. Amit Kumar
Assistant Professor (SG)
Department of CSE & IT
JUIT, Wagnaghat, Solan, India

(Signature of Supervisor 2)

Dr. Pradeep Kumar Singh
HOD & Professor
Department of Computer Science
KIET Group of Institutions
Ghaziabad, UP, India

ACKNOWLEDGEMENT

My first and foremost thanks to **Almighty God** for providing me the strength and blessings throughout this journey. Now, I would like to extend my foremost gratitude and special thanks to my Ph.D. supervisors **Dr. Amit Kumar and Dr. Pradeep Kumar Singh** for their tremendous encouragement, support and guidance in my research work. **Dr. Amit Kumar**, Assistant Professor (Sr. Grade), JUIT Waknaghat, has always helped me with his perseverance and constructive criticism. **Dr. Pradeep Kumar Singh**, Professor and Head, KIET Ghaziabad, has always fortified me by his careful guidance and positive feedback during this entire PhD work. They both have always supported and guided me to the right path, inspiring me for the successful completion of my research work. I have been blessed with their continuous moral support, invaluable inputs and suggestions when I needed the most.

I gratefully acknowledge JUIT for offering me the platform for this research and providing the necessary facilities and support. I would like to thank the JUIT authorities for providing such great facilities and resources to conduct my research work. My heartfelt appreciation to **Prof. (Dr.) Vivek Kumar Sehgal**, Head of Department of CSE & IT, for his co-operation, support and constant encouragement. I wish to convey my sincere thanks to all the faculty members of Department of CSE & IT, for their help and guidance at the various stages of this study. It is my pleasure to acknowledge the timely help of the members of technical staff of the department, for always providing the technical support. I am also thankful to my DPMC members **Dr. Vivek Sehgal, Dr. Yugal Kumar and Dr. Rakesh Bajaj** for their guidance and valuable suggestions throughout my research work.

This work has not been possible without the blessings of my family throughout this journey. I am also very thankful to my friends and lab mates for always listening to me, finding time for fun and letting my focus towards research work.

I am indebted to all those people who have made this PhD work possible and because of whom this research experience and wonderful journey shall remain everlasting and memorable forever.

Thanks to all of you!

Namita Agarwal

LIST OF ACRONYMS & ABBEVIATIONS

AES	Advanced Encryption Standard
ANN	Artificial Neural Networks
APDCBT	All Phase Discrete Cosine Biorthogonal Transform
AR	Association Rules
BER	Bit Error Rate
BPNN	Back Propagation Neural Network
DCT	Discrete Cosine Transform
DConT	Discrete Contourlet Transform
DCurvT	Discrete Curvelet Transform
DFT	Discrete Fourier Transform
DST	Discrete Shearlet Transform
DWT	Discrete Wavelet Transform
EEG	Electroencephalography
EGI	Extended Gaussian Image
FIS	Fuzzy Inference System
GA	Genetic Algorithm
GDPSO	Guided Dynamic Particle Swarm Optimization
ICA	Independent Component Analysis
IP	Intellectual Property

KLТ	Karhunen-Loeve Transform
LSB	Least Substitution Bit
LSVR	Langrangian Support Vector Regression
LUT	Look up Table
LWT	Lifting Wavelet Transform
MOPSO	Multi-objective particle swarm optimization
MPE	Modification of Prediction Errors
MSE	Mean Square Error
NCC	Normalized Cross-Correlation
NPCR	Number of Changing Pixel Rate
NSCT	Nonsubsampled Contourlet Transform
PDFB	Pyramidal Directional Filter Bank
PNN	Probabilistic Neural network
PSNR	Peak Signal-to-Noise Ratio
PSO	Particle Swarm Optimization
QHT	Quaternion Hadamard Transform
QIM	Quantization Index Modulation
QP	Quadratic Programming
RDWT	Redundant Discrete Wavelet Transform
SPIHT	Set Partitioning in Hierarchical Trees
SVD	Singular Value Decomposition

SVDD	Support Vector Data Description
SVR	Support Vector Regression
UACI	Unified Average Changed Intensity
VQ	Vector Quantization

LIST OF FIGURES

Figure No.	Caption	Page No.
1.1	Characteristics of watermarking	3
1.2	Applications of watermarking	5
1.3	a.) Watermark embedding	6
	b.) Watermark extraction	6
1.4	Digital watermarking classification	7
1.5	a.) Spatial domain techniques	8
	b.) Transform domain techniques	9
2.1	Identify the techniques used to measure robustness in image watermarking	34
2.2	Watermarking system	35
2.3	Representation of 2 nd level DWT decomposition	37
2.4	Watermarking embedding and extraction in DWT domain	38
2.5	Watermark embedding and extraction in DCT domain	39
2.6	i.), ii.) host image and iii.) secret image iv.) signed image	41-42
3.1	Diagrammatic representation of the proposed watermarking system	49
3.2	Encryption process	51
3.3	Watermarking process for image Lena	51
3.4	NPCR Values for standard images	52
3.5	UACI Values for standard images	53
3.6	NC values for standard images under watermarking attacks	54
3.7	Comparative analysis of PSNR with previous techniques	55
4.1	Watermarking with genetic algorithm	59
4.2	Flow chart of presented technique	61

4.3	Graphical representation of PSNR value of sample images	65
4.4	Image Seashore used in watermarking procedure	65
4.5	a.) Watermarking attacks from Lena image b.) Watermarking attacks from Seashore image	66
4.6	Graphical representation of PSNR value at YCbCr color model	71
4.7	Graphical representation of PSNR value at YIQ color model	75
5.1	Image fusion using wavelet fusion method	81
5.2	Proposed embedding procedure	82
5.3	Proposed extraction procedure	83
5.4	Original and watermark images	84-85
5.5	Fused watermark image	85
5.6	Graphical representation of different watermarked images	86
5.7	Graphical representation of NC values from Baboon image	87
5.8	a.) Proposed embedding procedure b.) Proposed extraction procedure	88 89
5.9	a.), b.), c.), d.) Original and watermark images	90

LIST OF TABLES

Table No.	Caption	Page No.
1.1	Different watermarking applications and their characteristics	5
2.1	Comparative analysis of domain-based watermarking	23
2.2	Comparative analysis of Encryption-based image watermarking	29
2.3	Comparative analysis of optimization-based watermarking	32
2.4	Investigation on various watermarking characteristics on image watermarking	33
2.5	Analysis of various studies according to size of host and watermark image used in image watermarking	34
2.6	Results of SVD, DCT, and DWT for different images	42
2.7	Results of DconT, QHT, and DcurvT	42
2.8	Results of SVD, DCT, and DWT for attacks	42
2.9	Results of DconT, DCurT, and QHT for attacks	43
3.1	Performance analysis of proposed method	52
3.2	NC values under several attacks	53
3.3	Comparative analysis of proposed method with previous methods	54
3.4	Comparative analysis of NC values with previous methods for attacks	55
4.1	Results of discussed method	64
4.2	Comparative analysis of PSNR values with a previous approach for different planes of color images	66
4.3	Outcome of imperceptibility and robustness at distinct attacks for RGB plane	67
4.4	Comparative study of PSNR (dB) with the previous method	68
4.5	Evaluation at YCbCr color space	70
4.6	Imperceptibility and robustness attained under various attacks at YCbCr color constituent from Lena image	72
4.7	Outcome of YIQ color space	74
4.8	Imperceptibility and robustness attained under various attacks of YIQ color constituents from Lena image	76

5.1	PSNR values tested for different watermarked images	85
5.2	NC values for different recovered watermarks	86
5.3	NC values for different recovered watermarks	86
5.4	Performance evaluation of proposed method at altered gain value	90
5.5	Performance evaluation for different images at same gain value	91
5.6	Performance tested against attacks for image Barbara	91

ABSTRACT

In today's modern world, it is easily accessible to replicate and broadcast digital content through the Internet. There are three different modes to shield multimedia contents such as steganography, cryptography and watermarking. Among them watermarking is the most popular technique and holds excessive ability. Digital watermarking gained wide interest in the field of multimedia objects. Digital watermarking systems are implemented to assure data authentication, copyright protection in multimedia data transmission. Moreover, it guarantees to shield the digital media from malicious attacks, piracy, interfering, and distribution of information. Digital watermarking is broadly pre-owned as a robust technique for enhancing trust in the distribution of multimedia contents. In this thesis, transform-domain-based robust, secure and imperceptible watermarking schemes are presented using encryption and optimization techniques for color images. A new watermarking and encryption results are defined based on these methods. The main purpose of this work is to increase the robustness, imperceptibility, security, and embedding capacity of multimedia data. The first objective is implemented to achieve a secure and robust watermarking system for color images. The purpose of the second objective is to boost the robustness without damaging the image quality of the signed images. In the third objective security, embedding capacity, and robustness are improved with the wavelet fusion method. In the last objective, multiple watermarking based on transform-domain techniques is implemented to attain imperceptibility and robustness. These four objectives are also capable of resisting some image processing attacks. The proposed techniques achieve good performance in terms of Peak Signal-to-Noise Ratio (PSNR), Normalized Correlation (NC), Number of Changing Pixel Rate (NPCR), and Unified Average Changed Intensity (UACI) and found to be better when compared with previous approaches.

CHAPTER-1
INTRODUCTION

Chapter-1

INTRODUCTION

The recent technological development in information and communication technologies resulted in an exponential rise in the digital data exchange process through wireless communication networks [1]. Multimedia data broadly refers to audio, video, speech, image, and text [2]. The data exchange over the internet may suffer from severe security threats due to the unreliability of wireless communication networks, lack of robustness in encryption and authentication protocols, etc. [3], [4]. Digital watermarking is an extensively used approach to enhance the security of digital data by inserting secret media into the original data [5]. Furthermore, watermarking is also a subsist for several other techniques such as encryption, decryption, and geometrical manipulation [6], [7]. Security, imperceptibility, embedding capacity, and robustness are the main requisites of watermarking [8]. Though, meeting all these constraints simultaneously is a challenging research problem. In this thesis, different watermarking procedures are investigated to strengthen the security of multimedia information inclusion to robustness and imperceptibility. Therefore, we design and implement novel watermarking techniques to attain a good trade-off among different characteristics of watermarking for real-time applications.

1.1. Characteristics of watermarking

Security, imperceptibility, and robustness are the three major performance attributes for watermarking applications [9], [10]. Although, most of the watermarking applications primarily focus on security aspects only. However, integration of digital watermarking in many applications such as healthcare, copyright protection, broadcasting and remote sensing requires robustness, imperceptibility and security of data simultaneously, therefore, all these performance metrics are used in this thesis work. Fig. 1.1 represents the fundamental characteristics of watermarking and some of them are defined as follows.

- **Security** – For watermarking schemes, security is the foremost important characteristic. It is measured by eliminating or changing secret information without damaging the original media.

- **Imperceptibility** – It represents the watermark characteristic that does not destroy the significance of the marked media.
- **Robustness** – It defines the ability of the watermarking to survive in the presence of various image-processing attacks in terms of legal or illegal alterations.
- **Embedding Capacity** – It is outlined as the total measure of data such as image, text, and number hold by secret media that is inserted into the cover media.
- **Computational Cost** – It is used to measure the computational complexity incurred in the watermarking process (embedding and extraction) in the content into/from the host media. Ideally, it should be zero for watermarking [9].
- **Fragility** – It is used to measure the authentication of multimedia contents in contrast to robustness.
- **Data payload** – It is the quantity of information held by the watermark. A good watermark should preserve all essential information. There are 2^n possible watermarks, for n bits size watermark.
- **Tamper resistance** – It is used to measure the reliability and authenticity of digital information. This watermark is delicate to information changes, exchange, and inequalities, thus assuring reliability and information reliability.

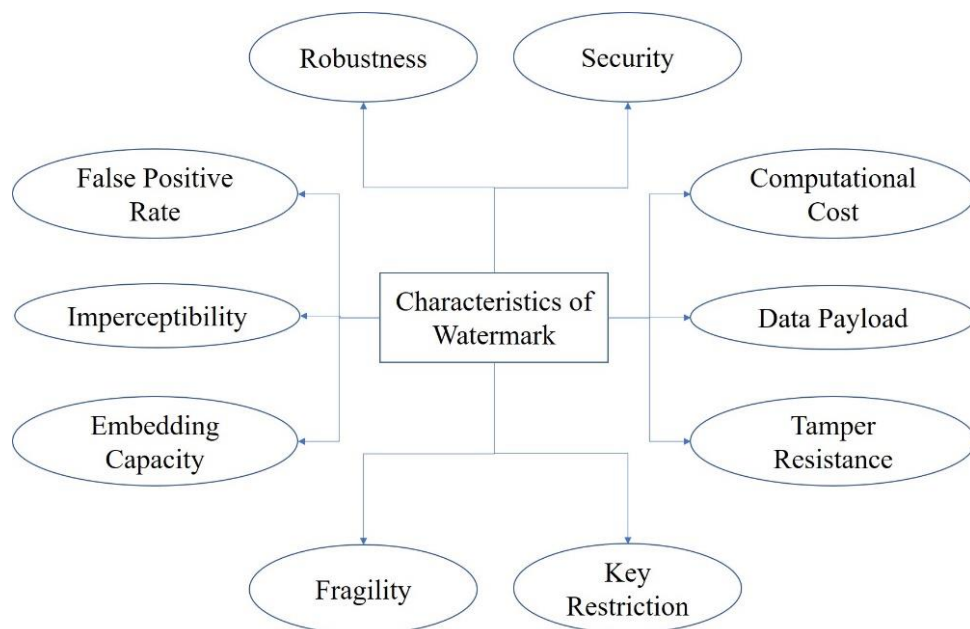


Fig. 1.1: Characteristics of watermarking [5]

1.2. Applications of watermarking

Watermarking is being used in a plethora of applications such as military systems, electronic voting systems, medical, digital cinema, copyright protection, content authentication, cloud computing, remote education, and many more [11] [12] [13]. Fig. 1.2 denotes the numerous applications of watermarking and some of the watermarking applications are described as follows:

- **Copyright protection-** It is a basic attention of watermarking. It represents the information about the copyright proprietor and is entrenched as secret information in the host data to be shielded.
- **Fingerprinting-** It is defined as identifying the dispatcher or receiver of peculiar multimedia information. The fingerprinting procedures should have the imperceptible characteristic for distinct attacks aforesaid filtering and lossy compression. Fingerprints must not be affected by any attack which can embed more than one ID number to the host data to avoid a bunch of workers having similar images.
- **Medical applications-** Watermarking in the medical field extends a secure platform in implementing electronic health applications by providing verification and privacy to medical information.
- **Electronic voting system-** Electronic voting system is nowadays being used everywhere including in small villages too. Digital watermarking can be used to provide security at each stage of the election process.
- **Chip and hardware protection-** There are several ways in which software and hardware devices need watermarking e.g., trojan security, buyer ownership, intellectual property rights, core, and computer hardware guard in contradiction of intellectual property piracy, and merchant proprietary.
- **Remote education-** Remote teaching and learning has been proven a very good strategy after the coronavirus pandemic. Digital watermarking can be used to provide security and verification in the information exchange involved in remote education.
- **Cloud computing-** Cloud computing is a suitable choice in a variety of applications, especially in big data applications. Digital watermarking is used on medical and non-medical images for their authentication before they are transmitted to other places [14] [15].

In addition, Table 1.1 describes various characteristics of watermarking with its applications. It is observed that a large number of watermarking applications exist.

However, in this thesis, different watermarking algorithms are investigated focusing on authentication, healthcare and digital transmission applications due to their wide range of usage in real-world.

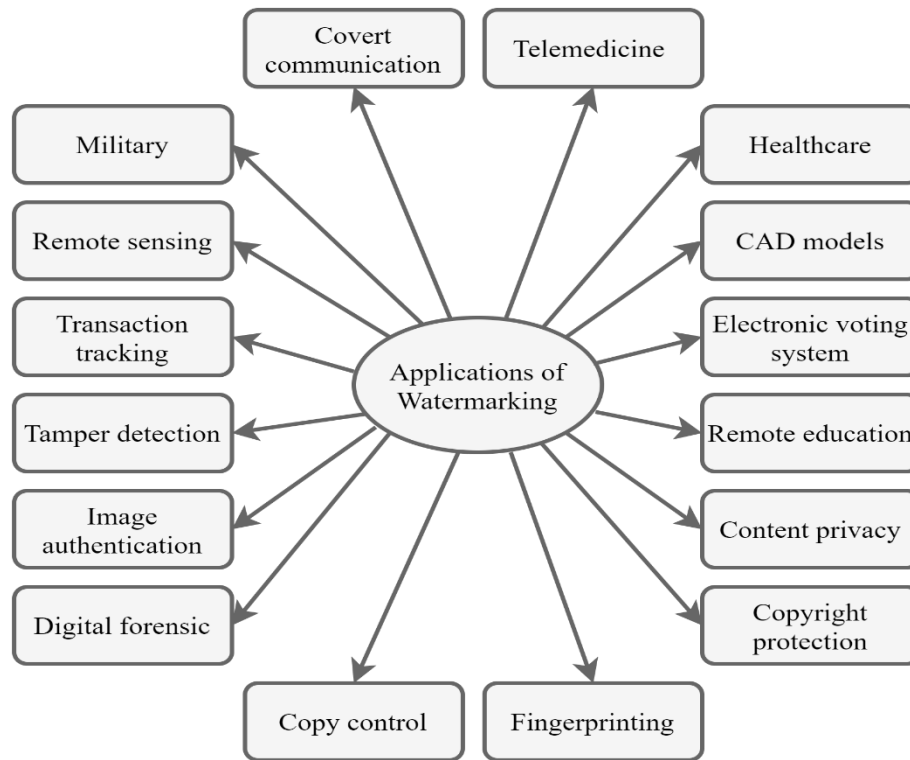


Fig.1.2: Applications of watermarking [5]

Table 1.1 Different watermarking applications and their characteristics

Characteristic	Definition	Application
Robustness	The ability of the watermarking to persist in the presence of various image-processing attacks in terms of legal or illegal alterations [16].	Copyright protection
Imperceptibility	Represents the watermark characteristic which does not destroy the significance of the marked media [17].	Digital imaging, E-health, portable information
False Positive Rate	It is defined as possible detecting secret marks in unwatermarked locations.	Proprietorship and copyright
Fragility	Used to measure the authentication of multimedia contents in contrast to robustness [5].	Content validity and multimedia information integrity
Security	Eliminating or changing the secret information without damaging the original media.	Military, E-health

Capacity	The total amount of data e.g., image, text, and number inserted into the cover media.	Digital cinema, telemedicine, media distribution
----------	---	--

1.3. Watermarking embedding/ extraction process

To achieve a watermarked image, the host message is embedded by watermark information with the secret key in an encoder as shown in fig. 1.3(a). The signed image (watermarked) is thus the output of the host and watermark image. Afterward, in the extraction (recovery) procedure, the watermark and host image are extracted by loading the same secret key as shown in fig. 1.3(b) [18], [19].

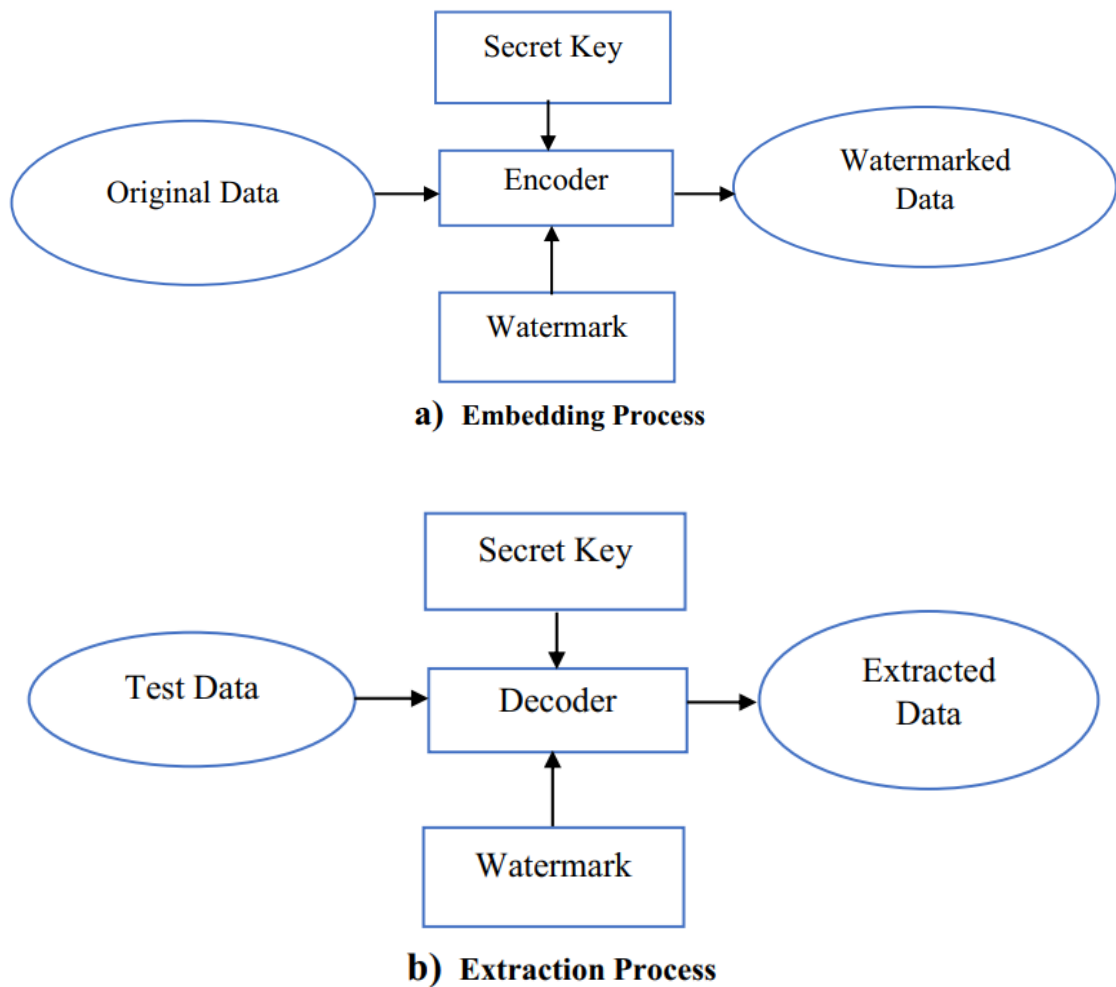


Fig. 1.3: a.) Watermark Embedding b.) Watermark Extraction

1.4. Classification of watermarking

Digital watermarking is mainly categorized into five types based on robustness, type of data, implementation domain, the recovery process, and human perceptivity [20], [21]. These five types are further subcategorized as shown in fig. 1.4. Robustness watermarking is subcategorized into three categories fragile, robust, and semi-fragile. On the basis of media, it is subcategorized further into graphics, image, text audio, and video. Based on human perceptivity, further, it is defined in two parts i.e., invisible and visible. And in the class of watermarking working domain, it is classified into two types, spatial and transform-domain watermarking.

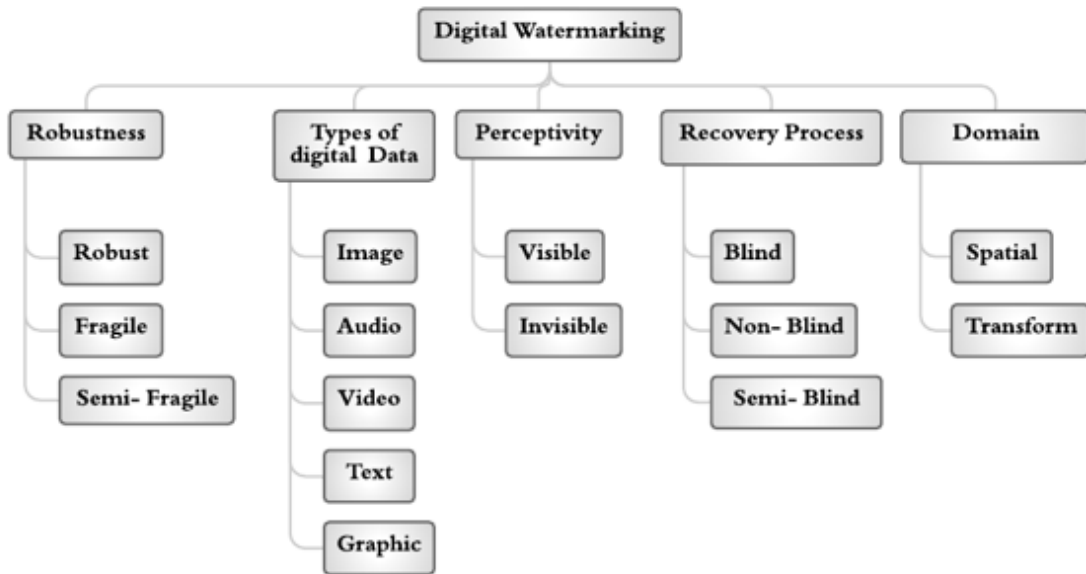


Fig. 1.4: Digital watermarking classification [22]

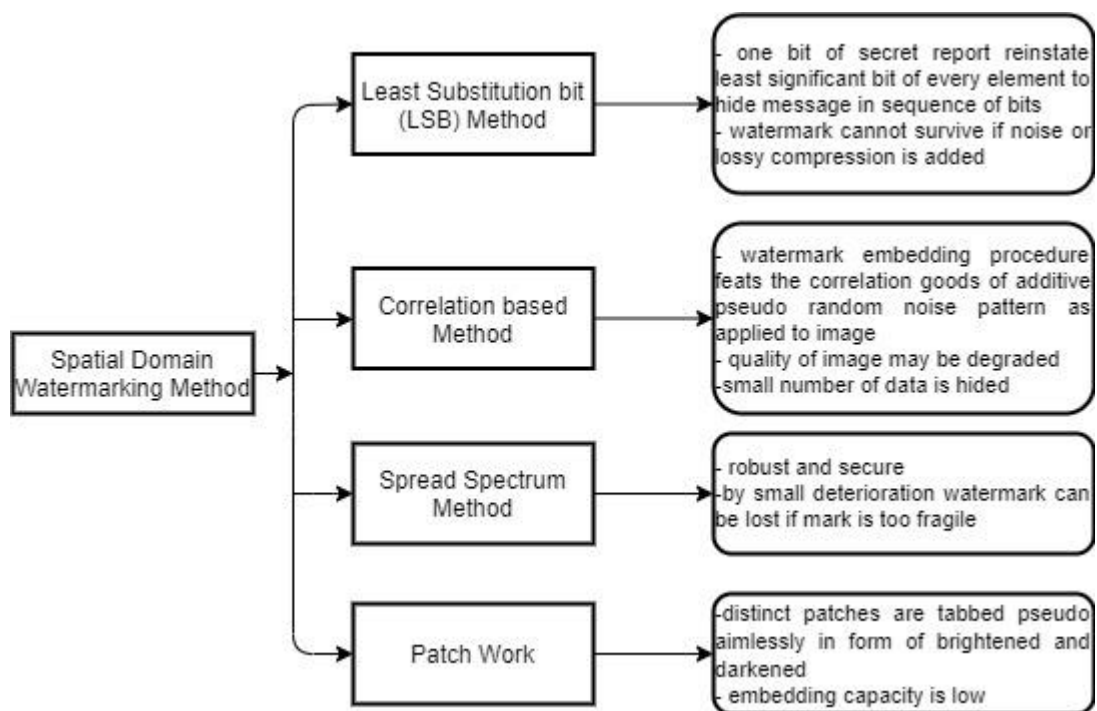
According to watermark retrieval process, digital watermarking is classified into three different classes i.e. semi-blind, non-blind, blind, based on creation and provision scheme [23], [24].

- Blind watermarking- In this class, a host image is not obligatory but only watermarked image is necessary at the time of watermark retrieval. Major applications of this watermarking class are found in e-healthcare and e-voting schemes.
- Non-blind watermarking- In this class, watermarking requires only original media to distinguish the watermark. Copyright protection and media communication are major applications of this class.

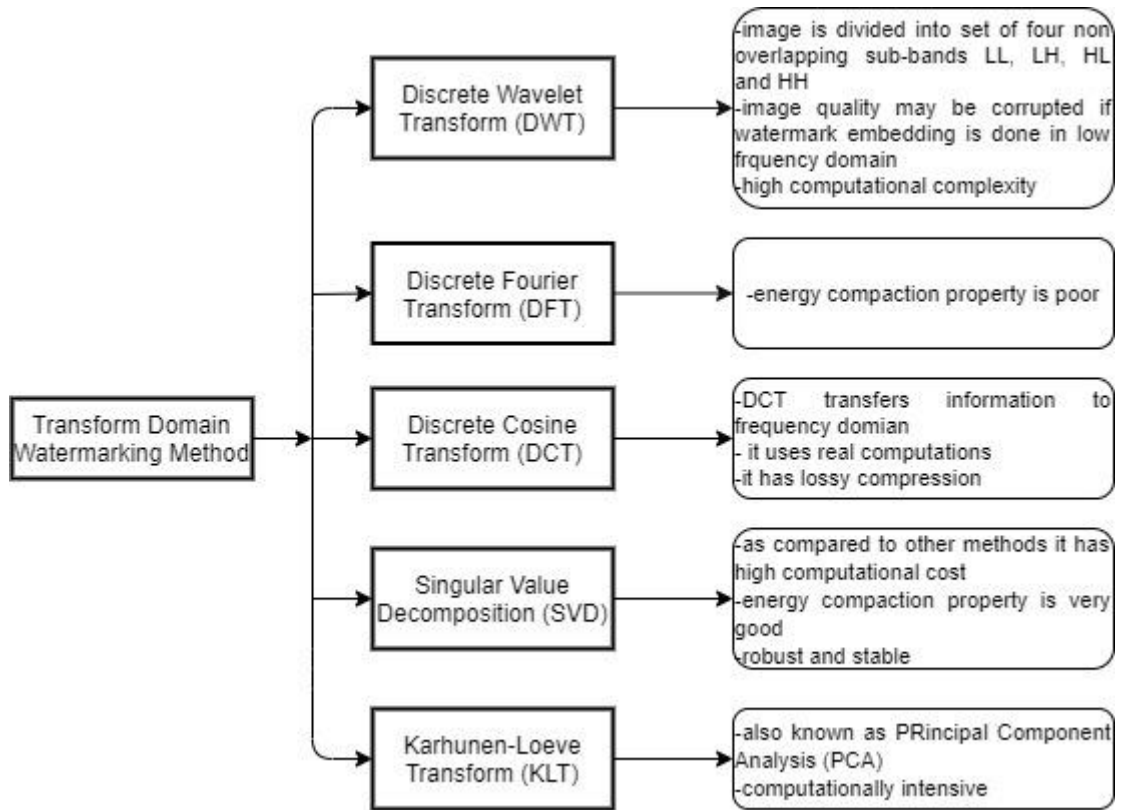
- Semi-blind watermarking- In this class of watermarking, it requires the watermarked image along with the secret key to detect the embedded watermark. Some major applications of this watermarking class are data authentication and integrity variation in multimedia data.

1.4.1. Watermarking domain techniques

Spatial and transform are two main watermarking working domains. Spatial domain systems are very effortless in terms of computational complexity, but they are less robust. In contrast, the transform-domain technique has high computational complexity but has robustness against different attacks [25]. Different types of spatial and transform domain-based systems are presented in fig. 1.5.



a.) Spatial domain techniques



b.) Transform domain techniques

Fig. 1.5: a.) Spatial domain techniques b.) Transform domain techniques

1.5. Watermarking performance metrics

To estimate the performance of watermarking algorithms, some important metrics PSNR, NC, NPCR, and UACI are mainly considered in this thesis work [26]–[28] [29]. Most existing studies consider one or more than one performance metrics depending on the watermarking application. However, there is a trade-off between these performance metrics in the presence of attacks according to the strength of gain factor.

a) Peak signal-to-noise ratio (PSNR)

The PSNR is computed here to check the peculiarity of a watermarked image after embedding the secret media into host media [26]. The higher PSNR indicates more transparent watermarking system. It also measures the imperceptibility of the watermarked image. It is defined in eq.1 as follows:

$$PSNR = 10 \log_{10} \frac{(I_{max})^2}{MSE(R,S)} \quad (1)$$

where, mean square error (MSE) defines the pixel values inequality between the host and watermarked image and is represented in eq. 2.

$$MSE = \frac{1}{PQ} \sum_a \sum_b (R(a, b) - S'(a, b))^2 \quad (2)$$

where, (R, S) are images of size (P, Q) and $R(a, b)$ and $S'(a, b)$ are the pixels of cover and watermarked image.

b) Normalized cross-correlation (NCC)

This parameter is computed to verify the robustness and similarity between the original and extracted watermark [27]. Robustness determines the perseverance of the hidden mark and ability of watermarking algorithm to survive in the presence of different attacks. The NCC value varies in the range 0 to 1. Generally, the NCC value larger than 0.7 is found to be appropriate for suitable applications of watermarking [19]. The NCC is mathematically represented in eq. 3:

$$NCC = \frac{\sum_x \sum_y X_{org}(x, y) X'_{extd}(x, y)}{\sum_x \sum_y X_{original}^2(x, y)} \quad (3)$$

where, X_{org} denotes the original watermark and X'_{extd} represents the extracted watermark.

c) Number of pixel change rate (NPCR) and Unified averaged changed intensity (UACI)

The NPCR denotes the percentage of pixel change between input and encrypted images and UACI denotes the average intensity difference between the input and encrypted images [28], [29]. These two parameters present strong security capability of an encryption scheme. The NPCR is modelled in eq. 4:

$$NPCR = \sum_{x, y} \frac{P(u, v)}{Z} \times 100\% \quad (4)$$

where, P defines the bipolar array and Z represents the overall quantity of pixels.

$$P(u, v) = \begin{cases} 0, & \text{if } C_1(u, v) = C_2(u, v) \\ 1, & \text{otherwise } C_1(u, v) \neq C_2(u, v) \end{cases} \quad (5)$$

C_1 is pixel value before encryption and C_2 is pixel value after encryption. The value of the bipolar array is zero for similar pixels and one for distinct pixels.

The UACI is modeled in eq. 6:

$$UACI = \sum_{x,y} \frac{|X_1(x,y) - X_2(x,y)|}{A-Z} \times 100\% \quad (6)$$

where A represents the largest supported pixel is related to the format of the encrypted image.

1.6. Watermarking attacks

In digital watermarking systems, the information needs to be conserved during its transmission to a receiver [30]. However, there are various types of attacks that may destroy the quality of unseen secret information or broadcast of information conveyed by watermark [31]. Watermarking attacks are of mainly two types: intentional and unintentional attacks [32]. In intentional attacks, as the name suggests, attackers knowingly attempt to obstruct the functioning ability of the secret data. A few examples of this type are protocol, geometric and cryptographic attacks. In unintentional attacks, attackers do not knowingly attempt to obstruct the functioning ability of the secret data. Signal processing attacks are an important example of this type. A brief description of selected attacks is presented as follows:

a) Signal Processing attacks

It is an unintended attacks type and causes information distortion during the information exchange process. A few examples are demodulation, filtering, JPEG coding distortion, and JPEG 2000 compression.

b) Geometric attacks

It is an intended attacks type that destroys the watermark secret data rather than alteration of the inserted data. A few examples are binding, clipping, linear and rotational transformation.

c) Cryptographic attacks

It is an intended attacks type that interrupts the security characteristic of the watermarking process and can eliminate the inserted watermark data or embed misleading information. A few examples are oracle attacks and collusion attacks.

d) Protocol attacks

It is a very strong type of attack which can change the entire logic of the digital watermarking system. During this attack, the attacker can get the information of the watermark itself as compared to altering or damaging the watermark. An

attacker can acquire ownership of the host and watermarked images. A few examples are invertible and copy attacks.

e) Other deliberate attacks

In these attacks, the attacker aims to change the genuineness of the proprietorship data by embedding a new legal watermark. A few examples are forgery attacks, rescanning, and printing.

In this thesis work, geometric attack, signal processing attacks and cryptographic attacks are taken into consideration.

1.7. Research objectives and contributions

This thesis focuses on exploring digital image watermarking techniques to improve robustness, imperceptibility, and security properties during transmission of color images. Robustness, imperceptibility, and security are three major performance metrics of a digital watermarking system. However, it is a very challenging research problem to improve all performance parameters simultaneously i.e., without compromising one over the other. Most previous studies investigate different watermarking techniques with a focus on just one or two parameters whereas settling with another constraints. In this thesis, different transform-domain-based watermarking techniques are investigated and a new approach is developed to obtain the security and robustness of multimedia data in digital watermarking.

The research objectives of the thesis are as follows:

- a)* To investigate the robustness and security of color images by applying transform-domain techniques with encryption.
- b)* To investigate watermarking methods that are capable of improving the robustness and imperceptibility of color images for several attacks.
- c)* To implement transform-domain-based watermarking schemes with fusion method to enhance the security and robustness for color images.
- d)* To implement a multi-level watermarking using the transform-domain-based procedure to enhance the imperceptibility.

To achieve the above research goals, an intensive literature survey has been conducted on different watermarking techniques for both grey and color images. During this stage, different transform-domain-based techniques are explored to achieve good robustness and simulation results are discussed. Different techniques such as particle swarm optimization (PSO), encryption, and neural networks are studied. With these techniques, algorithms are categorized according to the size of various host and watermark images.

To fulfill the security requirement of the multimedia data, homomorphic encryption with the Arnold transformation method is presented. This method signifies a secure and robust watermarking grounded on the Paillier Homomorphic cryptosystem. In this encryption-based watermarking system, the watermark is embedded into the encrypted original image. Different watermarking performance metrics like PSNR, NCC, NPCR, and UACI are analyzed. Results show that the encryption-based transform domain method is more robust and secure against many attacks.

The next contribution of this thesis is to guarantee data authentication and copyright protection during data transmission. The proposed method is created with the DCT and the Genetic algorithm. The DCT technique is employed to disintegrate the original media into 8by8 sections and a genetic algorithm is applied on top of the DCT technique to obtain the optimal results. This approach is verified under distinct color models e.g., YIQ and YCbCr, and watermarking attacks. PSNR and NCC performance parameters are evaluated and found to be superior as compared to the previous schemes.

Towards achieving robustness and security, a fusion-based watermarking method is proposed for color images to improve data security for e-health applications. The wavelet fusion technique unites two different watermark images to make a single fused watermark, and then Arnold scrambling is operated on the fused watermark image to enhance its security and robustness under distinct attacks. The outcome illustrates that the system achieves good robustness and security as compared to existing methods. Furthermore, a multi-level watermarking is designed with three transform-domain methods DWT, DCT, and SVD. The presented approach is implemented under various attacks, and the outcome shows that this method achieves good robustness and imperceptibility.

1.8. Thesis organization

The thesis includes six chapters including **Chapter 1** that presents the introduction of watermarking along with a classification of different watermarking techniques and their characteristics.

Chapter 2 presents the literature survey of different transform domain-based watermarking techniques with encryption and optimization, then a comparative study of various transform domain techniques with their results is discussed.

Chapter 3 describes the objective 1 proposed in this research work with Paillier homomorphic cryptosystem and Arnold transformation, to accomplish the security and robustness for color images.

Chapter 4 presents objective 2 of this research work based on DCT and genetic algorithms. This approach is tested under different color models.

Chapter 5 presents a fusion-based watermarking for color images and multi-level watermarking is discussed in detail.

Chapter 6 presents the concluding remarks of this thesis and future scope for the extension of this research work for real-time application.

CHAPTER-2
LITERATURE SURVEY

CHAPTER-2

LITERATURE SURVEY

This chapter consists of a widespread study of published articles related to the area of research with a focus on their concepts and outcomes. The literature survey is also valuable for drafting the research gaps and their requirements.

Digital watermarking is always a dominating area for both ordinary users and researchers. The prime focus of this research is to offer secure, imperceptible, and robust watermarking systems for various applications. The key determination of this literature review is to analyze numerous digital watermarking approaches to recognize the most efficient method for robust and secure multimedia data. Some research databases are explored for the previous studies, as there is a variety of research articles available in the sphere of digital image watermarking. In this study, different databases for analysis of current advancements in the arena of digital image watermarking are available. The list of databases explored are listed below:

- Google Scholar
- Science direct
- Springer
- IEEE
- ACM digital library

For the last few years, to improve the robustness, imperceptibility, and security of multimedia content, domain-based watermarking methods (spatial and transform) along with encryption and machine learning techniques are imposed into digital image watermarking schemes. Robustness against intentional and non-intentional attacks, quality of signed image, and security of multimedia content are the important issues for watermarking schemes. Several research activities have been carried out using the transform domain watermarking scheme and optimization method to solve these issues.

2.1. Review of related research

A detailed review of articles is presented in this section, regarding the application of digital media by using domain-based watermarking with encryption and genetic algorithms.

2.1.1. Domain-based watermarking

In [1], a robust watermarking technique is implemented with discrete cosine transform and decision tree (ID3) for both greyscale and color images. The original and watermark image pixels are altered by discrete cosine transform. To hide the secret watermark, decision tree induction technique is used. Arnold transform is implied here for high security. The results analysis has discovered that the presented system is robust but the method is limited to JPEG compression attack. The author of [2], introduced feature-based watermarking with a combination of graph theoretical clustering algorithms. Synchronization error of image can be resolved with the use of Affine invariant point on the image. The achieved PSNR is greater than 40dB and has a high computational cost. The experimental outcome is compared with several prior methods [33]–[35] and found that presented logic is robust against watermarking attacks.

The author of [36], implemented a feature-based watermarking to enhance the security and robustness of multimedia contents. The logic used an auto-correlation matrix with the Laplacian-of-gaussian procedure to find out the rounded mark sections and to trade-off between watermarking factors. A multidimensional knapsack problem is expressed which is resolute by genetic algorithm for the optimal selection process. The experimental outcome shows that this method is secure and found better as compared with other techniques [34], [35], [37], [38]. In [24], the author discussed a spread spectrum and transportation theory-based secure watermarking for greyscale images. To achieve acceptable robustness with minimum distortion, authors used a multiplicative embedding procedure. The author of [39] proposed a watermarking technique with association rules (AR) and vector quantization (VQ). Firstly, procedures are resolute for the two, 2D barcode and watermark information. In this method, the 2D barcode is treated as host information and generated rules for watermark information as a watermark. In the embedding process, generated rules are embedded with the association algorithm of original barcode data. The experimental demonstration indicates that the suggested method is secure and has admirable embedding capacity.

The author of [40] proposed a reversible as well as high-capacity watermarking method with sorting, histogram shift, and rhombus *pattern*. Firstly, the original information is split into two distinct groups and embedded by the payload data. The proposed technique is robust as well as imperceptible against watermarking attacks but computational time is high. This method obtained better results when compared to previous methods [41]–[44].

The author of [45] described a pixel-based information hiding procedure. This method is used as an error-diffused image matrix to embed the secret media. The concept of a look-up table is imposed here for the speedy recovery of the extracted watermark. The 512×512 is the host image size and 32×32 is the size of the watermark, taken for the experimental analysis. In this method, both original and watermark images are RGB images. The implementation outcome has indicated that the process is robust in contrast to scanning and printing attacks, even decoding rate is high. This method is also compared with the previous method [46].

In [47], the author discussed a perturbation logic to validate the watermark information into cover media and achieve perturbed information back to the original state. For experiment purposes, dataset taken here is compared with other references [48], [49] [50]. The degree of dilemma in original data is estimated by an adjustable weighing approach. Results have shown that this method is secure as well as robust at the high payload. Direct sequence spread spectrum watermarking methods for audio signals are proposed in [51]. The discussed method achieves increased robustness with imperceptibility, vigorous against image processing attacks, and sustaining a secret interaction with the public audio station.

A watermarking scheme based on a modification of prediction errors (MPE) with a combination of histogram shift procedure and median edge detection is discussed in [52]. This procedure is operated in two parts, initially embedding process and then extraction process is done with image restoration technique. Stego image has a PSNR value larger than 40dB, which is produced by MPE. The outcome of the method shows that embedding capacity attained by MPE is superior as compared to other techniques [53]–[55]. In [56], the author proposed a watermarking scheme created on VQ with the concepts of data mining. The association rules are used in original information as well as in watermark information. The performance parameters such as PSNR and NC are

checked at a unique threshold. The technique achieved good robustness against attacks and high embedding capacity in comparison to the previous method [57].

The author of [58] proposed a watermarking system created with different transform domain techniques i.e., DCT, SVD and DWT. For more security, transform domain methods with Arnold transform is applied here for copyright protection. The size of the host image is 1024×1024 and 128×128 watermark size is taken for the experiment. The algorithm was found robust against many attacks. Additionally, the experimental outcome is compared with previous methods [59]–[63]. In [64], the author proposed a multilevel secure digital watermarking procedure with a 2D barcode for biometric characters. In this algorithm, a 2D barcode is treated as host information and biometric characters are used as secret information. At a suitable matching score, this algorithm embeds the watermark in 2D cover information. The evaluation of this method is based on the human visual method and achieves better results for the visual logic methods [65]–[67]. The author developed a hologram-based watermarking to provide document integrity in [68]. In this particular method, hologram coding-based data is embedded into personal data printed on the ID card. This is a fragile watermarking technique. Various types of holograms with their advantages, important issues and challenges of the hologram secret information are also discussed in this article.

An enhanced embedding capacity watermarking approach using JPEG is presented in [69]. The technique uses LSB of quantized DCT constants to indiscernibly embed the secret information at an agreeable security level. The author of [70], proposed a secure watermarking method for outsourced datasets. The dissimilar outsourced datasets are strings, numeric, and non-numeric datasets. For classification accuracy, the author used distinct machine learning methods. For evaluation purposes, the secret mark is used as a length of 16bits. To offer security of watermark information, this technique takes all available rows of datasets to offer security of the watermark information. Further, this method is compared with another method [71] and found to be robust. In [72], the author presented a watermarking approach based on independent component analysis (ICA). The algorithm works on employing the visual mask on the watermark and then take the transpose of generated secret information. Then the secret information is implanted with the host image. The 512×512 is size of the host image and 64×64 is size of secret information. The outcome shows that this algorithm is robust

against several attacks and attains good performance when compared with other procedures [73]–[79].

The author of [80] discussed secure watermarking algorithm based on 1D neighborhood technique [80]. Without using the concept of cryptography, authors proposed a low computational complexity algorithm. The Watermarking procedures are conducted in a zigzag manner. Experimental results show that the PSNR value gained by this technique is 51dB.

The author of [81] described a secure, imperceptible and robust watermarking procedure based on transform-domain methods (DCT, SVD and DWT) with Arnold transform and backpropagation neural networks (BPNN). Transform-domain techniques are implied here to keep secret distinct encoded secret information into original media. Arnold transform is applied here for more security of the medical data. The host media (image) is of size 512×512 and the secret information size is 256×256 with 190 characters. Additionally, the concept of neural networks makes algorithms more robust against watermarking attacks. NC values for the same are compared with previous methods [82] [83]. In [84], the author proposed a robust digital watermarking for a human visual method for greyscale images. The author used an additive method to hide secret information containing a binary sequence in the images. The experimental outcome represents that the bit error rate (BER) is extremely low in contrary to lossy compression. The author of [85], discussed imperceptible watermarking for the distribution of medical data. The presented procedure used the knowledge digest method to update databases and recollect images through the noisy station. This method is also studied with the compressed image like JPEG and expands to the reversible pattern.

In [86], the author designed a robust watermarking approach via the vertex scrambling method. In this method, converting the distance of vector that corresponds to a vertex as the center of the pattern. Experimental evaluation has shown that this approach is robust in contradiction of attacks like model cropping, noising, and mesh applications. In [87], the author developed a blind watermarking technique by using a spread spectrum with a look-up table (LUT). The function of LUT is to embed a spread-spectrum watermark imperceptibly. The experimental evaluation states that the algorithm is secure and has a fast recovery process. An imperceptible and robust

watermarking for 3D polygonal is discussed in [88]. The technique used for this watermarking algorithm is patch classification, vector distribution, and extended gaussian image (EGI). This method does not need a genuine model to distinct the secret information, and robust against many attacks.

In [89], the author has suggested a secure multilevel watermarking based on the spread spectrum and wavelet method. This algorithm is proposed for medical data verification. In this algorithm, encrypted text information of medical documents is embedded into wavelet coefficients of medical host information. The technical outcome represents that this algorithm is robust against attacks and suitable for the medical information. In [90], the author introduced robust and imperceptible watermarking via quadratic programming (QP). The technique uses the spread spectrum method to the starting point, then the QP scheme adjusts the watermark embedding necessities. The robustness is enhanced in comparison to the baseline method.

In [91], the author has suggested a watermarking scheme for binary images by exploitation of probabilistic neural network (PNN) and discrete wavelet transform (DWT). The key purpose of this technique is to generate a high imperceptible watermarked image. In this method, a Haar wavelet filter is used to embed a greyscale watermark to particular sub-bands of DWT. PNN is functional here to extract the binary secret image. The 512×512 is the original image size and 64×64 is the binary watermark size, taken for the experimental analysis. The result represents that this technique is imperceptible and robust against attacks. The author of [92] designed a robust and visible watermarking approach for greyscale images by use of the discrete contourlet transform (DConT) and quantization index modulation (QIM). After applying contourlet, constants are separated into three parts using the symmetrical features of contourlet transform. Then angle quantization constants are framed for these three parts. This method achieved good PSNR and NC values in comparison to others [93].

The author of [94] suggested an enhanced secure and robust digital watermarking by the use of discrete wavelet transform (DWT), discrete cosine transform (DCT), and singular value decomposition (SVD) with set partitioning in hierarchical trees (SPIHT) for greyscale images. Arnold scrambling is applied here on the watermark image and get scrambled image (watermark) before embedding to the original data. Through these transform domain methods, watermark data is implanted

into the original data. After that, SPIHT is employed to compress the watermarked image for better performance. The 512×512 is the host image size and 256×256 is size of the watermark, taken for experimental analysis. Results have shown that this technique is robust and secure in comparison to other methods [95]–[100]. In [101], the author presented a watermarking technique through the lifting wavelet transform (LWT), Lagrangian support vector regression (LSVR), QR decomposition and Arnold transform method. The original image matrix is decayed by LWT, then a LL sub-band is adapted for the watermark embedding process. Further, sub-bands are transferred to sub-block. Each sub-block is decomposed by an QR decomposition code. This technique achieves acceptable robustness and imperceptibility, and technical outcomes are found better when compared with previous methods [102]–[104]. The author of [105] proposed a robust and imperceptible watermarking based on Schur decomposition and quaternion hadamard transform (QHT) for color images. A host image is holistically embedded by QHT and secret information is encoded by shifting the values of the Q matrix, gained by Schur decomposition. To make this method robust against geometric attacks, a geometric distortion detection scheme is presented by the quaternion Zernike moment. The $512 \times 512 \times 24$ is the measurement of host image and $64 \times 64 \times 2$ is the measurement of watermark image used for the experiments. Results reveal that the system is robust against attacks but it has some distortion issues. Robustness is also compared with the previous method and found to be better [106].

A medical data verification watermarking created with SVD and Arnold transform is proposed by the author of [107]. Firstly, the original image is altered by DCT and divided into blocks. The particular block is iterated by Arnold transform, and then SVD is applied on the block with zero LSB. This scheme controls some bits to embed into the LSB of the host data. The method achieves robustness against attacks and is found suitable with other techniques [108]–[111]. In [112], author presented a watermarking system for proprietorship rights. The method is created with hashing permutation and Z language. The result shows that this method is applicable for the validation of digital data. The author of [113], proposed greyscale watermarking through adaptive logo texturization (ALT_MARK). Arnold transform is applied here not only for security but also to enhance the robustness by texturizing the logo and embedding the information in the wavelet domain. The method shows better results as compared to others [114]–[117]. In [118], author introduced a watermarking system for

medical records. In this system, pseudo-noise is encoded into the certain sub-bands of DWT and generates the wavelet statistical possessions of signed image, and for recovery phase, probability distribution function (PDF) is employed. The author of [119] suggested robust watermarking with applying DCT, SVD, DWT, and all phase discrete cosine biorthogonal transform (APDCBT). The original image matrix is decomposed by DWT and particular coefficients of DWT are embedded with two similar watermarks. APDCBT is applied for the security of watermarks as it has better energy concentration. DC coefficients are retained for better imperceptibility. The results of this method are compared with another method [120] and are appropriate for copyright protection. The author of [121] suggested an effective watermarking created on SVD, wavelet fusion, and multilevel DWT with HH band. The high-resolution band is very much sensitive to human eyes. In fusion method, two distinct watermarks are combined to make a single fused watermark. Using fusion method, a high embedding capacity is achieved. After that, the fused watermark is encoded with the coefficients of singular values of HH band of the host image during an embedding process. Experimental analysis has indicated that the suggested technique is robust against numerous image processing attacks and increases the imperceptibility.

In this section, we have studied various domain-based watermarking for multimedia data. In addition, the comparative analysis of domain-based watermarking is presented in table 2.1. Transform domain watermarking methods provide more robust results as compared to the spatial domain. These methods achieve good performance for visual quality of signed images, embedding capacity, robustness and security. Furthermore, after the transformation, the image is more responsive to its characteristics and easier to handle.

Table 2.1 Comparative analysis of domain-based watermarking

Ref.ID	Aim	Watermarking system	Techniques used	Host image size/ watermark image size	Outcome	Comments
[1]	Robust watermarking based on data mining	NA	DCT and ID3	512×512/32×32	For ced Component max PSNR= 50.8609	20480 is the total no. of occurrences
[2]	Upgraded feature-based robust watermarking	NA	Indirect inverse normalization, graph theoretical clustering algorithm, and affine covariant sections	512×512 / 256-length	PSNR is larger than 40dB	-100 images are used for evaluation. -Resolve the recovery ratio.

						-Excessive computational cost
[32]	Enhancement in security and robustness within feature-based watermarking	Blind	Noise visibility function	512×512/ created watermark span of 256 and recurrent 16 times	-PSNR= 42.21dB (Pepper) -finding ratio = 0.46 (Linear) -Repeatability ratio=0.77 (JPEG 50) - BER= 0.34 (Aspect Ratio Change)	-UCID database is taken -nembedding potency is fixed with Noise visibility function
[20]	Secure watermarking based on transportation theory	NA	DWT, spread-spectrum	512×512 groupings	- Average PSNR is 44.05 dB - At same PSNR, BER=6.268750e-02	-Embedding is multiplicative -2, 000 images are taken for experiment
[35]	Data verification with watermarking and 2D barcode	Blind	AR and VQ	-For greyscale images 2D barcode 900×1782 -Secret media is 480×360 grey-scale	PSNR is 31.62dB The algorithm output is 60.62%	Key used as own password
[36]	Less distortion with high-capacity watermarking	NA	Rhombus, histogram sorting, and shift Method	512×512/-	Payload locked to 0.5b/pixel	- Important enhancements over other approaches
[41]	Robust digital watermarking aimed at Halftone images	NA	Lookup table	512×512/32×32	For 11×11 decoding region Decoding rate = 95.77	-Outstanding embedding capacity -Less Computational complexity.
[43]	Digital watermarking based on data mining	Blind	Native bytes, decision Tree	NA	The payload for RDT is 9,000,000 at KDD cup KDD cup PDE is 6,000,000	- Accomplishment time & memory space and secret mark payload is assessed and linked
[47]	Secure and robust digital watermarking for audio signal	NA	-Moderated composite lapped transform, spread spectrum	NA	At copy sample, watermark detection is 0.0761	-Vigorous for various attacks
[48]	High capacity and imperceptible watermarking	Blind	Histogram-shift technique and median edge detection	512×512/Can embed 138,327 bits	For c, PSNR is 49.12dB Increased payload%= 487	- Histogram of prediction errors are modified
[52]	Robust watermarking	Semi-blind	AR and VQ	512×512/different dimensions	NC and PSNR are evaluated at	- Method may insert larger

	through data mining				a unique threshold	than original media -Threshold is distinct -Decrease the false judgment amount
[54]	Digital watermarking for copyright protection	Blind	Arnold transform and transform domain techniques	1024×1024/128×128	For Lena image NC= 0.9785 and PSNR= 52.34 dB	-Permitted from false positive problem
[60]	Security-based digital watermarking	Blind	Embedding and extraction with threshold	Height and width of barcode/ Dimensions of the face and fingerprint images are 240×320 and 300×300, correspondingly	At 2D barcode PSNR=86.47, For Face image 64.33, For Finger-print image 58.87	-Able to resist attacks -Biometric and barcode images are used
[64]	Secure digital watermarking	Fragile	Hologram methods	NA	NA	Assistances to stop ID card counterfeit
[65]	High-capacity Digital Watermarking	NA	LSB and DCT	256×256/-	For Girl PSNR=39.14dB	Equated with JPEG tool
[66]	Secure digital watermarking	Blind	Machine learning methods, feature ranking, data alliance, and threshold calculation	NA/Secret mark length = 16 bits	Good extraction accuracy	Used 25 various datasets for the investigational purpose
[68]	Robust digital watermarking	Blind	ICA	(Expt 2) 512×512/64×64	(Expt2) PSNR= 43.99dB	The altered image also measured as a watermark
[76]	Secure digital watermarking	Blind	1-D neighbourhood	256×256/-	PSNR is 51dB	Appropriate for potential applications of watermarking
[77]	Secure, imperceptible, and robust watermarking for identity verification	NA	Arnold Transform and DCT, SVD, DWT with BPNN	512×512/256×256 and 190 characters	-At gain 0.01, PSNR is 43.88 dB -For signature BER=0 -At gain 0.08 NC is 0.9861 (without BPNN) and NC is 0.9888 with BPNN)	-Used for inhibition of patient identity information
[80]	Robust digital watermarking for human visual model	NA	Additive watermarking technique	NA	BER is 3.0	2 ²²⁰ potentials chosen for embedding constraints

[81]	Imperceptible digital watermarking for medical application	Blind	KDD	365×378 pixels/ 2373 bits	PSNR is 41.7dB	Evaluated for JPEG-compressed images - Deliberate 750 images for challenging
[82]	Robust digital watermarking for 3D objects	NA	Vertex Scrambling	NA/50 bits	NCC is 1	- 2,955 apexes and 5,870 triangle faces are current in the mesh
[83]	Secure digital watermarking	Blind	Spread spectrum and LUT	NA	Circulation LUT correlation is 8.3×10^9	-Fast discovery procedure
[84]	Robust and imperceptible watermarking for 3D polygonal	NA	Patch classification, vector distribution, and EGI	1-bit secret mark with 50 measurements	At random noise and cropping attacks, BER is 0	-Stanford bunny pattern is used
[85]	Gives verification for medical information with digital watermarking	NA	Spread spectrum, discrete wavelet transform	512×512/-	BER=0.1538 and PSNR=40.02 dB	Attained 2 stages of security
[86]	Robust 3D watermarking	NA	QP and spread spectrum transform	NA	Distortion near 0.37	-Database of 10 meshes among 20k and 100k vertices
[87]	Robust digital watermarking	Blind	PNN and DWT	512×512/64×64	NCC is 0.9779 and PSNR is 68.27dB	-Executed superior to other methods
[88]	Imperceptible and robust digital watermarking	Fragile	QIM and DConT	512×512/-	-PSNR=61.9914 -Without attack NCC=1	-For optimization Lagrange technique is used -High transparency
[90]	Secure and robust digital watermarking	NA	Arnold Transform and DCT, SVD, DWT with SPIHT	512×512/256×256	-For MRI PSNR is 34.68 dB - For Barbara NC is 0.9973 -SSIM is 0.995857	-SPIHT provides compressed signed image
[97]	Digital watermarking for copyright fortification	NA	Arnold transform, LSVR, QR Decomposition, LWT	512×512/32×32	-For Lena PSNR is 45.9283 dB - BER=0 - Without attack NC is 1	Computational cost and memory is less
[101]	Imperceptible and robust digital watermarking	NA	QHT and Schur decomposition	512×512×24/ 64×64×2	-For Lena SSIM is 0.9917 - For Lena, Pepper, Baboon NC is 1 at no attack	-Complexity is less as compared to RGB color space

					-For Lena NC is 1 at gamma correction and brighten attack	
[103]	Secure and robust digital watermarking	Fragile	Arnold scrambling, SVD	512×512/-	-Copy and paste type 1 PSNR are 38.96 dB and tamper localization are 99.56% for the image plane -For content removal, copy and paste attack 1 NCC_1 is 0.9999 for kidney image -Copy and paste attack 2 for image Liver NCC_2 is 0.9985	- Extremely dependable
[108]	Digital watermarking for ownership rights	blind	Hashing and permutation and Z language	-/8 bit	100% accuracy rate	- Badge dataset is used -It promises to cover information recovery, after watermark decoding
[109]	Robust digital watermarking	NA	Adaptive logo texturization, Arnold transform, and DWT	512×512/64×64	-For Peppers PSNR is 44.21dB -For Mandrill NC is 0.979	The method is effective in terms of computational speed
[114]	Robust digital watermarking	NA	Spread spectrum and DWT	1024×1024/50×9	-Maximum PSNR is 43.9986dB -Maximum NC value is 0.9953 WDR is 20 dB	-Used Cauchy statistical method
[115]	Robust digital watermarking	NA	APDCBT, DCT, DWT, and SVD	512×512/32×32	NCC is 0.9724 PSNR is 101.97dB	-APDCBT is presented by joining of DWT and SVD
[117]	Fusion-based watermarking	NA	DWT, SVD, wavelet fusion	256x256/256x256	PSNR is 92.5872 at HH band of DWT PSNR is 58.60 (cameraman) at 0.5 gain value	HH band is sensitive to human eyes.

2.1.2. Encryption-based watermarking

The author of [122] presents a watermarking technique designed with DCT, DWT, SVD, and encryption for digital images. These three different transforms are

applied here to embed two distinct watermarks and give robust results against attacks. Furthermore, an encryption method is used to reduce the implementation time and complexity to make it appropriate for real-time applications. The experimental evaluation has been compared with older techniques [82] [123]–[125].

A secure watermarking is suggested by the author of [126], through SVD, redundant discrete wavelet transforms (RDWT), nonsubsampled contourlet transform (NSCT), and chaotic encryption for greyscale medical images. Watermarking performance parameters provide a solution for medical data verification. Security, distortion, and robustness are achieved by the experimental analysis. The designed algorithm shows that it attains good results in comparison with other techniques [81], [122].

The author proposed a high imperceptible watermarking system based on QIM and encryption procedures in [127]. The presented algorithm is evaluated on medical data (image). The PSNR value is greater than 60dB. The algorithm uses distinct outlines to offer the reliability of secret information at extremely low distortion.

The author discussed a robust, secure, and imperceptible watermarking approach for medical data authentication by using DWT-SVD with error correction codes in [128]. For embedding purposes, the method used the 'U' integral of SVD transform to formulate it, then unrestricted it from the false positive problem. Furthermore, the outcome has compared with other previous techniques [129], [130] and found suitable for medical applications.

In [131], author suggested a H.264/AVC watermarking scheme through the DCT and BCH. In this scheme, secret data is encoded by BCH code prior to information embedding, and encoded secret information embeds into the constants of DCT. For the experiment purpose, various numbers of bits are taken, PSNR value is recorded as 45.55dB and BER is increased by 1.06%. The designed technique was found to be robust in comparison to another method [132] and the embedding capacity of this method is also acceptable.

For more security and robustness, the author of [133], introduced a dual watermarking approach based on the transform domain with error correction code and BPNN for color images. In this approach, the cover image decomposes into third level

DWT and LH2 (vertical frequency band) is taken for inserting an image, and LL3 (low-frequency band) is chosen for embedding the text data. By using BPNN, robustness is enhanced and it controls the distortion error of extracted watermark from watermarked images. Further, this approach issues the channel noise alterations in identity information. An error-correcting codes are used for text watermark prior to embed into the host data. However, the selective encryption method is applied for more security. The cover image size of 512×512 and the watermark image size of 128×128 with 100 strings of text watermark are taken for experiments and the result shows that this method is robust, secure, and has acceptable visual quality, however, computation time is more in this method. Further, this approach attains good performance when compared with previous methods [134]–[139]. In [140], the author proposed a watermarking system with support vector data description (SVDD), DWT, and chaotic encryption for outsourced biomedical data. The embedding is done on the approximation sub-band of DWT, and the correlation among updated transform constants and watermark sequence in the wavelet domain is learned by machine learning techniques. The performance outcome on biomedical electroencephalography (EEG) data with machine learning methods shows good imperceptibility and robustness in comparison to other methods [141]–[143]. Furthermore, by applying chaotic encryption to the above method, security is also enhanced.

In this section, various encryption-based image watermarking systems are discussed. Moreover, a correlative study of encryption-based watermarking is tabulated in table 2.2, detailing the objective of watermarking, techniques applied, outcome, and size of images. However, these methods achieve good performance but algorithms are computationally complex.

Table 2.2 Comparative analysis of Encryption-based image watermarking

Ref.ID	Aim	Watermark ing system	Techniques used	Host image size/ watermark image size	Outcome	Comments
[118]	Less complex and robust watermarking with encryption	Non-blind	Encryption, SVD, DWT and DCT	-512×512/ 512×512 - Text watermark is 185 letterings	-At gain factor 0.01PSNR=28.5 1dB - For gain 0.1, NC is 1	-Unaffected to many attacks - Computational complexity is high

[122]	Security-based digital watermarking	Semi-blind	Chaotic encryption, NSCT, RDWT and SVD	512×512/256×256 and 128×128	NPCR and UACI are greater than 0.99, 0.32 respectively PSNR and NCs are greater than 35dB and 0.7 in many cases	-Nine different original images are measured
[123]	High imperceptible watermarking for medical images	Fragile	QIM, AES, substitutive watermarking procedure	100×100 ultrasound images of 576×688 pixels	PSNR > 60dB	-Delivers image honesty
[124]	Robust, secure, and imperceptible digital watermarking	Blind	SVD-DWT and error correction code	1024×1024/32×32 and 1022 bits	PSNR= 45 dB (X-ray2) BER=0	-Robust at checkmark attack
[127]	Imperceptible and robust digital watermarking	Blind	DCT, BCH code, H.264/AVC	I-frames/various number of bits	-PSNR is 55.45 dB -BER increases 1.06%	-Used to prevent the distortion error - Video orders are fixed during evaluation
[129]	Dual watermarking	Non-blind	BPNN, SVD, DWT, DCT, and encryption	512×512/128×128, 100 letters of text watermark	Max PSNR is 34.88dB For gain 0.1, NC is 0.9965 BER=0	-Offer a solution for social network information
[136]	Digital watermarking for EEG biomedical data	Blind	SVDD, DWT, and chaotic encryption	NA/32×32	-Normal PSNR is 66.55 -BER is 0 -NC is 1 -Error analysis is 0.97	Good imperceptibility and robustness is achieved

2.1.3. Optimization-based watermarking

A digital watermarking procedure designed on SVD and genetic algorithm (GA) is presented in [144]. For embedding a watermark, a singular vector is used in original media. The original image size of 512×512 and the watermark size of 32×32 are used for the watermarking process. Further, a genetic algorithm is implied here to enhance the result of the designed method. In [145], a wavelet-based watermarking technique is proposed. The scaling feature is applied to alter the singular vector of the original image along with a secret mark. Additionally, multi-objective particle swarm optimization (MOPSO) is applied here to optimize the trade-off between different constituents of digital watermarking.

A imperceptible and robust blind watermarking using transform domain (DWT, SVD) with support vector regression (SVR) and PSO is discussed in [23]. The SVD and DWT are used in watermark embedding to implant the watermark into the host image. Optimization is used to optimize the watermarking performance metrics. For evaluation, the cover image size of 512×512 and watermark size of 32×32 are taken into consideration. Evaluation outcome shows that this method achieved good transparency and robustness.

Author Ali and Ahn discussed a robust and imperceptible algorithm based on wavelet domain and cuckoo search [146]. The cuckoo search is used here for optimization to maintain a trade-off between PSNR and NC parameters of watermarking. The original image size of 256×256 size with two different watermark sizes 128×128 and 64×64 are taken for experimental analysis. Results indicates that the algorithm is appropriate for many watermarking applications. In [147], the author suggested a reversible watermarking for numeric relational data. The presented scheme is semi-blind watermarking grounded on GA. The proposed technique is robust in contrary to deliberate attacks. The author of [148], designed a watermarking algorithm grounded on DWT, SVD with guided dynamic particle swarm optimization (GDPSO). Stuckness and premature convergence are two difficulties of PSO [149]. GDPSO is applied here to conquer these two problems of PSO as it is appropriate watermark potency in DWT-SVD based watermarking system. The outcome of experimental analysis shows that it accomplishes good robustness and imperceptibility in comparison to other schemes [150]–[152]. In [153], the author suggested an optimal blind watermarking scheme for real-time applications. In this model, discrete Shearlet transform (DST), DCurvT, and grasshopper optimization are used. The cover image is decomposed by DST to acquire low-frequency bands, then DCurvT is operated on DST constants of the cover image. The watermark information is implanted with the host data to provide more security. The imperceptibility of the model is achieved by optimal quantities that are gained by employing DCurvT along with metaheuristic optimization (Grasshopper optimization). The experimental analysis shows that model is robust, imperceptible, and achieves additional security.

In this section, the optimization-based watermarking is discussed for multimedia data. A correlative study of image optimization watermarking is presented

in table 2.3. Moreover, these algorithms offer superior outcome in terms of imperceptibility and robustness.

Table 2.3 Comparative study of optimization-based watermarking

Ref.ID	Aim	Watermarking system	Techniques used	Host image size/ watermark image size	Outcome	Comments
[140]	Imperceptible and robust watermarking	NA	SVD and GA	512×512//32×32	Results are obtained at phases of GA	-Number of generations is 400 for each experiment. - GA iterates 30 times at distinct populations
[141]	Imperceptible and robust watermarking	Blind	LWT, MOPSO, SVD	256×256/32×32	-For Boat, PSNR is 54.907 dB and NC is 1	-Multiple scaling factors are used
[19]	Imperceptible and robust watermarking	Blind	SVD, DWT, PSO, SVR	512×512/32×32	-NC is 0.988 -PSNR is greater than 35dB	-Computation time is high
[142]	Imperceptible and Robust digital watermarking	NA	Cuckoo search and DWT	256×256/ 128×128,64×64	- PSNR is 38.0358 (for two distinct watermarks) - Image Pepper at 1 st level DWT NC is 0.9613 - Image Baboon, Lena, Pepper at 2 nd level NC is 1	Stability among inconsistent features of digital watermarking
[143]	Robust digital watermarking	Semi-Blind	Watermarking with GA	More than 300 tuples	- Max mean and variance are 55.019, 81.697 correspondingly	-No. of productions are 100 and population size is 50 - Result analysis at various datasets
[144]	Imperceptible and robust digital watermarking	Non-blind	DWT, GDPSO, SVD	512×512/512×512	-Applying GDPSO, PSNR is 36.877771, and fitness value is 1.977786 - Applying DWT-SVD with GDPSO, PSNR is 39.792252, and fitness value is 1.984123	-GDPSO provides better results than PSO -Offered method resist to various attacks also

[148]	Robust and secure image watermarking	Blind	DST, DCurvT, and Grasshopper Optimization	512x512/-	PSNR=56.78dB (for trial 1000) PSNR=54.11dB (for trial 2000)	Computation time is high
-------	--------------------------------------	-------	---	-----------	--	--------------------------

Table 2.4 Investigation on various watermarking characteristics on image watermarking

Reference Number (Study ID)																
Parameters	[1]	[2]	[140]	[141]	[118]	[32]	[19]	[20]	[35]	[36]	[41]	[43]	[47]	[122]	[48]	[52]
Accuracy	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Bit error rate	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Computational complexity	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Distortions	x	✓	x	x	x	x	x	x	x	✓	x	x	x	x	x	x
Efficiency	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Embedding Capacity	x	x	x	x	✓	x	x	x	✓	x	x	x	x	x	✓	x
Imperceptibility	✓	x	✓	✓	x	x	✓	x	x	x	x	x	✓	x	x	x
Payload	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x
Preserves image quality	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Robustness	✓	x	✓	✓	✓	✓	✓	✓	x	x	✓	x	✓	x	x	✓
Security	x	x	x	x	x	✓	x	x	x	x	x	x	x	✓	x	✓
Reference Number (Study ID)																
Parameters	[54]	[60]	[64]	[65]	[66]	[123]	[68]	[76]	[77]	[80]	[81]	[124]	[82]	[83]	[84]	[85]
Accuracy	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Bit error rate	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x
Computational complexity	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x
Distortions	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	x	x
Efficiency	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Embedding Capacity	x	x	x	✓	x	x	x	x	x	x	x	x	x	✓	x	x
Imperceptibility	✓	x	x	x	x	x	x	x	✓	x	x	✓	x	x	✓	x
Payload	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Preserves image quality	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x
Robustness	✓	x	x	x	x	x	✓	x	✓	x	x	✓	✓	x	✓	✓
Security	✓	✓	✓	x	✓	x	x	✓	✓	x	x	✓	x	x	x	✓
Reference Number (Study ID)																
Parameters	[86]	[142]	[127]	[128]	[87]	[88]	[90]	[97]	[136]	[101]	[103]	[108]	[143]	[109]	[114]	[115]
Accuracy	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Bit error rate	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Computational complexity	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Distortions	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Efficiency	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Embedding Capacity	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Imperceptibility	x	✓	x	x	✓	✓	x	✓	✓	✓	x	x	x	✓	x	x
Payload	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Preserves image quality	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Robustness	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Security	x	x	x	✓	x	x	✓	x	x	x	✓	x	x	x	x	x
Reference Number (Study ID)																
Parameters	[144]	[117]	[148]													
Accuracy	x	x	x													
Bit error rate	x	x	x													
Computational complexity	x	x	x													
Distortions	x	x	x													

Efficiency	×	×	×
Embedding Capacity	×	✓	×
Imperceptibility	✓	✓	✓
Payload	×	×	×
Preserves image quality	×	×	×
Robustness	✓	✓	✓
Security	×	×	✓

The following fig. 2.1 shows the techniques used to measure the robustness for watermarking system. Various host and watermark images used in image watermarking are labelled in table 2.5. These studies show that the bigger pixel value has less impact of watermark on the host image. Therefore, most research has been carried out by considering images of bigger pixel values.

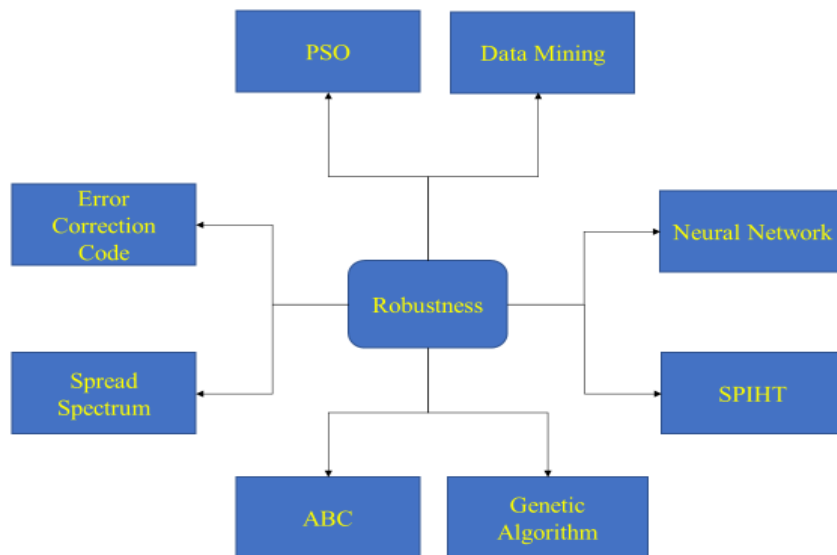


Fig. 2.1: Identifying the techniques used to measure robustness in image watermarking

Table 2.5 Analysis of various studies according to size of host and watermark image used in image watermarking

Image size Watermark size	1024×1024 Pixels	512×512 Pixels	256×256 Pixels	128×128 Pixels	64×64 Pixels	32×32 Pixels	4×4 Pixels
4 × 4	-	-	-	-	-	-	-
32 × 32	-	[1] [19] [41] [97] [115] [140]	[141]	-	-	-	-

64 × 64	-	[68] [87] [109]	[142]	-	-	-	-
128 × 128	[54]	[122]	[142]	-	-	-	-
256 × 256	-	[77] [90] [122]	[117]	-	-	-	-
512 × 512	-	-	[144]	-	-	-	-
1024×1024	-	-	-	-	-	-	-

2.2. Comparative analysis of transform domain watermarking

This section shows the comparison of six different transform domain-based watermarking procedures grounded on PSNR and NCC. These procedures were also evaluated for several attacks. Transform domain methods like DWT, DCT, SVD, DConT, DCurvT, and QHT are explained in detail. The outcome of these procedures shows that it can achieve good robustness and imperceptibility, as well as can resist attacks.

2.2.1. Structure of digital image watermarking

Digital image watermarking is defined as hiding secret information in the original data and operated in the digital domain where it inserts a secret data (image). A general watermarking scheme is explained in below fig. 2.2.

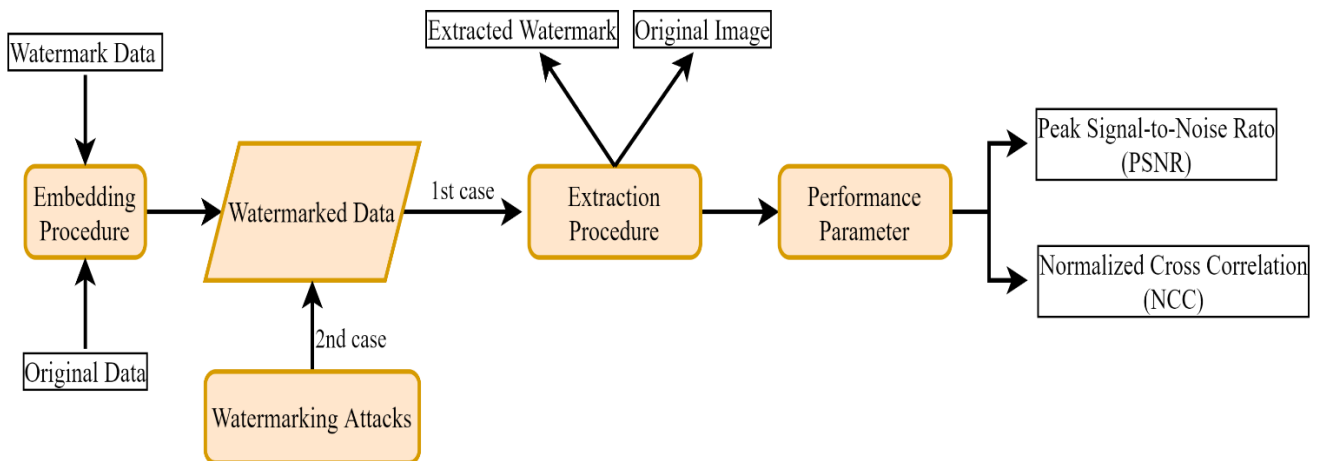


Fig.2.2: Watermarking system

The working of digital watermarking mainly comprises of three different steps: the watermark, the embedding procedure, and the extraction procedure. To generate or apply watermarks in original media, image processing operations and image transforms are generally used [154]. In watermark embedding, it consists of original data and

watermark data to produce watermarked data. Watermarking procedure can be applied to both spatial and transform domains. In the spatial domain, pixels are altered for both the watermark and the host image [155], [156]. In the other domain, watermark information is encoded in the constants of DWT, DCT, SVD, DCurvT, DST, and QHT. After that, a recovery method is employed to recover the watermark and original media from the watermarked media. And some watermarking attacks can also be imposed during the communication of watermarked data [157]–[159]. The main features considered during watermarking are robustness, imperceptibility, security, and embedding capacity.

2.3. Preliminaries of transform domain watermarking

A brief description of the transform domain watermarking system is described in below section:

a.) Discrete wavelet transforms (DWT)

Wavelets are extremely important for transformation in image processing and digital watermarking as it has very good energy compaction and excellent space property [146]. In DWT, a discrete-time signal is converted to discrete wavelet depictions [160]. It has a feature of multi-resolution breakdown. The functional and arithmetical analysis of DWT is wavelet transform where wavelets are tested at periods by some predefined set of instructions [161]. Discrete wavelet transform is beneficial in eliminating the noise from the data [162]. DWT is the frequency domain analysis of an image [163]. At every level, DWT analysis for an image is decayed into 4 sub-bands. These sub-bands are classified as low pass and high pass filters [154]. Actual information of image data is given by low passbands and information such as edges of the image is acquired by high pass bands. Fig. 2.3 is a representation of 2nd level DWT decomposition. Furthermore, DWT sub-bands [164] are explained below:

- Approximation sub-bands (LL) are a lower-frequency constituent in both vertical and horizontal.
- Horizontal sub-bands (LH) are a lower-frequency constituent in horizontal and higher-frequency constituent in vertical.
- A vertical sub-band (HL) is a higher-frequency constituent of a horizontal and low-frequency constituent in vertical.

- The diagonal sub-band (HH) is a higher-frequency constituent of both horizontal and vertical.

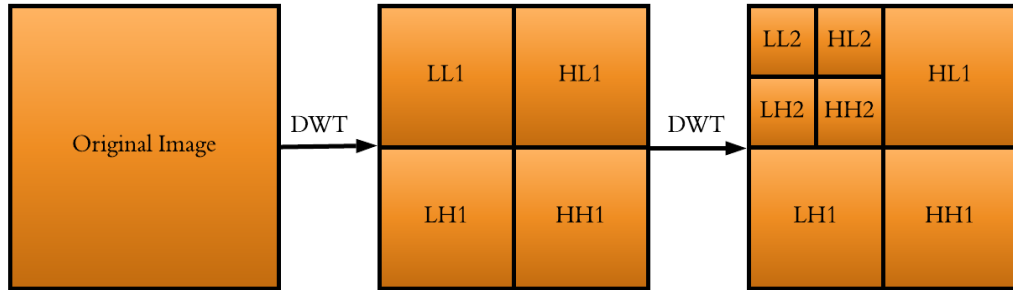


Fig.2.3: Representation of second level DWT decomposition

The original data is embedded by a watermark by applying a DWT_x algorithm ($x=1,2,3\dots$ levels of DWT decomposition), then apply the inverse of the DWT (IDWT) to acquire the signed image. In the recovery method, watermarked image is given as input, then apply the DWT of the same level. After that, the watermark image is gained by applying IDWT. Fig. 2.4 represents the watermarking processes in the DWT domain.

b.) Discrete cosine transform (DCT)

The cosine transforms are applied to decompose an image to transform domain from spatial domain [165] [166]. DCT works in separating an image into equivalent frequency coefficients. DCT has a good energy compaction property i.e., acquiring lots of energy in fewer coefficients, applied in image and signal processing. Energy compaction property can be depleted to choose the appropriate constants in watermark embedding [167]. DCT is also good for image compression [162]. Fig. 2.5 denotes the watermarking procedures in the DCT field.

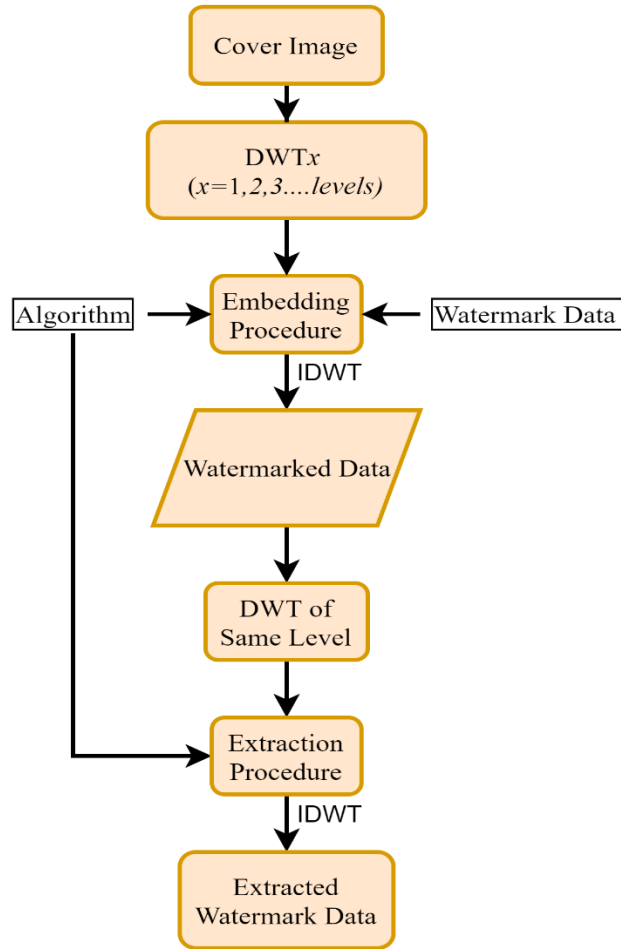
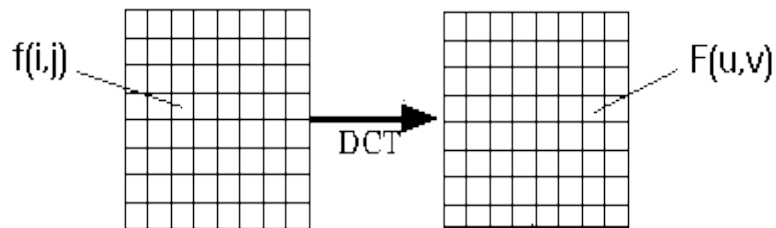


Fig. 2.4: Watermarking embedding and extraction in DWT domain



The equation for 1D DCT for N data points is described below in eq. 1:

$$F(p) = \left(\frac{2}{N}\right) \sum_{i=0}^{\frac{1}{2}N-1} A(x) \cdot \cos \left[\frac{\pi \cdot p}{2 \cdot N} (2x+1) \right] f(x) \quad (1)$$

The 1D DCT conversion to its inverse is $F^{-1}(p)$, is indicated in eq. (2)

where,

$$A(x) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for } \epsilon = 0 \\ 1 & \text{else} \end{cases} \quad (2)$$

Eq. 3 specified the 2-Dimension DCT as follows:

$$F(p, q) = \left(\frac{2}{N}\right)^{1/2} \left(\frac{2}{M}\right) \sum_{i=0}^{\frac{1}{2}N-1} \sum_{j=0}^{M-1} A(x) \cdot A(y) \cdot \cos\left[\frac{\pi \cdot x}{2 \cdot N}(2p+1)\right] \cos\left[\frac{\pi \cdot y}{2 \cdot M}(2q+1)\right] \cdot f(x, y) \quad (3)$$

further eq. (4) denotes the 2D inverse DCT:

where,

$$A(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for } \xi = 0 \\ 1 & \text{Otherwise} \end{cases} \quad (4)$$

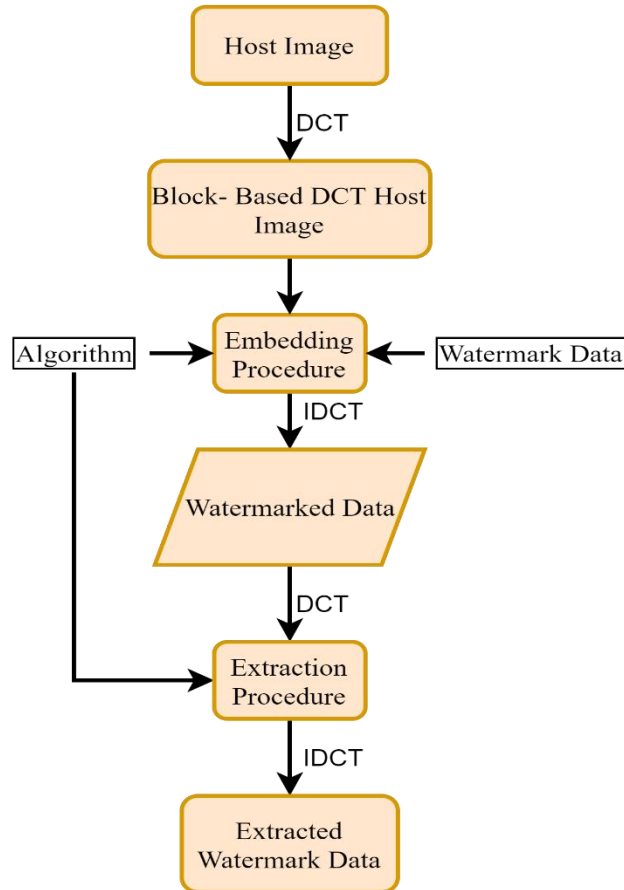


Fig. 2.5: Watermark embedding and extraction in DCT domain

c.) Singular value decomposition (SVD)

To evaluate matrices, SVD is treated as an arithmetical instrument in image processing [168]. The SVD transformation is broadly useful in digital signal processing and statistics [162]. A four-sided matrix is disintegrated into three matrices of equivalent size. The SVD matrix is defined in eq. 5.

$$\text{SVD (I)} = \text{USV}^T \quad (5)$$

where S represents diagonal matrix whereas orthogonal matrices are U and V [169].

The brightness and geometry properties of the image can be well signified by singular values [161]. This transform guarantees excellent stability in an image if little discrepancy befalls. So, deprivation is not appeared in the visual quality of a watermarked image [170].

d.) Quaternion hadamard transform (QHT)

QHT defines as an assortment of Hadamard transformation and quaternion revelation. In QHT, the quaternion number denotes that there is no loss of any color information [171]. A Walsh function is created when Hadamard sinusoidal and orthogonal transformation divides a signal or an image into a set of orthogonal and rectangular waveforms. Hadamard transform provides easy hardware execution, simple functioning, the computational cost is low which is also affluent for watermarking [105]. The two basic properties of this transform: - first elements are real and the second, row and column are orthogonal to each another.

e.) Discrete curvelet transform (DCurvT)

In the last few years, Candas [172] has announced a recent transform called Curvelet transform in the hierarchy of wavelet transforms. This transform resolves the issues raised by multiscale depictions. This is multiresolution transmute and offers the optimal sparse representations of the image matrix [173]. In image processing operations, wavelet transform is required to signify images more accurately. Moreover, wavelet transform is not appropriate to illustrate the objects casing aimlessly sloping boundaries as a curve and corners as an edge. Images are a combination of both corners as an edge and boundaries as a curve, therefore, demand a transform that can analyse both curves and edges accurately. This transform has orientation, direction, and scaling

parameters, due to which, it has a property of line singularity [174]. Curvelet transforms are a multiscale pyramid along with directions to be defined and obtain a sparse representation [175].

f.) Discrete contourlet transform (DConT)

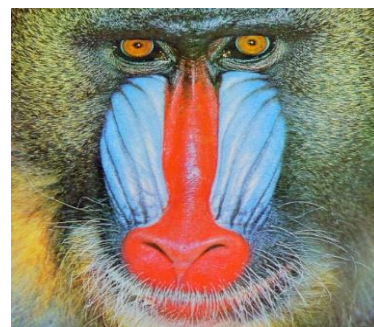
Contourlet transform is introduced by Do and Vetterli [176] and implemented by using PDFB (Pyramidal Directional Filter Bank) for multiresolution illustrations of images. The Laplacian pyramid in the contourlet transform decomposes an image in two bands in which one is lowest-frequency sub-bands and the other is highest-frequency sub-bands. By using directional filter banks, directional decomposition is applied to every bandpass. The main property of this transform over others is that it allows to contain distinct directions of diverse scales of an image while gaining critical sampling [177]. As it retains iterated filter banks, it is computationally easy. Contourlet transform is important in image watermarking because of its spreading property. This transform is not equal to the number of directional banks that can be identified by the person at any resolution and able to capture the directional edges of an image. So, the image is illustrated in form of directional sub-bands at multiple scales.

2.4. Experimental setup

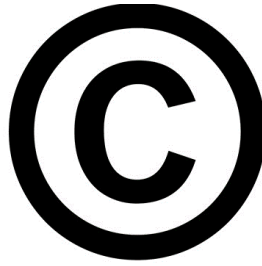
The comparison of six different transform domain methods is performed with four different standard images such as Pepper, Barbara, Lena, and Baboon of 512×512 size. The copyright symbol is taken as a watermark image of size 64×64.



i.



ii.



iii.



iv.

Fig. 2.6: i.), ii.) host image and iii.) secret image iv.) signed image

Table 2.6 Results of SVD, DCT, and DWT for different images

S. No.	Image	SVD		DCT		DWT	
		PSNR	NCC	PSNR	NCC	PSNR	NCC
1	Pepper	51.23	0.9921	50.87	0.9973	48.15	0.9955
2	Barbara	51.24	0.9923	50.89	0.9974	48.13	0.9958
3	Lena	51.26	0.9924	50.88	0.9974	48.12	0.9956
4	Baboon	51.25	0.9923	50.89	0.9974	48.14	0.9956

Table 2.7 Results of DconT, QHT, and DcurvT

S. No.	Image	DConT		QHT		DCurvT	
		PSNR	NCC	PSNR	NCC	PSNR	NCC
1	Lena	51.97	0.9959	53.77	0.9993	52.89	0.9988
2	Barbara	51.95	0.9962	53.76	0.9995	52.85	0.9984
3	Pepper	51.96	0.9962	53.76	0.9996	52.88	0.9985
4	Baboon	51.95	0.9963	53.78	0.9994	52.88	0.9985

Table 2.8 Results of SVD, DCT, and DWT for attacks

Images	Attacks	SVD		DCT		DWT	
		PSNR	NCC	PSNR	NCC	PSNR	NCC
Lena	Rotation	33.45	0.9629	33.88	0.9661	34.49	0.9706

	Salt & Pepper (0.01)	33.65	0.9647	34.08	0.9681	34.75	0.9722
	JPEG (90)	33.81	0.9659	34.14	0.9692	34.92	0.9735
	Gaussian Noise (0.01)	33.52	0.9639	33.95	0.9675	34.53	0.9711
Barbara	Rotation	33.42	0.9615	33.88	0.9661	34.45	0.9701
	Salt & Pepper (0.01)	33.65	0.9647	34.09	0.9685	34.75	0.9722
	JPEG (90)	33.79	0.9655	34.14	0.9692	34.88	0.9731
	Gaussian Noise (0.01)	33.55	0.9645	33.92	0.9669	34.51	0.9708

Table 2.9 Results of DconT, DCurT, and QHT for attacks

Images	Attacks	DConT		DCurvT		QHT	
		PSNR	NCC	PSNR	NCC	PSNR	NCC
Lena	Rotation	34.99	0.9749	35.98	0.9799	38.59	0.9879
	Salt & Pepper (0.01)	35.55	0.9782	36.55	0.9842	38.57	0.9872
	JPEG (90)	35.76	0.9791	36.15	0.9827	38.66	0.9882
	Gaussian Noise (0.01)	35.14	0.9765	36.88	0.9856	38.47	0.9865
Barbara	Rotation	35.01	0.9755	35.98	0.9799	38.56	0.9871
	Salt & Pepper (0.01)	35.55	0.9782	36.61	0.9844	38.55	0.9869
	JPEG (90)	35.82	0.9795	36.05	0.9815	38.69	0.9885
	Gaussian Noise (0.01)	35.15	0.9769	36.85	0.9851	38.47	0.9867

In this chapter, the literature on various domain-based watermarking, encryption-based watermarking, and optimization-based watermarking has been discussed. Further, a comparison of six different transform-domain watermarking procedures has been presented in a normal and noisy environment.

CHAPTER-3

ROBUST AND SECURE COLOR IMAGE

WATERMARKING WITH PAILLIER

HOMOMORPHIC CRYPTOSYSTEM

AND ARNOLD TRANSFORMATION

Chapter-3

ROBUST AND SECURE COLOR IMAGE WATERMARKING WITH PAILLIER HOMOMORPHIC CRYPTOSYSTEM AND ARNOLD TRANSFORMATION

This chapter presents color image watermarking with homomorphic encryption with Arnold transformation for the robust and secure transmission of digital content. In this scheme, transform domain techniques DWT-DCT are employed in encrypted domain. To encrypt the original media, cryptosystem is exploited here. Further, for the security of digital media, watermark image is twisted through Arnold scrambling method, and achieved prior to the embedding process. There are many scrambling techniques available in the literature, Arnold transform is used in this work because it is an iterative process to alter the coordinates of pixel position to change the layout of an image. On one hand, an encoded watermarked image is generated after the embedding process with encryption. On the other hand, an extracted watermark is obtained after the extraction process with decryption rules. The performance of the discussed method is tested with watermarking performance parameters like PSNR and NC. Further, some encryption parameters such as NPCR and UACI are also estimated. The presented method is also evaluated for different attacks.

3.1. Introduction

In real-world scenarios, multimedia contents is rising with a terrible amount, so these data need to be secured efficiently [178]. However, content is not secured over the internet because of manipulating, copying, replicating, storing, or deletion. Some efficient methods are required to avoid unauthorized access to data. So, researchers analyzed that digital watermarking is suitable for it. Image watermarking was found to be an inspiring research topic that includes ethics and methods of exchanges, signal processing, and encryption [179]. This research has many applications towards a proficient watermarking system that can be positively applied in spatial and/or transform domains. Further, some robust, secure, and imperceptible watermarking techniques with transform domain and encryption are discussed. In [180] author has used Rivest, Shamir, Adleman (RSA) encryption with logistics, for robust and secure watermarking. The author proceeds their work in RSA encryption for embedding and logistic scrambling. The outcome of watermarking is found to be better in comparison to others. The

technique that works with the DWT-SVD domain is observed to be robust. However, a disadvantage of this technique is that it extracts watermark data in an informed way. This procedure involves both original and watermark data for extraction. Further, LSB and AES encryption are used for the medical cloud to secure the medical data (images and reports) in [181]. In this scheme, the LSB technique is exploited to hide the reports, and AES encryption is utilized here to encrypt the text file in the medical data. This technique achieves better results as compared to other methods. A buyer-seller image watermarking method with DCT and homomorphic encryption is discussed in [182]. The authors claimed that their algorithm has good perceptibility against attacks. Paillier cryptosystem is discussed for large and increasing dataset administering in [183]. Cryptosystem shows a foremost part in this dataset and achieves better performance. The author of [184] discussed a concept of Homomorphic image watermarking with SVD. The secret information is encrypted by applying chaotic encryption. Homomorphic transform is used before embedding, then SVD is employed over the original signal. Embedding is ensured in a block-by-block mode and achieved better outcomes. But authors have reported that encryption is not applied in the host signal. Both symmetric and asymmetric encryption schemes have their merits and demerits related to image watermarking. Multiplicative homomorphic encryption such as RSA is found to be slower than Additive homomorphic encryption like Paillier cryptosystem. The reason behind initiating homomorphism in encryption is that without decryption, the encoded message can be functioned [185]. Recent cryptography trails durable scientific schemes and cryptographic procedures and such procedures are stiff to disrupted by an unauthorized person. Due to the importance of encryption and watermarking for multimedia data, a secure and robust watermarking system for color images, by operating Arnold transform and cryptosystem is described here. This chapter has the subsequent contributions:

- The watermarking scheme with the grouping of DWT and DCT performed superior.
- The confidentiality of watermark data is upgraded by applying the Arnold scrambling into watermark data and generating the scrambled watermark image.
- The cover image and scrambled watermark image are undergoing encryption procedures. Further, the embedding process is done on both encrypted images and the encrypted watermarked image is generated.
- Results indicated that our technique gives a better outcome for several image processing attacks, some are salt & pepper, filtering, JPEG compression, and rotation.

3.2. Paillier homomorphic cryptosystem

A French researcher Pascal Paillier (1999) invented an asymmetric key cryptography system called as Paillier cryptosystem. The Asymmetric cryptography method is a grouping of both, the public and private keys. In this system, the private key is reserved secretive while the public key gets dispersed. By use of a public key, information is encrypted and by private key, information is decrypted [186].

3.2.1. Key generation steps

- 1.) Two numbers (prime) r and s are chosen randomly but not dependent to one another such as,

$$\text{gcd}(rs, (r-1)(s-1)) = 1 \quad (1)$$

- 2.) Evaluate n ,

$$n = rs, \quad (2)$$

$$\lambda = \frac{|(r-1)(s-1)|}{\text{gcd}(r-1, s-1)} \quad (3)$$

where, gcd is the greatest common multiple.

- 3.) Choose one number (random) u , where, $u \in \mathbb{Z}_{v^2}^*$.
- 4.) Confirm v divides u , the multiplicative inverse is represented in eq. 4

$$\mu = (X(u^\lambda \bmod v^2))^{-1} \bmod v \quad (4)$$

where, X is represented as

$$X(a) = \frac{(a-1)}{v} \quad (5)$$

3.2.2. Encryption

- 1.) Pick i as information to be ciphered where $i \in \mathbb{Z}_v$
- 2.) Choose casual digit r , where $r \in \mathbb{Z}_v^*$
- 3.) Compute ciphertext:

$$ca = i^u \cdot r^n \bmod v^2 \quad (6)$$

3.2.3. Decryption

- 1.) Now decrypt the ciphertext data ca , where $ca \in \mathbb{Z}_{v^2}^*$
- 2.) Compute the plaintext data as represented in eq. 7:

$$u = X(ca^\lambda \bmod v^2). \mu \bmod v \quad (7)$$

3.3. Arnold transformation

The watermark image must be scrambled prior to embedding, to develop the security of the host image. It is a continual procedure to vary the pixels of the image to transform the arrangement of an image [187]. The image scrambling method provides a non-password security algorithm for data hiding. It has a feature of periodicity and simplicity so it is broadly utilized in digital watermarking [84]. Due to the periodicity property, an original image can be brought back after several cycles. The periodic feature of Arnold transformation is conditional on the image size for restoring an image because it has to wait for a long time [188]. The transformation of pixel coordinates (a, b) in the unit square changing to other coordinates (A', B') is defined in the following eq 8.

$$\begin{bmatrix} A' \\ B' \end{bmatrix} = \left\{ \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} \pmod{1} \right\} \quad (8)$$

where P' and Q' are transformed pixel coordinates. The places of pixels are varying from one point to other.

$$\begin{bmatrix} A' \\ B' \end{bmatrix} = \left\{ \begin{bmatrix} 1 & m \\ n & mn + 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} \pmod{N} \right\}^Q \quad (9)$$

Eq. 9 illustrates the 2D Arnold transformation of the image matrix, where A' and B' are transferred pixel coordinates of a and b after Q repetitions, N denotes the size of the digital image, and m and n are two positive integers.

3.4. Proposed Paillier homomorphic cryptosystem-based watermarking

The proposed block diagram is employed for a digital image watermarking scheme in an encrypted environment with transform domain (DWT-DCT) for amending the robustness and security of multimedia data. A complete watermarking procedure is demonstrated in the following figure 3.1. Firstly, the original image 'A' is encoded by operating homomorphic encryption in the hybrid transform (DWT-DCT) domain. Here, the original image is disintegrated by DWT to achieve coefficients of DWT, then DCT is operated on particular DWT coefficients to acquire encrypted image 'E[A]'. Afterward, a scrambled watermark image is produced by the exploitation of Arnold transformation and obtained prior to the

embedding process. Then scrambled watermark image is underdone for the encryption process and generates an encrypted scrambled image 'E[W]'. Further, the encrypted original information is embedded by encrypted scrambled watermark image to generate an encoded watermarked image 'E[AW]'. Subsequently, the extraction process and decryption are employed to extract the watermark image and the original image.

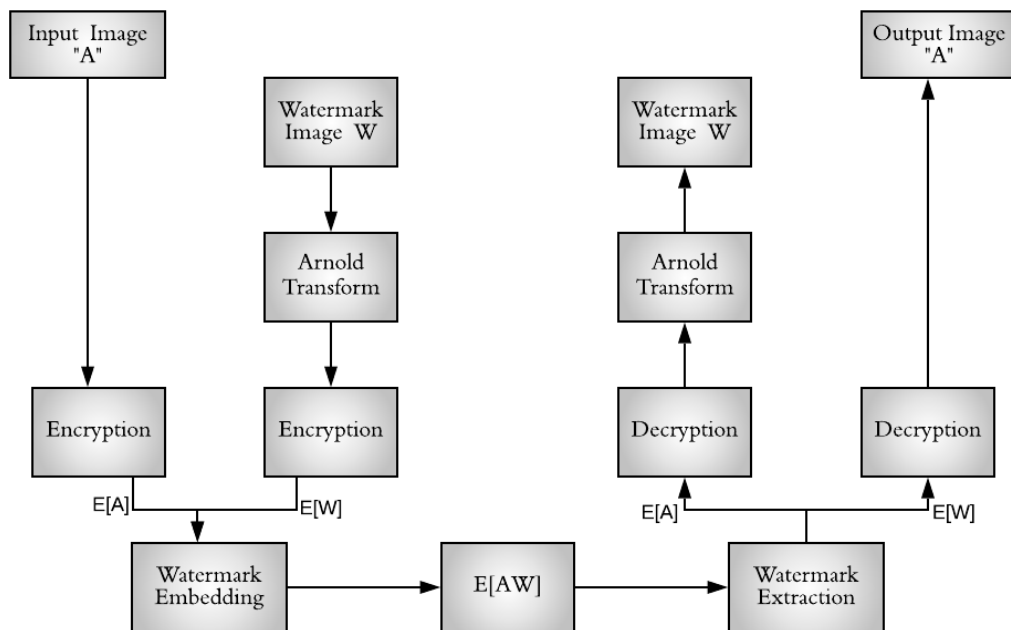


Fig. 3.1: Diagrammatic representation of the proposed watermarking system

Watermarking procedures are carried out in an encrypted domain. The extraction procedure is just contrary to an embedding procedure. The following sub-section defines the embedding and extraction procedure of the presented system.

3.4.1. Steps for embedding

The embedding procedures are explained below:

- a.) Firstly, upload a cover image of size 512×512 , and 32×32 is the size of the watermark image.
- b.) Cover image is decayed by DWT and generates DWT constants as dA , dH , dV , dD sub-bands.
- c.) Then, DCT is operated on individually wavelet constants to attain the DCT constants like $dA'(r, s)$, $dH'(r, s)$, $dV'(r, s)$, $dD'(r, s)$.

- d.) Then encryption process is functional on both scrambled image matrix and all DCT constants of the cover image.
- e.) Watermark embedding of the cover image is done using the equation number 10 as follows:

$$X = Y + \alpha \times Z \quad (10)$$

where X is an encrypted watermarked image matrix, Y symbolizes an encrypted original image matrix in DWT-DCT domain, α is the gain value and Z signifies the scrambled watermark image.

- f.) Post embedding procedure requires converse of DCT, then DWT is retained to acquire the watermarked image (encrypted).
- g.) The key is produced by implementing the XOR function between the encoded host matrix and the scrambled watermarked matrix.
- h.) Lastly, watermarked image is displayed.

3.4.2. Steps for extraction

The extraction procedures are described below:

- a.) Here, a decryption procedure is done on the encoded watermarked image to achieve a decrypted watermark image
- b.) A DWT decomposition is employed on decoded watermark images to achieve DWT constants as $dA1$, $dH1$, $dV1$, $dD1$.
- c.) A DCT is done on the same DWT constants to perceive DCT constants as $dA11(r, s)$, $dH11(r, s)$, $dV11(r, s)$, $dD11(r, s)$.
- d.) Now, the watermark image is extracted by using the equation number 11 as follows:

$$A = \frac{B-C}{\alpha} \quad (11)$$

where A is the recovered watermark image, B represents the watermarked image (encrypted), C denotes the original image (encrypted) and α is a gain value.

- e.) After this process, inverse is employed over operated methods i.e., IDCT then IDWT to extract the watermark image.

Following figure 3.2 denotes the embedding procedure in an encrypted domain.

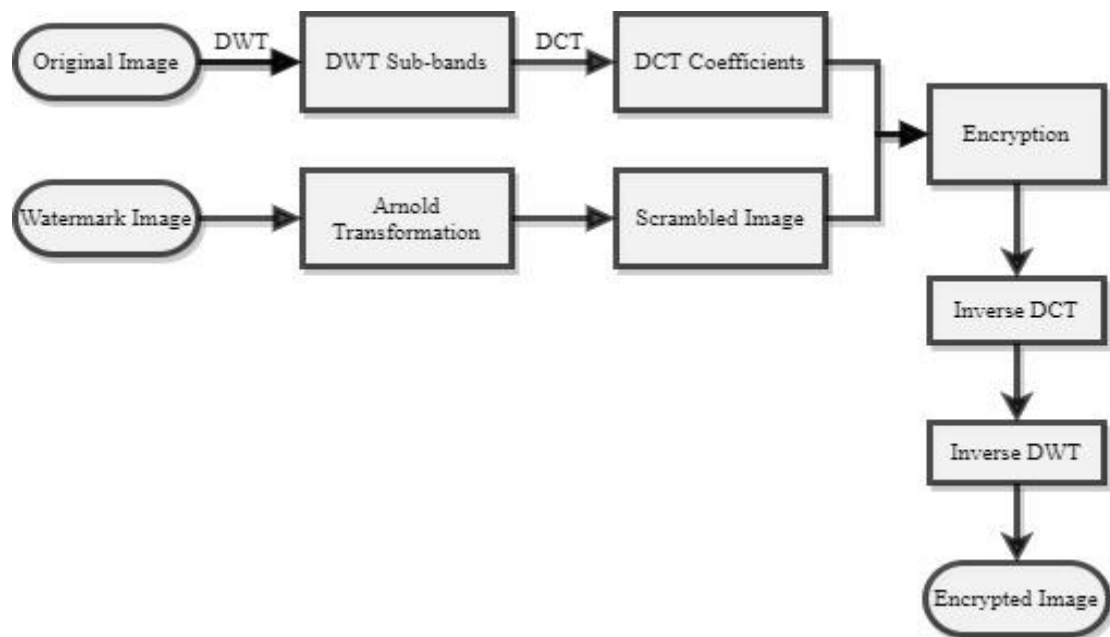


Fig. 3.2: Encryption Process

3.5. Experimental outcomes

The 512×512 and 32×32 size of the cover and watermark image are taken for experimental purpose. The PSNR and NC watermarking parameters are used to determine the impact of our method along with two encryption metrics NPCR and UACI, for the encryption scheme. A detailed explanation of these performance parameters is presented in chapter 1.

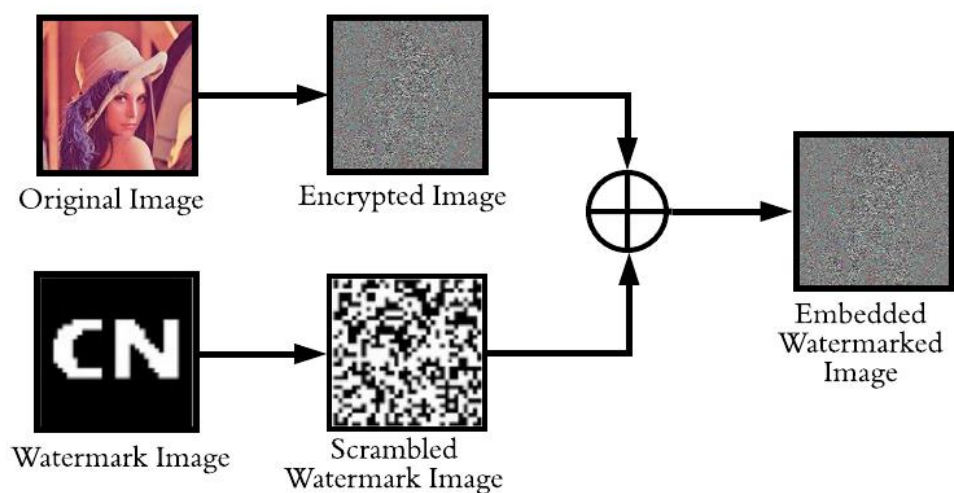


Fig. 3.3: Watermarking process for image Lena

Figure 3.3 is a representation of watermarking outcome for original and watermark images. The encryption process is applied to the original image to get an encrypted image, whereas Arnold transformation is employed on the watermark image to get a scrambled watermark image. After that embedding process is implemented to acquire the encrypted watermarked image. Table 3.1 shows the performance evaluation of PSNR, NC, NPCR, and UACI for six dissimilar standard images (Barbara, Lena, Goldhill, Mandrill, Peppers and Football) at a gain value of 0.01. Fig. 3.4 and fig. 3.5 depict the graphical illustration of NPCR and UACI results for distinct images respectively. From table 3.1, the finest PSNR found is 56.98 and the NC value from image Lena is 0.9974. Though, the lowest PSNR is 55.78 from Football image, and lowest NC is 0.9735 from the image Goldhill. Further, it is interesting to see that both NPCR and UACI are in an acceptable range.

Table 3.1 Performance analysis of proposed method

Sr. No.	Images	PSNR	NPCR	UACI	NC
1	Barbara	56.95	0.9954	0.3737	0.9968
2	Lena	56.98	0.9959	0.3444	0.9974
3	Goldhill	56.52	0.9952	0.3735	0.9735
4	Mandrill	56.55	0.9959	0.4464	0.9965
5	Peppers	56.12	0.9961	0.4572	0.9824
6	Football	55.78	0.9958	0.4501	0.9799

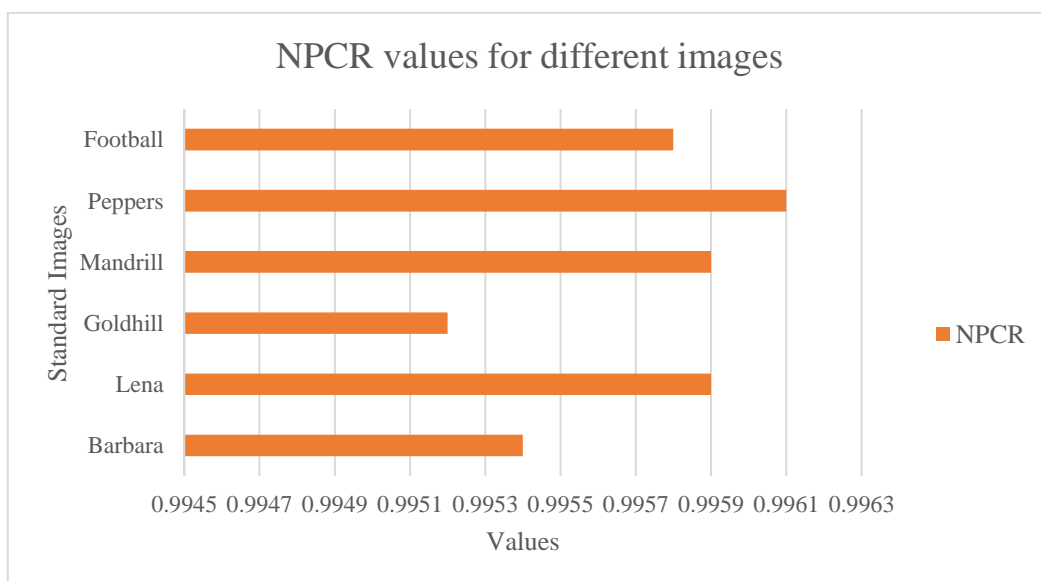


Fig. 3.4: NPCR values for standard images

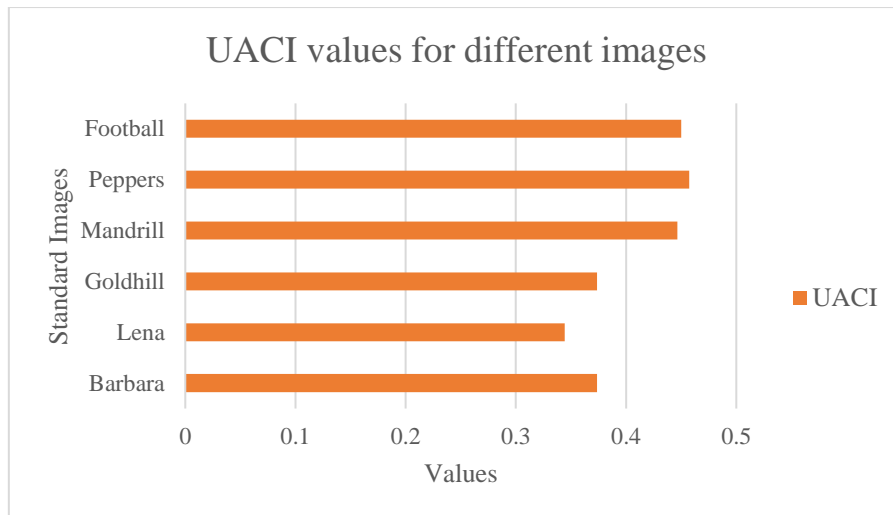


Fig. 3.5: UACI values for standard images

Table 3.2 compiles the NC value after applying watermarking attacks on six different images and values are attained within expected limits. At this time, salt & pepper noise is examined at 0.01, Gaussian noise at 0.01, JPEG is examined at (QF 90), rotation attack at 30° , and cropping attack at the top left corner of the image. So, this table displays that the proposed technique is sufficient robust for at least some particular watermarking attacks. Fig. 3.6 demonstrates the NC values attained under distinct attacks.

Table 3.2 NC values under several attacks

Image/ Attacks	Filtering (3x3)	Salt & Pepper Noise	Gaussian Noise	Rotation (30°)	JPEG (90)	Cropping
Lena	0.9684	0.9785	0.9726	0.9678	0.9816	0.9671
Mandrill	0.9779	0.9732	0.9719	0.9755	0.9799	0.9722
Barbara	0.9729	0.9788	0.9732	0.9725	0.9821	0.9745
Football	0.9742	0.9699	0.9722	0.9695	0.9818	0.9674
Peppers	0.9712	0.9685	0.9765	0.9682	0.9795	0.9688
Goldhill	0.9685	0.9739	0.9715	0.9679	0.9789	0.9669

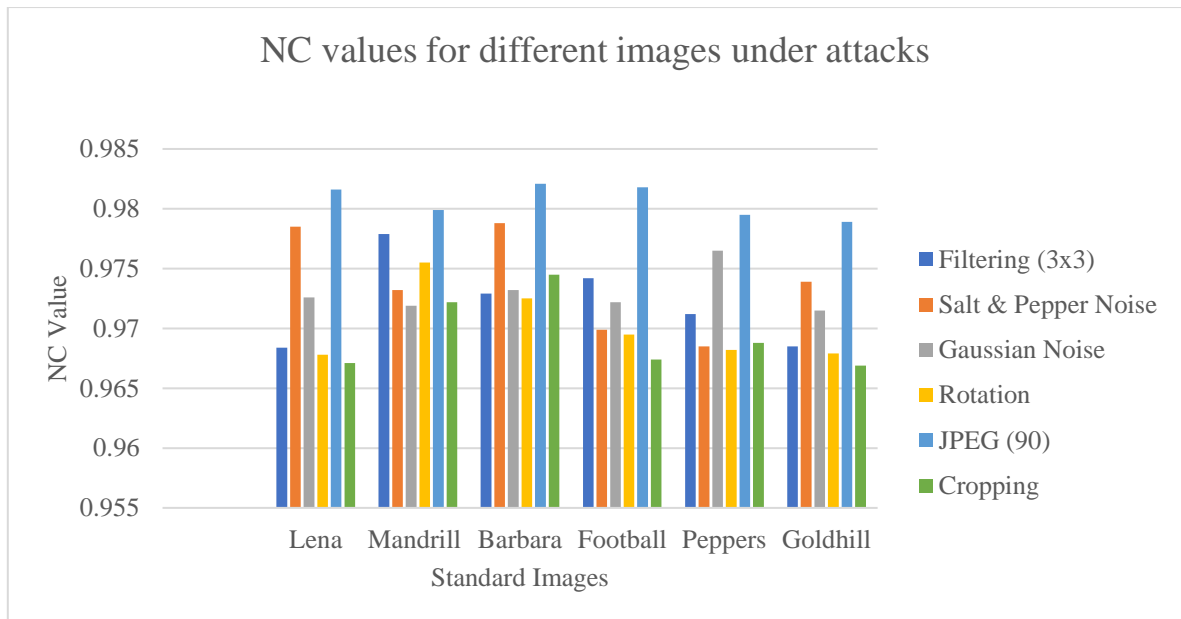


Fig. 3.6: NC values for standard images under watermarking attacks

Further, our approach is compared with two previous methods. Table 3.3 illustrates the comparison of the PSNR value of signed images of proposed method with previous methods. It is noted from the table that the visual quality of signed images is acceptable. Table 3.4 illustrates the comparison of NC values from previous methods. Fig. 3.7 shows the graphical depiction of PSNR value, compared with previous techniques. The quantitative analysis of the suggested method is shown in table 3.4. The outcome shows that the proposed technique achieves better robustness as compared to previous techniques.

Table 3.3 Comparative analysis of proposed method with previous methods

Images	Su et al. (2018) [183]	Das et al. (2014) [184]	Proposed Method
Peppers	50.08	41.01	56.12
Lena	49.98	41.78	56.98

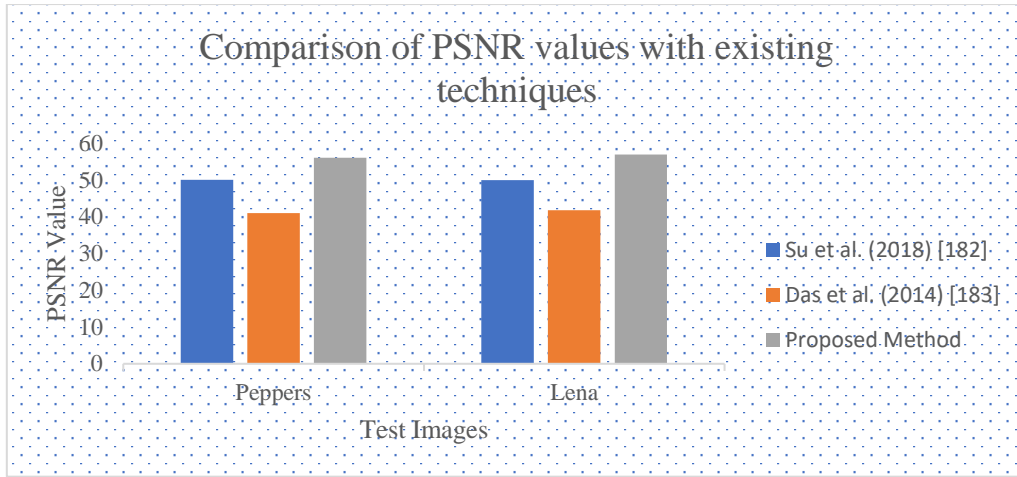


Fig. 3.7: Comparative analysis of PSNR with previous techniques

Table 3.4: Comparative analysis of NC values with previous methods for attacks

S. No.	Images	Attacks/ Noise Density	Proposed Method	Method of Su et al. (2018) [189]	Method of Das et al. (2014) [190]
1	Lena	Salt & Pepper (0.01)	0.9785	0.9009	0.6731
2	Peppers		0.9685	0.9378	0.7866
3	Lena	Filtering (3x3)	0.9684	0.9977	0.9118
4	Peppers		0.9712	1	0.9233
5	Lena	Rotation (30 ⁰)	0.9678	0.7612	0.7612
6	Peppers		0.9682	0.7851	0.7851

In summary, this chapter offers an enhanced method for secure and robust watermarking for color images by Arnold transformation and cryptosystem in a transform domain (DWT-DCT). The encryption is used here to protect multimedia data and Arnold transform offers an extra level of security. Experimental demonstration signifies that our technique is found robust against several attacks. The discussed technique determines to offer a possible way to report the security concern in the transmission of multimedia data.

CHAPTER-4
DCT AND GENETIC ALGORITHM
BASED WATERMARKING METHOD
FOR COLOR IMAGES

CHAPTER-4

DCT AND GENETIC ALGORITHM BASED WATERMARKING METHOD FOR COLOR IMAGES

A watermarking technique based on DCT and a Genetic algorithm is discussed in this chapter. The DCT transform divides the cover image into 8×8 blocks and then genetic algorithm is employed for obtaining the best pixel group for embedding the watermark to minimize data losses. In this approach, an optimal image watermarking method for multimedia objects resisting watermarking attacks is presented. Digital watermarking is applied here to guarantee and give data validation and copyright fortification to data broadcasting. An imperceptible and robust watermarking with the combination of DCT and GA is employed for color images. Firstly, a host image matrix is decayed into 8×8 blocks by the DCT. Then, the Genetic algorithm is used to obtain an optimized solution of digital watermarking. The foremost advantage of this presented method is to pick the finest group of pixels for embedding so that we can achieve an upgraded feature of the signed image. With the appropriate selection of the finest pixel group, data loss is less during embedding and gained better results. Further performance evaluation of our approach is calculated on color models (RGB, YCbCr, and YIQ). Different standard images are used to assess the watermarking performing parameters such as PSNR and NCC. The experimental evaluation of the presented technique shows superior results in comparison to other methods.

4.1. Introduction

As information technology is rising very vastly, the approach to the internet for everybody is not a big deal in the present scenario. With easy access and the rise in the internet technology, authentication and security of multimedia objects have become important issues for researchers. Multimedia objects such as images, audio, video, and text are easily reachable and communal nowadays. Hence, authentication and proprietorship of such digital data from replication and illegal use is a chief apprehension of the proprietors. Many algorithms have been discussed so far to cope up with such issues i.e., security, copyright protection, illegitimate repetition of multimedia data, but watermarking is utmost prevalent. It defines as a process of embedding watermark data in cover data like image, audio, and 3d models to build a secure data from illegitimate use [191]. Watermarking is a

better approach because information of digital documents remains safe even after the application of the decoding procedure [192]. Therefore, currently, the foremost attention of research in image watermarking is inadequate to three main concerns i.e., the quality of watermarked or attacked images, robustness, and embedding capacity. Now the problem is to diminish the adjustment between the earlier two. Because of this, image watermarking adopted an optimization problem to optimize watermarking parameters of robustness and good quality of signed images. For this purpose, many soft computing intelligence techniques such as genetic algorithms, artificial neural networks (ANNs), and fuzzy inference systems (FIS) [193] are developed [194]. In [195], authors described a watermarking process based on DCT and genetic algorithms. In this particular method, DCT is applied to the embedding process and a genetic algorithm is used in the recovery process. The experimental outcome shows that the technique is robust against many attacks, but limited to greyscale images. In [196], DNA covering for image encryption with the combination of chaotic function and genetic algorithm are discussed. The main aim of this hybrid grouping is to select the optimum DNA fore as a contribution to image encryption. Firstly, DNA covers are generated with the DNA sequence and logistic map. Then, the purpose of the genetic algorithm is to obtain the excellent DNA cover for encryption. This algorithm increases the entropy and reduces the connection among two one-on-one pixels. Results show that it has good strength against common attacks. Furthermore, an optimized watermarking system created with DWT and Hadamard transform is described in [197]. First, a 2-degree DWT on the original image is employed, after that hadamard transform is applied to generate hadamard coefficients, and a secret information is encoded into WHT constants. A GA optimization is applied purposely to determine the multiple SF, optimum for digital watermarking. In this method, recovery is completed with no debt of a host image and the original data is estimated by a decision tree. The performance outcome indicates that this technique is robust against attacks and attains a high NC value (i.e., extracted watermarks are recognizable). This chapter presents color image watermarking with hollands and benefits of the DCT. The functionality of DCT is explained in chapter-2 of this thesis and an introduction to the genetic algorithm is illustrated in the next section.

4.2. Watermarking with genetic algorithm

A genetic algorithm is an arbitrary search procedure designed upon the thought of inheritances [198]. This is the most powerful process to search, solve complex problems, and optimization problems [199], [200]. The following fig. 4.1 shows image watermarking

with GA [201] and it gives robust results. All individual is a static segment of variables then these individuals are associated in an organized way of chromosomes and creates a population [202], [203]. A fitness function is operated to evaluate the strings in the population, and find out the finest individual through the fitness values. To minimize and maximize the optimization values, fitness function is created [204]. The key occurrences of this algorithm are crossover, selection, and mutation [205] [144]. In process of selection, an innovative population is caused by picking the characters with the supreme appropriate standards. Crossover is defined by selecting two characters from the people and swapping them to build a novel pair of individuals [206]. The mutation is a process where random changes are made to generate children from the individual parents [207]. The rate of mutation must be less. GA is applied here to idolize the optimum use of constants applied in a watermarking method to achieve a balance between imperceptibility and robustness.

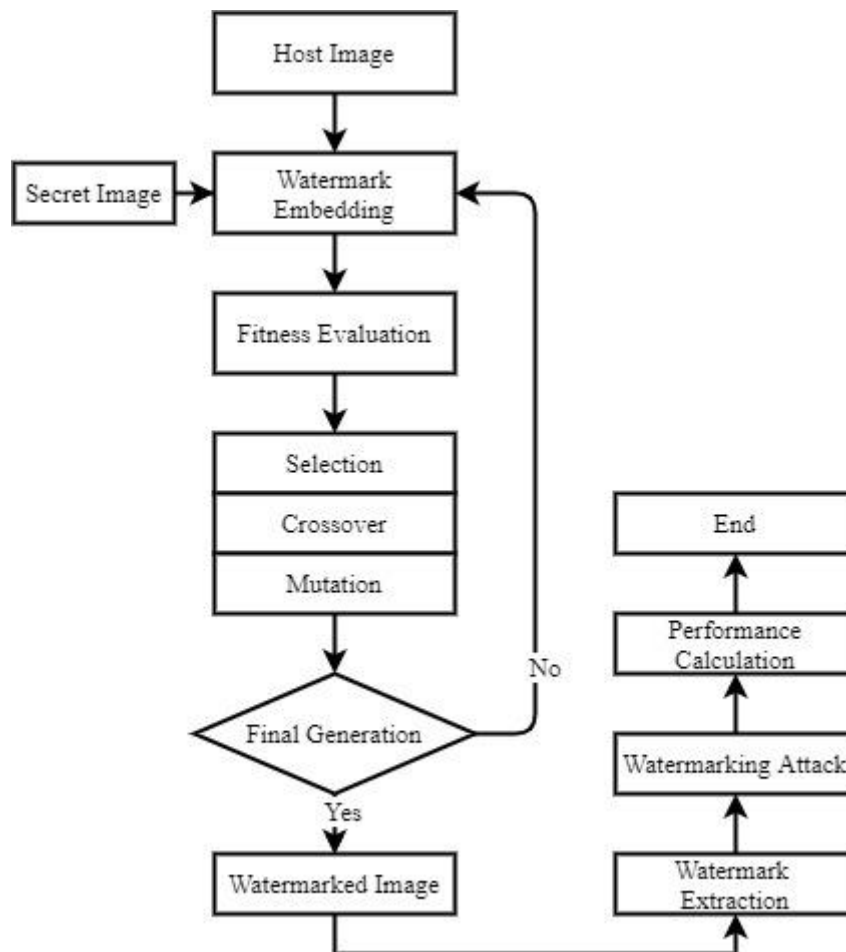


Fig. 4.1: Watermarking with genetic algorithm

An imperceptible and robust watermarking is discussed for color images. The main contributions of this chapter are explained below:

- Due to the properties of DCT in image processing, it is preferred to use it with a genetic algorithm for standard images. And, it is suitable to acquire the greatest pixel set for embedding. To expand the pertinency of GA, it is used to enhance the robustness and imperceptibility of multimedia objects.
- Further, this technique is evaluated through two distinct (YCbCr and YIQ) color spaces.
- Results indicate that this method achieved good imperceptibility and robustness in comparison with previous methods.

4.3. Designed method

This section explains the image watermarking with DCT and genetic algorithm for color images. The fig. 4.2 explains the presented watermarking scheme. Firstly, an original image is split into non-overlapping 8x8 blocks, and then the DCT coefficients of individual blocks are evaluated. After that, a genetic algorithm is applied to pick the finest block. If an appropriate block is achieved, then the secret mark is encoded with the similar block. The key is generated with the same block used for embedding and extraction. We employ the inverse of DCT to get the signed image. In the recovery process, the signed image is taken as an input, then the appropriate extraction algorithm is applied to reproduce the watermark image. The following sub-sections explain about the watermarking procedures in detail.

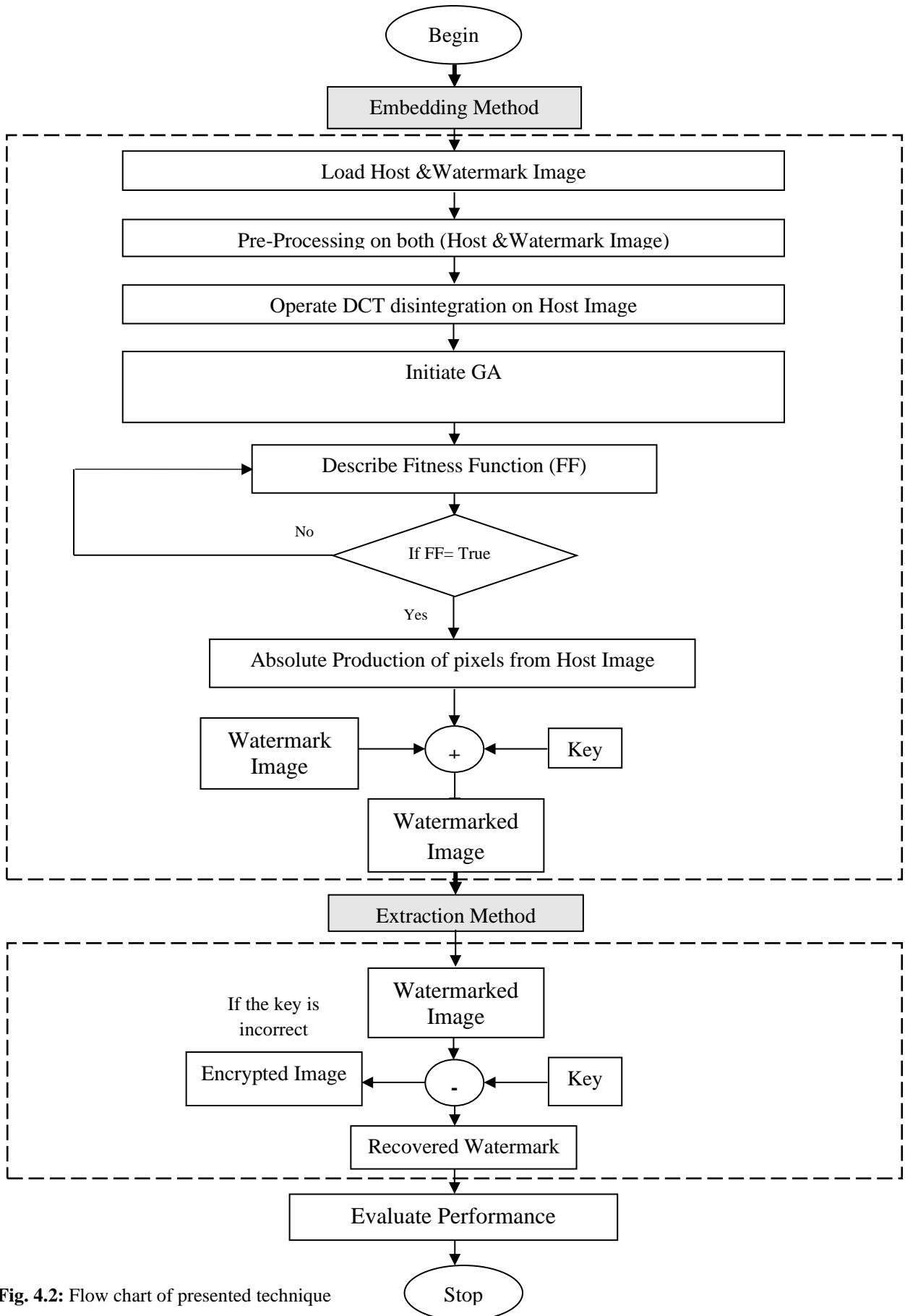


Fig. 4.2: Flow chart of presented technique

4.3.1. Steps for embedding

The step-by-step embedding procedure are explained as follows:

- i. Load 512×512 size of host image and 32×32 size of secret image (watermark) to start the image watermarking

$$H_{\text{IMG}} \leftarrow (H_{\text{IMG}}, [512 \times 512])$$

$$S_{\text{IMG}} \leftarrow (S_{\text{IMG}}, [32 \times 32])$$

- ii. Split the host media into 8by8 non-overlying sections and apply DCT to every section to generate DCT constants

$$BL \leftarrow 8 \times 8 \text{ block division on original image}$$

$$D \leftarrow \text{DCT decomposition on each block}$$

$$DC \leftarrow \text{DCT coefficients of each block}$$

- iii. Apply genetic algorithm to select the appropriate block for embedding

$$DC1 \leftarrow \text{ga (suitable block for embedding)}$$

- iv. Key generation with the same block for embedding and extraction

$$DC11 \leftarrow \text{key (K)}$$

- v. Embedding the watermark on the same block

$$\text{Watermarked Image (WI)} = \sum_{i=1}^C DC1 + (\alpha \times \text{Wimg}) \quad (1)$$

where DC1 has picked DCT constants with optimization, C is RGB components (red, green, and blue) of the host image and α is the gain value.

- vi. Operate inverse DCT to get a watermarked image

$$WI \leftarrow \text{inverse DCT}$$

- vii. Display watermarked image

4.3.2. Steps for extraction

The step-by-step watermarking extraction are described below:

- i. Read the watermarked image
- ii. Decompose an image into 8by8 non-overlying sections and compute DCT for every section and generate DCT constants

$$BL \leftarrow 8 \times 8 \text{ block division on the watermarked image (WI)}$$

D1 ← DCT decomposition on each block

DC2 ← DCT coefficients of each block

- iii. Load the same embedding key for extraction

DC11 ← key (K)

- iv. Recover a watermark from the watermarked image

$$\text{Watermark Image (Wimg1)} = \sum_{i=1}^C WI - \left(\frac{DC2}{\alpha}\right) \quad (2)$$

where DC2 is selected DCT coefficients with optimization, WI is watermarked image, C is RGB components (red, green, and blue) of the host image and α is a gain value.

- v. Apply inverse DCT on Wimg1

Wimg1 ← inverse DCT

- vi. Get extracted watermark

4.4. Experimental study

To define the outcome of the proposed work, genetic algorithm toolbox of the MATLAB software is used. The genetic algorithm toolbox used here was generated by the University of Sheffield. Various images of 512×512 size e.g., Lena, Barbara and a secret image of 32×32 size are taken for the experiment. The genetic algorithm parameters used in this experiment are described as: 60 is the population size, 0.8 is the crossover rate, and 0.05 is the mutation rate. To check the performance of the proposed watermarking, PSNR and NC parameters are measured. The proposed algorithm achieves good PSNR because images are free from watermarking attacks.

Table 4.1 Results of discussed method

Host Image	Extracted Watermark	PSNR	NC
		55.1727	0.9934
		57.1795	0.9997
		56.1547	0.9976
		57.2615	0.9998
		56.1558	0.9943
		56.1504	0.9967
		56.1579	0.9946
		57.1745	0.9988

Table 4.1 represents the outcome of the presented scheme for distinct host and watermark images. Fig. 4.3 displays the graphical illustration of the above table 4.1.

The 57.2615 is the greatest PSNR gained from image Lena and 0.9998 is the greatest NC value attained from the same image. The 56.1504 is the lowest and 57.2615 is the highest PSNR attained by this scheme, correspondingly. The smallest NC value of 0.9934 is attained by this method from Barbara.

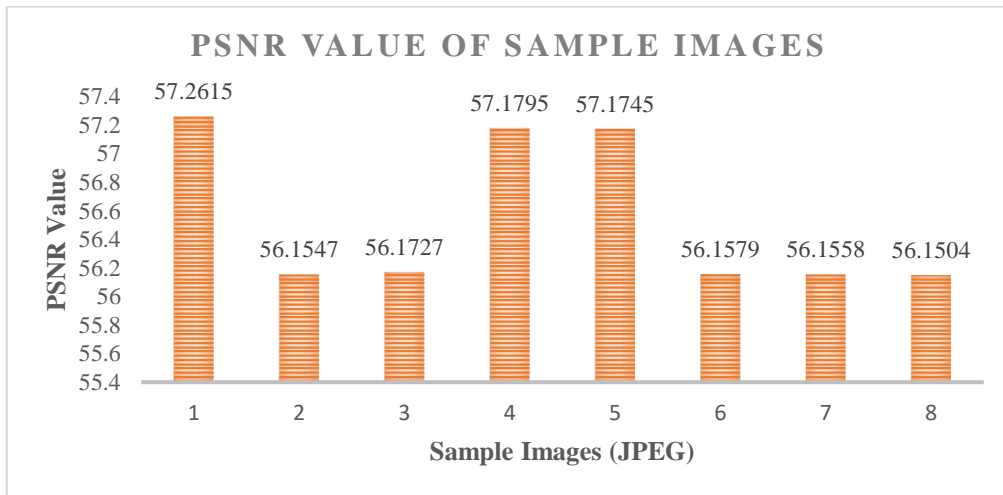


Fig. 4.3: Graphical representation of PSNR value of sample images

Fig. 4.4 describes the procedure of watermarking for the image Seashore. Fig. 4.4 (a) represents the Seashore image taken as the host image, then fig. 4.4 (b) shows a secret mark which is used for embedding. In fig. 4.4 (c), a signed image of a Seashore generated after embedding is shown and last image shown in fig. 4.4 (d) is a recovered watermark.

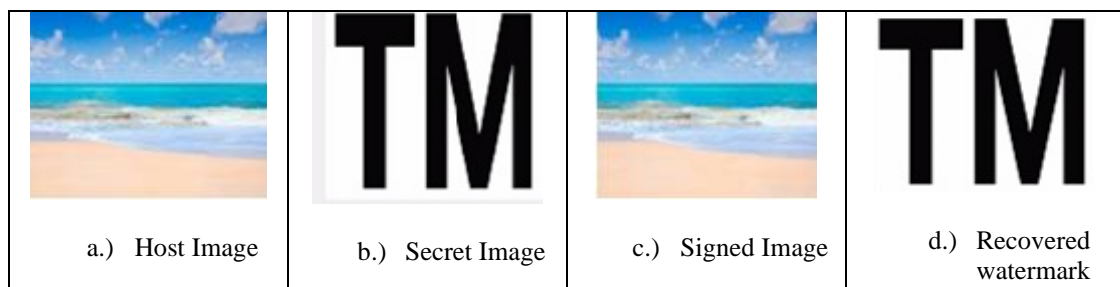


Fig. 4.4: Image Seashore used in watermarking procedure

Various watermarking attacks from Lena and Seashore images are shown in fig. 4.5 (a) and (b). In fig. 4.5 (a) and (b), first column represents the outcome of filtering attack on Lena and Seashore image, then the second column shows the noising attack (gaussian) of the Lena and Seashore image, then noising attack (salt & pepper) is pointed in the third column of fig. 4.5 (a) and (b) and in fourth column, JPEG compression of the Lena and Seashore image is presented.



Fig. 4.5: a.) Watermarking attacks from Lena image

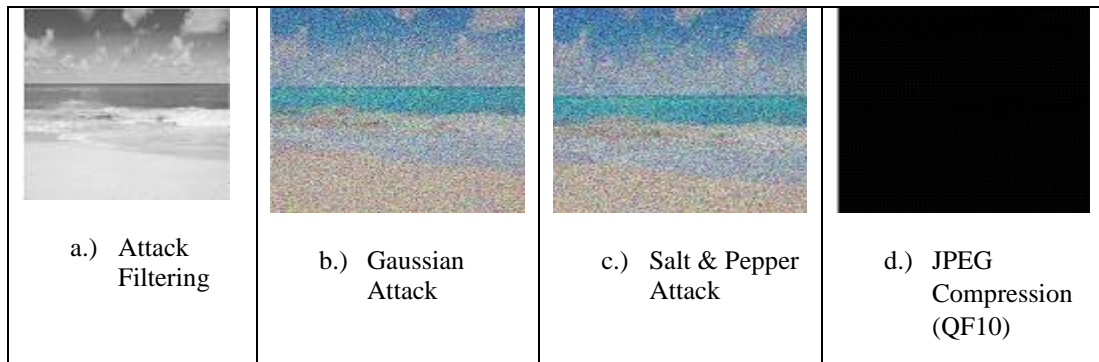


Fig. 4.5: b.) Watermarking attacks from Seashore image

Table 4.2 shows the comparison with Patel et. *al* method [1] for four different images Lena, Sailboat, Seashore, and Bridge at different RGB components. Watermark embedding is employed to the components of RGB (red, green, and blue) of different images.

Table 4.2 Comparative analysis of PSNR values with a previous approach for different planes of color images

Images	Patel et al. Approach [1]			Presented Approach		
	Red plane	Green plane	Blue plane	Red plane	Green plane	Blue plane
Sea_shore	47.51	47.55	47.54	53.838	53.835	53.822
Lena	50.8609	47.9892	49.77	57.012	57.013	57.168
Bridge	47.72	47.44	47.47	55.878	55.836	55.827
Sailboat	47.32	47.31	47.43	55.741	55.706	55.747

From image Lena, the highest PSNR at the blue component is 57.168 and the lowest PSNR is 57.012 at the red component. The maximum PSNR at blue component is 55.747 and minimum PSNR at the green component is 55.706 from the Sailboat. The

highest PSNR is 53.838 on a red component and the lowest PSNR value is 53.822 on a blue plane for the Seashore image. Though, 55.878 is the highest PSNR on a red component and at the blue plane, 55.827 is the lowest PSNR for bridge image.

Table 4.3 Outcome of imperceptibility and robustness at distinct attacks for RGB plane

Images	Attack/Noise Intensity	Color Component	PSNR	NC	Noise Intensity	PSNR	NC	Noise Intensity	PSNR	NC	Noise Intensity	PSNR	NC		
Lena	Filtering/ 1×1	Red	36.16	0.9515	Filtering / 2×2	34.97	0.9407	Filtering / 3×3	34.54	0.9358	*****				
		Green	35.63	0.9508		34.95	0.9403		34.52	0.9355					
		Blue	36.21	0.9516		34.97	0.9407		34.49	0.9347					
	Gaussian/ 0.001	Red	36.17	0.9521	Gaussian / 0.01	35.04	0.9419	Gaussian / 0.1	34.55	0.9361					
		Green	35.61	0.9522		35.03	0.9417		34.61	0.9367					
		Blue	36.19	0.9513		35.01	0.9415		34.62	0.9368					
	JPEG Compression (QF90)	Red	36.44	0.9531	JPEG Compression (QF70)	35.28	0.9449	JPEG Compression (QF50)	34.89	0.9404		JPEG Compression (QF10)	34.11	0.9314	
		Green	36.34	0.9527		35.26	0.9446		34.88	0.9401			34.15	0.9318	
		Blue	36.14	0.9526		35.28	0.9449		34.78	0.9388			34.12	0.9315	
	Salt and Pepper/ 0.001	Red	36.25	0.9525	Salt and Pepper/ 0.01	35.16	0.9435	Salt and Pepper/ 0.1	34.72	0.9383		*****			
		Green	36.25	0.9528		35.11	0.9429		34.69	0.938					
		Blue	36.26	0.9529		35.12	0.9431		34.7	0.9381					
Sea_shore	Filtering/ 1×1	Red	36.56	0.9512	Filtering / 2×2	34.91	0.9401	Filtering / 3×3	34.45	0.9343	*****				
		Green	36.56	0.9512		34.96	0.9404		34.42	0.9339					
		Blue	36.57	0.9514		34.93	0.9405		34.39	0.9333					
	Gaussian/ 0.001	Red	35.69	0.9487	Gaussian / 0.01	34.99	0.9411	Gaussian / 0.1	34.57	0.9363					
		Green	36.47	0.9492		35.01	0.9415		34.56	0.936					
		Blue	35.71	0.9491		34.99	0.9411		34.57	0.9363					
	JPEG Compression (QF90)	Red	36.44	0.9506	JPEG Compression (QF70)	35.19	0.9441	JPEG Compression (QF50)	34.81	0.9391			JPEG Compression (QF10)	34.05	0.9304
		Green	36.04	0.9502		35.21	0.9439		34.83	0.9395				34.09	0.9311
		Blue	36.24	0.9503		35.18	0.9438		34.87	0.9399				34.03	0.9302
	Salt and Pepper/ 0.001	Red	35.65	0.9488	Salt and Pepper/ 0.01	35.08	0.9425	Salt and Pepper/ 0.1	34.71	0.9382		*****			
		Green	36.47	0.9493		35.1	0.9428		34.65	0.9374					
		Blue	35.71	0.9489		35.09	0.9427		34.67	0.9378					
Sailboat	Filtering/ 1×1	Red	35.29	0.9451	Filtering / 2×2	34.94	0.9406	Filtering / 3×3	34.47	0.9348	*****				
		Green	36.39	0.9455		34.92	0.9402		34.44	0.9346					
		Blue	35.67	0.9453		34.94	0.9406		34.41	0.9338					
	Gaussian/ 0.001	Red	35.29	0.9461	Gaussian / 0.01	34.98	0.9409	Gaussian / 0.1	34.58	0.9364					
		Green	36.39	0.9469		35.01	0.9415		34.59	0.9365					
		Blue	35.68	0.9462		34.98	0.9409		34.58	0.9364					
	JPEG Compression (QF90)	Red	35.99	0.9485	JPEG Compression (QF70)	35.27	0.9445	JPEG Compression (QF50)	34.82	0.9393			JPEG Compression (QF10)	34.08	0.9309
		Green	35.78	0.9479		35.23	0.9444		34.85	0.9397				34.06	0.9307
		Blue	35.82	0.9481		35.25	0.9445		34.86	0.9398				34.13	0.9316
	Salt and Pepper/ 0.001	Red	36.47	0.9493	Salt and Pepper/ 0.01	35.05	0.9421	Salt and Pepper/ 0.1	34.66	0.9377		*****			
		Green	35.44	0.9472		35.02	0.9418		34.63	0.9371					
		Blue	36.03	0.9475		35.02	0.9418		34.68	0.9379					

Table 4.3 illustrates the outcome of PSNR and NC values of three dissimilar color images with RGB planes under different attacks with different noise densities. Salt & Pepper, and Gaussian attacks with noise intensity 0.1, 0.01, and 0.001 and filtering attack are also evaluated. And JPEG compression (QF 90, 70, 50,10) attack is also evaluated for the same. For image Seashore, the highest PSNR attained by the presented approach is 36.57 dB in the filtering attack. However, the highest NC value gained by the image Lena in noising attack (i.e., salt & pepper at 0.001 intensity) is found to be 0.9529. In Salt & Pepper with noise intensity 0.01, the highest PSNR and NC value are 35.16dB and 0.9435 respectively, for image Lena. Similarly, in Salt & Pepper with 0.1 noise intensity, the highest PSNR and NC attained by the presented method is 34.72 dB and 0.9383 respectively, for image Lena. In JPEG compression (QF 90), the highest PSNR is 36.44 dB for the image Lena and Seashore, and lowest PSNR attained by JPEG compression (QF 10) for the image Seashore is 34.03 dB.

Table 4.4 Comparative study of PSNR (dB) with the previous method

S. No.	Image	Presented Approach	Mehta et al. [208]
1	Baboon	52.1589	45.4328
2	Penguins	56.1579	46.0723
3	Flower	56.1558	45.5903
4	Lena	57.2615	46.16

Table 4.4 represents the comparative study of the Mehta *et al.* method [208] with the presented approach. The technique applied by Mehta *et al.* is LWT with a GA. The image pixels (host and watermark) are identical in both techniques. Our proposed method achieves better results as compared with the previous approach.

Now, we denote the complexity of discussed method i.e., based on time-taking phases of image watermarking. The time complexity is $O(M \log M)$, time taken by the 2D DCT and converse of DCT, where M entitles the host image size [209]. The steps of the genetic algorithm involve the phases of mutation, crossover, and estimation of fitness value. The complexity is denoted as $O(Sp \times Cl \times Ng)$, where population size is denoted by Sp , length of code is Cl and the generation number is represented by Ng . Finally, the overall time complexity of the discussed model is indicated in eq. (3) as,

$$O (M \log M + Sp \times Cl \times Ng) \quad (3)$$

In addition, the presented technique is compared with other two-color spaces (YIQ and YCbCr). The amount of data harm is lower by using the RGB color model in comparison to YIQ and YCbCr. The RGB model has a property of additive color model where RGB components are adjoined collectively in numerous manners to produce a wide-range of different colors. The RGB color model is designed for real-time images. In the YCbCr color model, red and blue components are offered as different signals. Subsequently, when numerical processes are operated on the color spaces (YCbCr and YIQ), the retrieval of data loss is not probable due to the entropy gap.

4.4.1. YCbCr color space

This color model is acquired from the cube of RGB color spaces. Each color in the RGB color model has different YCbCr values. In YCbCr color space Y denotes the luminance value whereas Cb and Cr denote the chromatic blue and red values, respectively [210]. The main purpose of this color model is the alteration in single color space of the host image while embedding of the secret information has the slightest impact on alterations in another color model as YCbCr color model are less correlated. The YCbCr color model is originated for color TV broadcasting.

The RGB values are changed to YCbCr color model and conversion formula is given below in eq. 4:

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.169 & -0.331 & 0.500 \\ 0.500 & -0.419 & -0.081 \end{bmatrix} \begin{bmatrix} X_{Red} \\ X_{Green} \\ X_{Blue} \end{bmatrix} \quad (4)$$

Furthermore, YCbCr color model can be transformed back into RGB values. and transformation is given in the following eq. 5:

$$\begin{bmatrix} X_{Red} \\ X_{Green} \\ X_{Blue} \end{bmatrix} = \begin{bmatrix} 1.0 & 0 & 1.5 \\ 1.0 & -0.344136 & -0.715 \\ 1.0 & 1.772 & 0 \end{bmatrix} \begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} \quad (5)$$

Table 4.5 Evaluation at YCbCr color space






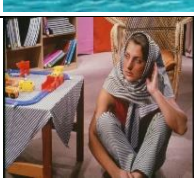


Host Image	Recovered Watermark	PSNR	NC
	TM	54.1795	0.9846
	C	56.1334	0.9834
	C	55.1524	0.9881
	TM	54.8615	0.9889
	TM	53.1547	0.9772
	TM	55.1637	0.9847
	TM	55.1579	0.9765
	C	54.1277	0.9852

Table 4.5 represents the execution of the designed approach at YCbCr color space from several standard original and secret images. The highest PSNR accomplished by the presented method is 56.1334 dB from a flower image. Though,

the highest NC is 0.9889, from a Lena image. Moreover, the lowest PSNR value of 53.1547 is attained by image sailboat and the lowest NC is 0.9765 for the sea-shore image.

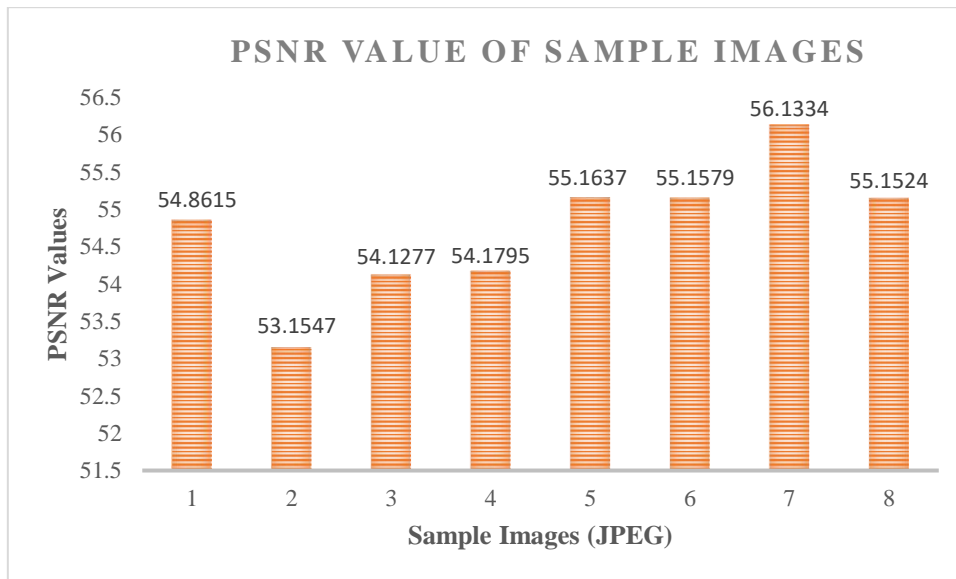


Fig. 4.6: Graphical representation of PSNR value at YCbCr color model

Table 4.6 Imperceptibility and robustness attained under various attacks at YCbCr color constituent from Lena image

Color Constituent	Attack/Noise Intensity	NCC	PSNR	Attack/Noise Intensity	NCC	PSNR	Attack/Noise Intensity	NCC	PSNR	Attack/Noise Intensity	NCC	PSNR
YY	JPEG Compression (QF50)	0.9212	33.25	JPEG Compression (QF70)	0.9261	33.67	JPEG Compression (QF90)	0.9301	34.01	JPEG Compression (QF10)	0.9113	32.15
	Salt and Pepper/ 0.1	0.9205	33.13	Salt and Pepper/ 0.01	0.9249	33.59	Salt and Pepper/ 0.001	0.9290	33.89	*****		
	Gaussian/ 0.1	0.9194	33.01	Gaussian/ 0.01	0.9234	33.49	Gaussian/ 0.001	0.9281	33.83			
	Filtering/ 3×3	0.9181	32.89	Filtering/ 2×2	0.9223	33.35	Filtering/ 1×1	0.9272	33.75			
YCb	JPEG Compression (QF50)	0.9211	33.22	JPEG Compression (QF70)	0.9258	33.65	JPEG Compression (QF90)	0.9296	33.95	JPEG Compression (QF10)	0.9107	32.11
	Salt and Pepper/ 0.1	0.9203	33.09	Salt and Pepper/ 0.01	0.9245	33.57	Salt and Pepper/ 0.001	0.9289	33.88	*****		
	Gaussian/ 0.1	0.9192	32.99	Gaussian/ 0.01	0.9231	33.45	Gaussian/ 0.001	0.9277	33.81			
	Filtering/ 3×3	0.9177	32.84	Filtering/ 2×2	0.9221	33.34	Filtering/ 1×1	0.9267	33.73			
YCr	JPEG Compression (QF50)	0.9209	33.19	JPEG Compression (QF70)	0.9256	33.64	JPEG Compression (QF90)	0.9299	33.97	JPEG Compression (QF10)	0.9109	32.11
	Salt and Pepper/ 0.1	0.9201	33.07	Salt and Pepper/ 0.01	0.9242	33.55	Salt and Pepper/ 0.001	0.9284	33.85	*****		
	Gaussian/ 0.1	0.9188	32.96	Gaussian/ 0.01	0.9229	33.42	Gaussian/ 0.001	0.9279	33.82			
	Filtering/ 3×3	0.9179	32.85	Filtering/ 2×2	0.9219	33.33	Filtering/ 1×1	0.9269	33.74			
CbCb	JPEG Compression (QF50)	0.9206	33.15	JPEG Compression (QF70)	0.9252	33.61	JPEG Compression (QF90)	0.9291	33.89	JPEG Compression (QF10)	0.9104	32.09
	Salt and Pepper/ 0.1	0.9199	33.06	Salt and Pepper/ 0.01	0.9239	33.54	Salt and Pepper/ 0.001	0.9286	33.87	*****		
	Gaussian/ 0.1	0.9186	32.93	Gaussian/ 0.01	0.9228	33.39	Gaussian/ 0.001	0.9274	33.78			
	Filtering/ 3×3	0.9174	32.82	Filtering/ 2×2	0.9217	33.31	Filtering/ 1×1	0.9266	33.71			
Cr Cr	JPEG Compression (QF50)	0.9208	33.17	JPEG Compression (QF70)	0.9253	33.63	JPEG Compression (QF90)	0.9294	33.91	JPEG Compression (QF10)	0.9101	32.05
	Salt and Pepper/ 0.1	0.9196	33.04	Salt and Pepper/ 0.01	0.9236	33.52	Salt and Pepper/ 0.001	0.9283	33.84	*****		
	Gaussian/ 0.1	0.9183	32.91	Gaussian/ 0.01	0.9225	33.37	Gaussian/ 0.001	0.9275	33.79			
	Filtering/ 3×3	0.9171	32.79	Filtering/ 2×2	0.9214	33.29	Filtering/ 1×1	0.9263	33.69			

Table 4.6 represents the outcome of the presented scheme with several watermarking attacks. The YCbCr color model is evaluated with different combinations of color components on the Lena image. The 512×512 size of the original image and 32×32 size of the watermark image are taken for evaluation. Refereeing to the table, the Y color part from the YCbCr model is preferred for embedding the watermarks. At the YY component, the uppermost PSNR value of 34.01 dB is attained by the JPEG compression (QF 90), and lowest PSNR value of 32.05 is achieved by the JPEG compression (QF 10) at the CrCr component. The maximum NC 0.9301 is acquired by JPEG compression (QF 90) at the YY component, and the minimum NC value of 0.9101 is obtained by the JPEG compression (QF 10) at the CrCr component.

4.4.2. YIQ color space

In YIQ, the luma information is contained by the Y part i.e., the only component utilized by black and white TV. A combination of RGB strengths is selected for the Y component. The I and Q component represent the chromatic information.



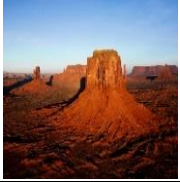
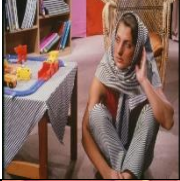


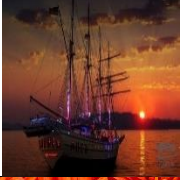



The RGB values are converted to the YIQ color model and the conversion formula for the same is described in below eq.6

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.5959 & -0.2746 & -0.3213 \\ 0.2115 & -0.5227 & -0.3112 \end{bmatrix} \begin{bmatrix} I_{Red} \\ I_{Green} \\ I_{Blue} \end{bmatrix} \quad (6)$$

Likewise, YIQ is converted back into the RGB model and the conversion formula for the same is using the following eq. 7

$$\begin{bmatrix} I_{Red} \\ I_{Green} \\ I_{Blue} \end{bmatrix} = \begin{bmatrix} 1.0 & 0.956 & 0.619 \\ 1.0 & -0.272 & 0.647 \\ 1.0 & -1.106 & -1.703 \end{bmatrix} \begin{bmatrix} Y \\ I \\ Q \end{bmatrix} \quad (7)$$

Table 4.7 Outcome of YIQ color space

Host Image	Recovered Watermark	PSNR	NC
	TM	52.8615	0.9447
	TM	53.1279	0.9772
	TM	52.1525	0.9546
		52.3235	0.9629
	TM	52.1457	0.9746
		52.1427	0.9536
	TM	53.1558	0.9754
	TM	53.1637	0.9627

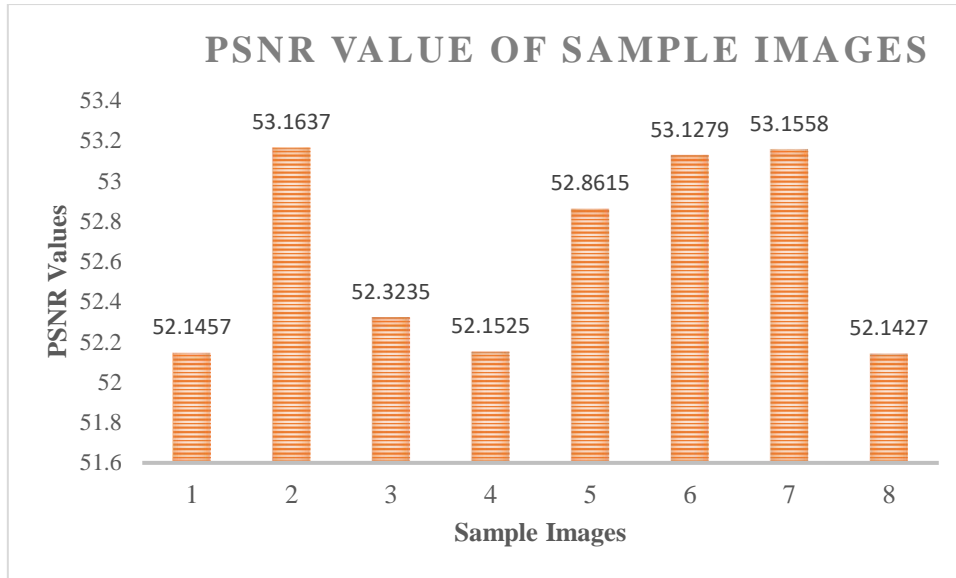


Fig. 4.7: Graphical representation of PSNR value at YIQ color model

Table 4.7 demonstrates the outcome of the YIQ color model for the proposed method. For the watermarking procedures, color images (original and watermark) have been taken into consideration. Fig. 4.7 represents the graphically illustration of PSNR values attained from different images at the YIQ component. The maximum PSNR is 53.1637dB for the image Sailboat and the maximum NC value is 0.9772 from image Seashore. Then, the lowest 52.1427 dB value of PSNR is attained from the boat and the lowermost NC value of 0.9447 is attained from the Barbara image.

Table 4.8 describes the PSNR and NC values for numerous watermarking attacks from image Lena at distinct color sections of the YIQ space. Demonstrating this table, component Y is found appropriate for embedding the secret media. The finest performance in terms of PSNR and NC values are 32.03 dB and 0.9099 respectively, accomplished by the JPEG compression (QF 90) at the YY component. The lowest PSNR value is 30.22 dB and NC value is 0.8884, attained by JPEG compression (QF 10) at the QQ component.

Table 4.8 Imperceptibility and robustness attained under various attacks of YIQ color constituents from Lena image

Color Constituent	Attack/Noise Intensity	NC	PSNR	Attack/Noise Intensity	NC	PSNR	Attack/Noise Intensity	NC	PSNR	Noise Intensity	NC	PSNR
YY	JPEG Compression (QF50)	0.9014	31.15	JPEG Compression (QF70)	0.9056	31.59	JPEG Compression (QF90)	0.9099	32.03	JPEG Compression (QF10)	0.8895	30.32
	Salt and Pepper/ 0.1	0.9002	31.03	Salt and Pepper/ 0.01	0.9048	31.48	Salt and Pepper/ 0.001	0.9091	31.93			
	Gaussian/ 0.1	0.8988	30.78	Gaussian/ 0.01	0.9031	31.33	Gaussian/ 0.001	0.9079	31.84			
	Filtering/ 3×3	0.8976	30.69	Filtering/ 2×2	0.9027	31.27	Filtering/ 1×1	0.9068	31.69			
YI	JPEG Compression (QF50)	0.9009	31.12	JPEG Compression (QF70)	0.9055	31.56	JPEG Compression (QF90)	0.9094	32.00	JPEG Compression (QF10)	0.8891	30.29
	Salt and Pepper/ 0.1	0.8999	31.01	Salt and Pepper/ 0.01	0.9046	31.47	Salt and Pepper/ 0.001	0.9086	31.89			
	Gaussian/ 0.1	0.8986	30.75	Gaussian/ 0.01	0.9035	31.37	Gaussian/ 0.001	0.9075	31.81			
	Filtering/ 3×3	0.8974	30.66	Filtering/ 2×2	0.9024	31.25	Filtering/ 1×1	0.9063	31.66			
YQ	JPEG Compression (QF50)	0.9012	31.14	JPEG Compression (QF70)	0.9053	31.55	JPEG Compression (QF90)	0.9096	32.01	JPEG Compression (QF10)	0.8889	30.25
	Salt and Pepper/ 0.1	0.8996	30.98	Salt and Pepper/ 0.01	0.9044	31.45	Salt and Pepper/ 0.001	0.9088	31.91			
	Gaussian/ 0.1	0.8991	30.82	Gaussian/ 0.01	0.9033	31.34	Gaussian/ 0.001	0.9076	31.83			
	Filtering/ 3×3	0.8972	30.65	Filtering/ 2×2	0.9021	31.22	Filtering/ 1×1	0.9066	31.68			
II	JPEG Compression (QF50)	0.9008	31.09	JPEG Compression (QF70)	0.9051	31.52	JPEG Compression (QF90)	0.9093	31.99	JPEG Compression (QF10)	0.8887	30.24
	Salt and Pepper/ 0.1	0.8993	30.95	Salt and Pepper/ 0.01	0.9041	31.42	Salt and Pepper/ 0.001	0.9081	31.86			
	Gaussian/ 0.1	0.8983	30.73	Gaussian/ 0.01	0.9028	31.29	Gaussian/ 0.001	0.9072	31.79			
	Filtering/ 3×3	0.8969	30.61	Filtering/ 2×2	0.9019	31.19	Filtering/ 1×1	0.9062	31.64			
QQ	JPEG Compression (QF50)	0.9005	31.06	JPEG Compression (QF70)	0.9049	31.51	JPEG Compression (QF90)	0.9092	31.96	JPEG Compression (QF10)	0.8884	30.22
	Salt and Pepper/ 0.1	0.8994	30.97	Salt and Pepper/ 0.01	0.9038	31.39	Salt and Pepper/ 0.001	0.9084	31.88			
	Gaussian/ 0.1	0.8979	30.71	Gaussian/ 0.01	0.9029	31.31	Gaussian/ 0.001	0.9069	31.77			
	Filtering/ 3×3	0.8966	30.59	Filtering/ 2×2	0.9017	31.16	Filtering/ 1×1	0.9059	31.61			

In this chapter, an imperceptible and robust watermarking model is discussed based on DCT and GA. The discussed model is evaluated at distinct color images for embedding the secret media (watermark image) in the cover image then recovering the secret mark from the signed image via recovery process with the similar key. The presented model is evaluated for three color models (RGB, YCbCr, and YIQ) with similar conditions and the outcome shows that embedding at RGB components produce more robust results. The outcome also shows that the presented method attains better PSNR and NC values as compared to previous schemes and robust against various watermarking attacks too.

CHAPTER-5

An Effective Multiple Watermarking Using Transform Domain Methods with Wavelet Fusion for Digital Media

Chapter-5

AN EFFECTIVE MULTIPLE WATERMARKING USING TRANSFORM DOMAIN METHODS WITH WAVELET FUSION FOR DIGITAL MEDIA

In this chapter, two different watermarking schemes are discussed, one is based on transform-domain methods with wavelet fusion, and the other is based on multiple transforms domain-based watermarking for color images. In the first approach, two different watermarks (images) undergo the wavelet fusion method to make a single distinct fused watermark image. The wavelet fusion method offers high embedding capacity for several watermarking applications such as healthcare and remote sensing. Then Arnold transformation is operated on the fused image (watermark) to get a scrambled fused watermark image before embedding. Firstly, in the embedding procedure, an original image matrix is disintegrated by transform domain (DWT and DCT) algorithms then a scrambled fused watermark is implanted to the original image. Due to Arnold transformation, an extra level of security is achieved and robustness against different watermarking attacks. In the second approach, multiple transform domain techniques (DCT, SVD, and DWT) are operated on both the original image as well as on the secret mark to further improve the robustness and imperceptibility in the presence of various signal processing attacks. A secret message is embedded into the same multimedia object (image) to provide an extra level of security while achieving good performance. This technique is also evaluated for distinct watermarking attacks. Both approaches attain good results in terms of performance metrics.

5.1. Introduction

The internet grows to be a striking opulence of data to many billion handlers in the time of the twenty-first century. With the speedy evolution of multimedia data, expertise has flickered the mode, for broadcasting and data distribution over the world. The digital distraction of multimedia objects like copyright protection, replication, and illegal distribution, has cultivated the growth of these prohibited actions. In such cases, the security of consumers and content is of thoughtful significance [211]. Some illustrious process is expected to protect the digital media from an unofficial person.

So, researchers are using digital watermarking methods for the security of multimedia objects from illegal assailants [9], [19], [212]. Digital watermarking is a method of implanting secret image into the same media (image) without destroying the visual quality of multimedia data. After the extraction method, the same secret media is extracted from the original media. It is established that wavelet fusion-based watermarking can have high embedding capacity and robustness [121], [213]. A hybrid image watermarking model is designed using transform domain techniques (DWT-SVD) with the wavelet fusion method. In this method, two different watermarks are combined to make a single fused image before embedding, then the fused image is implanted into the original image using a hybrid domain (DWT-SVD) to generate a watermarked image. The fusion method shows that more images can be embedded in a watermarking system. Experimental outcome indicates that the method attains a good outcome for capacity and robustness. In [214] author discussed a watermarking system based on RDWT-DCT-SVD. In this particular approach, cover media (image) is disintegrated by RDWT-DCT and SVD techniques, then secret information is placed inside the host image. This method attains good robustness for different kinds of attacks. A method grounded on block SVD and RDWT is proposed by Gaur et al. [215]. For more security, two distinct watermarks are implanted in a host image. In this particular technique, the second watermark is scrambled by Arnold transform prior to embedding. This method gained high capacity but has small deprivation in the visible feature of the image. In transform-domain methods, information is inserted by altering the constants of DCT, DFT, DWT, and SCD transforms. These watermarking methods are complex in computation and achieve great robustness.

Image fusion is a technique that combines many images to generate a single image known as fused image as shown in below fig. 5.1. It offers an improved quality fused image for gathering the image content [216].

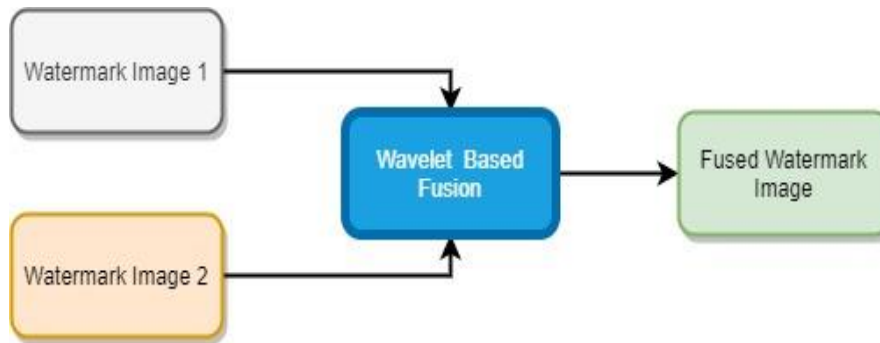


Fig. 5.1: Image fusion using wavelet fusion method

With the properties of transform domain watermarking and wavelet fusion methods, two different approaches have been discussed in this chapter. The main contribution of the proposed techniques has summarized below:

- The use of transform domain techniques with the wavelet fusion method provides a high degree of embedding capacity and robustness to multimedia objects.
- To further enhance the security of information Arnold transformation is employed.
- Quality of watermark and watermarked data is improved with the hybrid inclusions of many techniques and performance is enhanced in terms of security, robustness, and imperceptibility.

5.2. Proposed Method

5.2.1. With Wavelet Fusion Technique

In this work, two different transform domain techniques (DWT-DCT) with wavelet fusion and Arnold scrambling technique are presented. Two distinct watermark images are used to create a single fused watermark image. Then the fused image is scrambled with the Arnold method before embedding. The cover image is disintegrated by transform domain then scrambled watermark image is encoded with the host image and formulates a watermarked image. In the extraction procedure, the fused watermark image is recovered and

then anti fusion method is applied to extract two distinct watermark images. Fig. 5.2 and 5.3 describe the process of watermarking.

Input:

- a.) Host image
- b.) Two secret images

Output:

- a.) Watermarked image

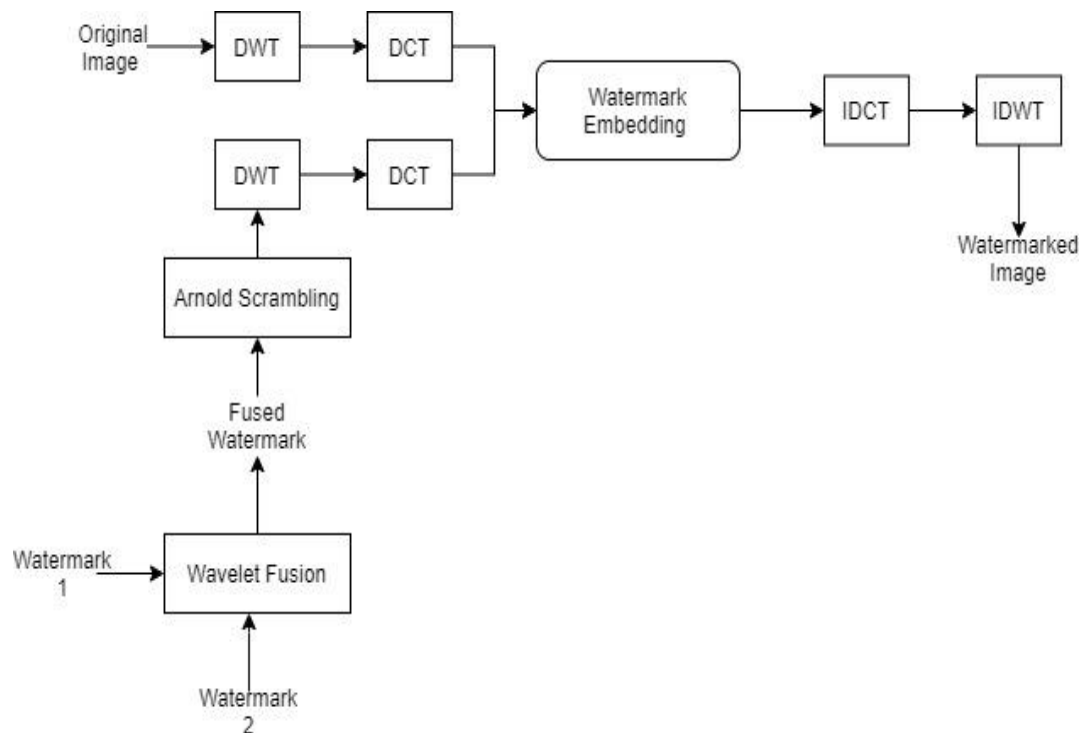


Fig. 5.2: Proposed embedding procedure

Steps:

The process of embedding the watermark into original media is demonstrated as follows:

- a.) An original image matrix is decayed by applying DWT up to 3-level using Haar wavelet to generate a DWT sub-band.
- b.) The DCT is imposed to choose a sub-band of DWT (X matrix of the original image).
- c.) A fused image is formed from both watermarks (watermark 1 and watermark 2) by using the wavelet fusion technique (Y_T matrix of the watermark image).

- d.) After that, Arnold scrambling is employed on the fused image to generate a scrambled watermark image.
- e.) Then, the third-degree DWT is operated on the fused scrambled watermark image. After that DCT is applied on coefficients of DWT on the scrambled matrix (Y_T^* matrix).
- f.) Embedding of the watermark image is performed using the following equation.

$$Z_{WT} = X + \alpha Y_T^*$$

where α is the scaling factor, Y_T^* is the watermark image and Z_{WT} is the watermarked image.

- g.) To get a watermarked image, the converse of DCT and DWT is performed.

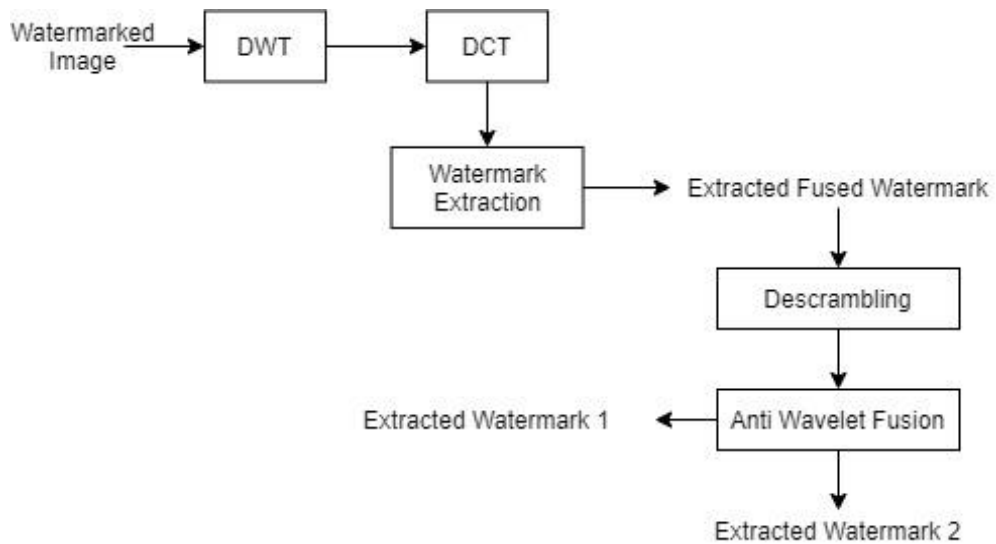


Fig. 5.3: Proposed extraction procedure

Input:

- a.) Watermarked image

Output:

- a.) Recovery of two distinct watermark images

Steps:

The extraction procedure for robustly extracting the secret data from the watermarked image is described below:

- a.) Apply same-level DWT on the watermarked image (Z_{WT} matrix).
- b.) Transform the DCT on the watermarked image ($X1$ matrix).
- c.) Watermark image extraction to get the fused watermark image.

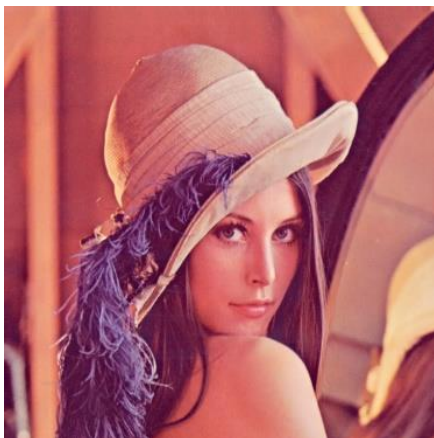
$$Y_{T1}^* = Z_{WT} - \left(\frac{X1}{\alpha}\right)$$

where, Y_{T1}^* represents extracted watermark, Z_{WT} denotes watermarked image, $X1$ is the original image and α is the scaling factor.

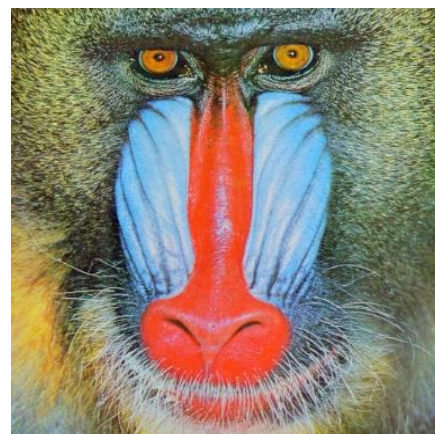
- d.) Apply descrambling method to the fused watermark matrix.
- e.) Apply Anti-fusion method to fused watermark images with the help of a wavelet fusion algorithm to get the watermark 1 and watermark 2 images.

5.2.2. Experimental analysis

For the experiment, 512×512 is the size of the cover image, and 64×64 is the size of both watermark images 1 and 2, correspondingly. Four different images i.e., Lena, Mandrill, Barbara, and Pepper of the same size are used for experiments. Fig. 5.4 represents the different original and watermark images and fig. 5.5 shows the fused watermark image. Robustness and imperceptibility image quality performance parameters are taken into consideration. A thorough explanation of these parameters is explained in chapter 1 of this thesis.



a.) Lena as an original image



b.) Mandrill as an original image



c.) Image 1 (watermark)



d.) Image 2 (watermark)

Fig. 5.4: Original and watermark images



Fig. 5.5: Fused watermark image

Table 5.1 PSNR values tested for different watermarked images

S. No.	Cover Image	Watermark Image	Gain Factor				
			0.1	0.3	0.5	0.7	0.9
1	Lena	Watermark Image 1 & 2	52.1569	47.5145	41.1771	38.2548	36.0711
2	Barbara	Watermark Image 1 & 2	52.1569	47.5145	41.1771	38.2548	36.0711
3	Pepper	Watermark Image 1 & 2	52.1569	47.5145	41.1771	38.2548	36.0711
4	Mandrill	Watermark Image 1 & 2	52.1569	47.5145	41.1771	38.2548	36.0711

Table 5.1 demonstrates the outcome for four different images at various gain factors. PSNR values for signed images Lena, Barbara, Pepper, and Mandrill are obtained. Transparency is higher for smaller gain factor values. Fig. 5.6 represents the graphical representation of PSNR values for these standard images at varying gain values.

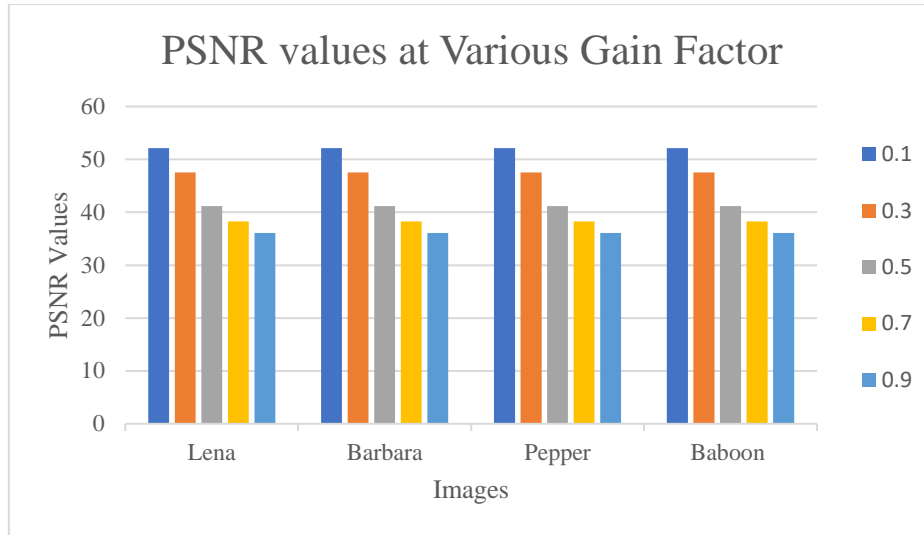


Fig. 5.6: Graphical representation of different watermarked images

Table 5.2 NC values for different recovered watermarks

S. No.	Attack	Watermark Image	Gain Factor				
			0.1	0.3	0.5	0.7	0.9
1	Salt & Pepper	Watermark Image 1	0.7643	0.8669	0.8993	0.9657	0.9817
		Watermark Image 2	0.7807	0.8743	0.9113	0.9777	0.9884
2	Gaussian	Watermark Image 1	0.9659	0.9959	0.9989	0.9996	0.9998
		Watermark Image 2	0.9742	0.9984	0.9993	0.9997	0.9999
3	Rotation	Watermark Image 1	0.9955	0.9875	0.9852	0.9845	0.9858
		Watermark Image 2	0.9975	0.9926	0.9907	0.9905	0.9901
4	Blurring	Watermark Image 1	0.8798	0.9565	0.9681	0.9726	0.9752
		Watermark Image 2	0.9317	0.9725	0.9805	0.9832	0.9855

Table 5.2 and Table 5.3 depict the values obtained from recovered watermarks after attacks for images Lena and Baboon. It is seen from these values that intense robustness is attained for larger gain factors. Image Lena and Baboon are tested under different watermarking attacks like Salt & Pepper, Gaussian, Rotation, and Blurring. Additionally, the recovered watermarks are identifiable after the same attacks, i.e., watermark images are more robust against many pertained attacks.

Table 5.3 NC values for different recovered watermarks

S. No.	Attack	Watermark Image	Gain Factor				
			0.1	0.3	0.5	0.7	0.9
1	Salt & Pepper	Watermark Image 1	0.7713	0.7764	0.9066	0.9619	0.9818
		Watermark image 2	0.7881	0.8352	0.9391	0.9759	0.9872
2	Gaussian	Watermark Image 1	0.8258	0.9845	0.9975	0.9986	0.9996

		Watermark image 2	0.8805	0.9905	0.9985	0.9995	0.9998
3	Rotation	Watermark Image 1	0.9778	0.9805	0.9811	0.9817	0.9819
		Watermark image 2	0.9865	0.9879	0.9882	0.9886	0.9889
4	Blurring	Watermark Image 1	0.8299	0.9448	0.9619	0.9784	0.9799
		Watermark image 2	0.8874	0.9654	0.9765	0.9808	0.9835

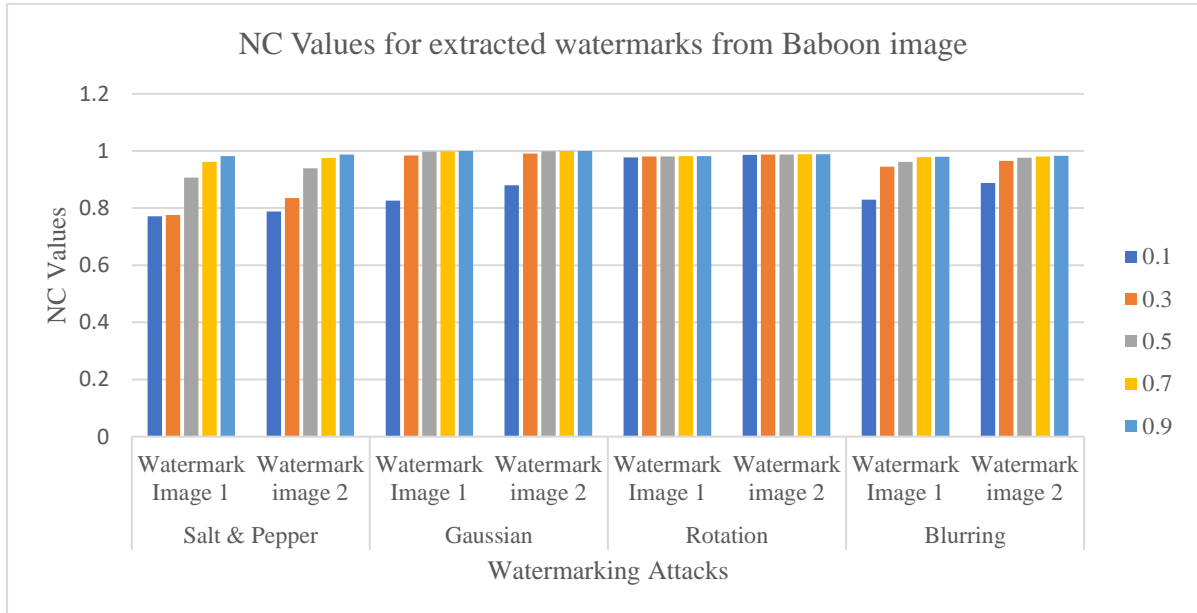


Fig. 5.7: Graphical representation of NC values from Baboon image

5.2.3. Multiple watermarking with transform domain

A multiple watermarking is presented combining three transform domain methods DCT, DWT, and SVD. For more security, secret data is implanted into a similar multimedia content to provide an extra security. In the embedding procedure, original media is disintegrated into first-level DWT and a lowest frequency sub-band is selected for DCT decomposition and then SVD transformation is performed. Then secret image is decomposed by DCT, then the coefficient of DCT is altered by SVD. Further, the inverse of the transform domain is employed to get a signed (watermarked) image. In contrast, the recovery procedure is functional in reverse order to extract the watermark image. Fig. 5.8 demonstrates the process of watermarking (both embedding and extraction).

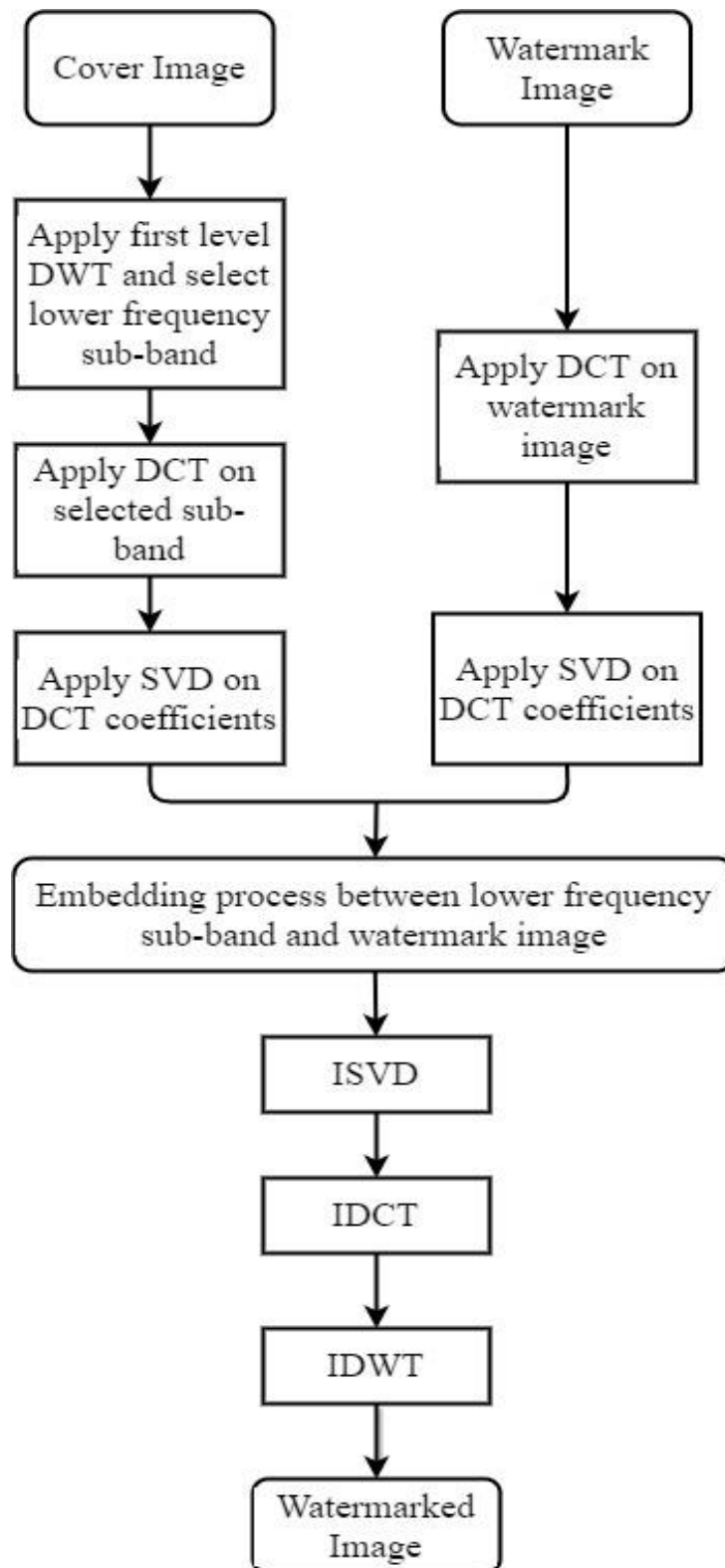


Fig. 5.8: a.) Proposed embedding procedure

The above-endorsed procedure is the grouping of multiple transform domain i.e., DWT, DCT and SVD techniques. This method helps to enhance the robustness without substantial

deprivation of the image feature against image processing attacks. The designed approach is the combination of two embedding and recovery algorithms.

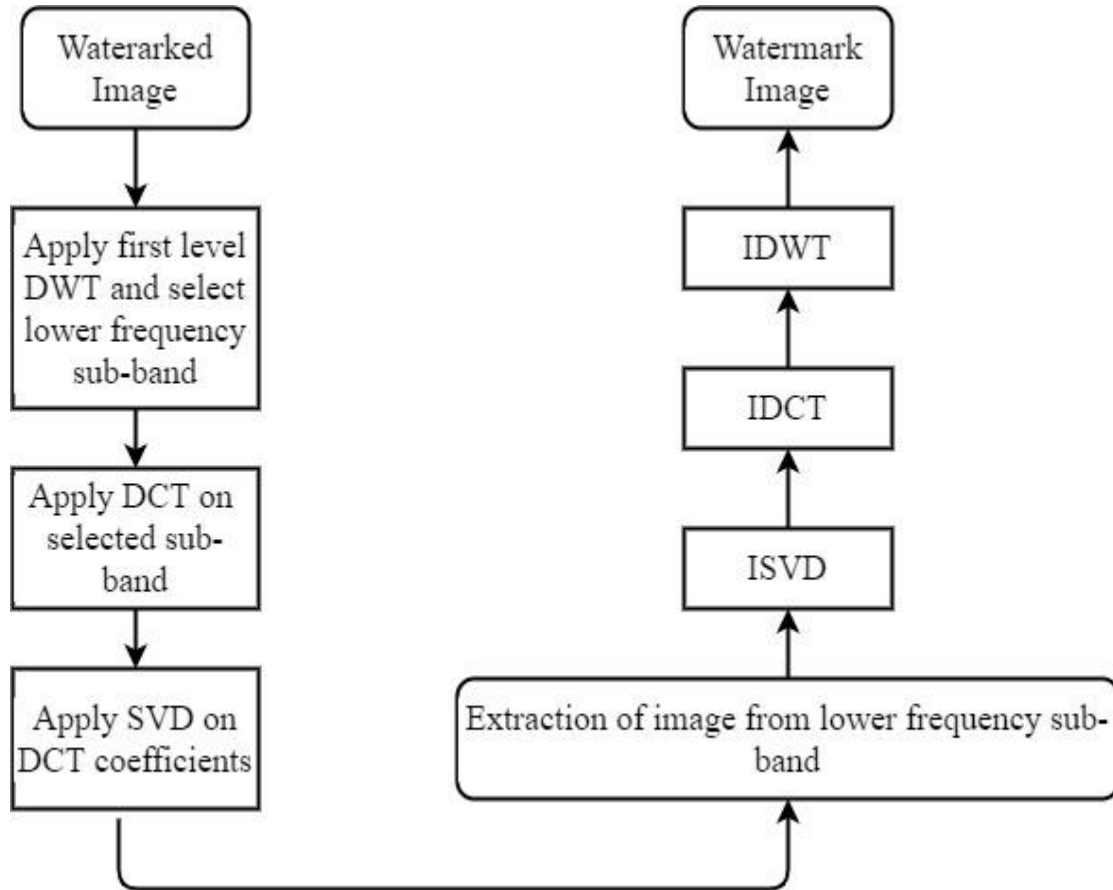


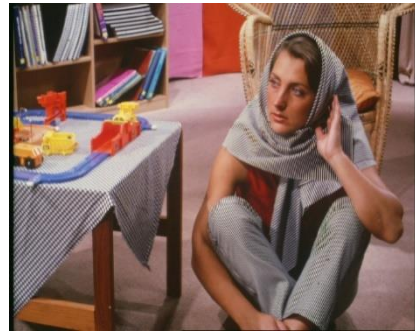
Fig. 5.8: b.) Proposed extraction procedure

5.2.4. Experimental analysis

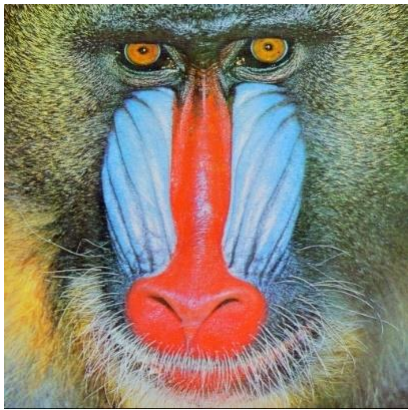
For our experiment, four different images Lena, Barbara, Peppers, and Baboon are taken as both cover as well as a watermark image. The size of these images are 512×512 for both original and watermark image for evaluating the proposed model. Original and watermark images considered for this experiment are presented in Fig. 5.9. In this experiment, PSNR and NC values are computed at distinct gain factors.



a.) Lena



b.) Barbara



c.) Mandrill



d.) Peppers

Fig. 5.9: a.), b.), c.), d.) Original and watermark images

Table 5.4 Performance evaluation of proposed technique at altered gain value

Image	Gain Value	PSNR	NC
Barbara	0.01	37.69	0.9936
Barbara	0.05	37.58	0.9958
Barbara	0.1	36.12	0.9998

In table 5.4, outcome of the presented system is described at distinct gain factors (0.01, 0.05, and 0.1) from image Barbara. Barbara image is taken as both the original as well as a watermark image. The presented method achieves the highest PSNR at the lowest gain value, and NC value is the highest at the highest gain value. The proposed

algorithm accomplishes the largest PSNR value of 37.69db at a gain value of 0.01 and the largest NC is 0.9998 at a gain value of 0.1 without any attack.

Table 5.5 Performance evaluation for different images at the same gain value

Cover Image	Watermark Image	Gain Factor	PSNR	NC
Lena	Lena	0.05	37.65	0.9948
Peppers	Peppers	0.05	36.27	0.9938
Mandrill	Peppers	0.05	35.98	0.9889
Barbara	Lena	0.05	37.55	0.9942

Table 5.5 represents the outcome of the presented technique for four dissimilar original images with different watermark images at the same gain value (0.05). The highest PSNR value of 37.65 is attained from image Lena and the lowest PSNR value of 35.98 is attained with image Mandrill. The highest NC value accomplished is 0.9948 for image Lena and the lowermost NC is 0.9889 for Mandrill image.

Table 5.6 Performance tested against attacks for image Barbara

S. No.	Attacks	Noise Density	NC
1	JPEG-Compression	QF=90	0.9995
2	JPEG-Compression	QF= 50	0.9728
3	JPEG-Compression	QF= 10	0.9613
4	Gaussian Noise	0.01	0.7883
5	Salt & Pepper	0.001	0.9978
6	Salt & Pepper	0.05	0.6998
7	Salt & Pepper	0.01	0.7989
8	Filtering	1x1	0.9992
9	Scaling	1.1	0.7651

Table 5.6 represents the outcome of robustness achieved by the discussed algorithm for various attacks at distinct noise densities. The method is tested with JPEG compression (at QF 10, 50, 90), noising attack (Salt & Pepper and Gaussian), filtering,

and scaling attacks. The maximum NC value of 0.9995 is attained at JPEG compression (QF 90), and the minimum NC value of 0.6998 is gained by Salt & Pepper (0.05). It can be observed that the proposed approach can robustly extract the watermark image even after imposing watermarking attacks.

In summary, a wavelet fusion-based image watermarking with transform-domain is presented in the first approach. This method attains the desired watermarking results, as it increases the embedding capacity without destroying the quality of the original data. In the second approach, multiple transform-domain watermarking is implemented for multimedia data. The designed method achieves better outcomes in terms of robustness and imperceptibility.

CHAPTER-6

CONCLUSION AND FUTURE SCOPE

Chapter-6

CONCLUSION AND FUTURE SCOPE

This chapter describes a conclusion depicted based on the research proposed in this thesis. This thesis begins with a vast literature survey of the different watermarking system for both grey and color images. During the literature survey, different transform-domain-based techniques are investigated to achieve good robustness and analyzed the simulation results. We studied and analyzed the different techniques such as artificial intelligence, machine learning, encryption, PSO, and neural networks and their inclusion to the transform-domain-based algorithms. We further categorized them according to the size of distinct host and watermark images.

To fulfill the security requirement of the multimedia data, homomorphic encryption with the Arnold transformation is used to create a robust and secure watermarking system. Different watermarking performance parameters such as PSNR, NCC, NPCR, and UACI are analyzed. Results show that the encryption-based transform domain method is more robust and secure against many attacks.

Furthermore, DCT and Genetic algorithm are applied to guarantee data validation and copyright fortification during data transmission. The DCT technique is implemented here to split the cover media into 8by8 sections and a GA is applied on top of the DCT technique to obtain the optimal results. This approach is verified under distinct color models e.g., YCbCr and YIQ, and watermarking attacks. PSNR and NCC performance parameters are evaluated and found to be better than the previous approaches.

Towards achieving the security and robustness further, a fusion-based watermarking method for color images is applied to improve data security for e-health applications. The wavelet fusion technique combines two different secret images to make a fused watermark and then Arnold transformation is employed on the fused watermark image to enhance its robustness and security under different attacks. Furthermore, a multi-level watermarking scheme is proposed built on DWT, DCT, and SVD. The proposed technique is evaluated under several attacks and compared with previous methods. The outcome shows that the presented technique offers better robustness, security and imperceptibility.

The work shown in this thesis has several involvements in the area of digital watermarking and its applications. A large number of watermarking applications are present in real-world scenarios. However, in this thesis, different watermarking algorithms are investigated focusing on authentication, healthcare and digital transmission applications due to their wide range of usage in real-world. However, it has various opportunities for future directions, e.g., it can be applied to develop electronic voting systems and healthcare systems. More watermarking performance parameters such as fault tolerance, tamper resistance could be considered in future work. New technology such as deep learning, blockchain can be applied to design a more efficient digital watermarking system. Furthermore, the presented methods can also be applied for different multimedia objects like audio and video.

LIST OF PUBLICATIONS

LIST OF PUBLICATIONS

JOURNALS PUBLISHED

1. N Agarwal, AK Singh and PK Singh, "Survey of Robust and Imperceptible Watermarking," *Multimedia Tools and Applications*, vol. 77, issue 7, pp. 8603-8633, 2019 [SCI Indexed, IF=2.313].
2. N Agarwal and PK Singh, "Robust and Secure Watermarking for Propagation of Digital Multimedia by Paillier Homomorphic Cryptosystem with Arnold Transformation," *International Journal of E-Health and Medical Communications (IJEHMC)*, IGI Global, vol. 12, issue 4, pp. 17-31, 2021 [Scopus].
3. N Agarwal and PK Singh, "Discrete Cosine Transform and Genetic Algorithm based watermarking method for robustness and imperceptibility of color images for intelligent multimedia applications", *Multimedia Tools and Applications*, 2021 [SCI Indexed, IF=2.313].

JOURNAL COMMUNICATED

1. N Agarwal, A Kumar and PK Singh, "An effective robust watermarking method based on DWT, DCT and wavelet fusion for color images and their application in healthcare applications" communicated in IETE Journal of Research.

CONFERENCES

1. N Agarwal and PK Singh, "Image processing for forestry using data mining techniques," published in 3rd Himachal science congress conference held at IIT Mandi, Oct 2018.
2. N Agarwal, A Kumar and PK Singh, "Comparative analysis of transform domain watermarking system based on performance measures", *Innovations in Information and Communication Technologies (IICT) Conference*, Springer, 2020.
3. N Agarwal, A Kumar and PK Singh, "Robust and imperceptible multiple watermarking using transform domain algorithm for digital media", *Emerging Technologies for Computing, Communication and Smart Cities (ETCCS)*, Springer, 2021.

REFERENCES

REFERENCES

- [1] S. B. Patel, T. B. Mehta, and S. N. Pradhan, "A unified technique for robust digital watermarking of colour images using data mining and DCT," *Int. J. Internet Technol. Secur. Trans.*, vol. 3, no. 1, p. 81, 2011, doi: 10.1504/IJITST.2011.039680.
- [2] X. Gao, C. Deng, X. Li, and D. Tao, "Geometric Distortion Insensitive Image Watermarking in Affine Covariant Regions," *IEEE Trans. Syst. Man Cybern. Part C Appl. Rev.*, vol. 40, no. 3, pp. 278–286, May 2010, doi: 10.1109/TSMCC.2009.2037512.
- [3] D. S. Chauhan, A. K. Singh, B. Kumar, and J. P. Saini, "Quantization based multiple medical information watermarking for secure e-health," *Multimed. Tools Appl.*, vol. 78, no. 4, pp. 3911–3923, 2019.
- [4] N. Aherrahrou and H. Tairi, "A new robust watermarking scheme based on PDE decomposition," in *2013 ACS International Conference on Computer Systems and Applications (AICCSA)*, May 2013, pp. 1–5. doi: 10.1109/AICCSA.2013.6616454.
- [5] N. Agarwal, A. K. Singh, and P. K. Singh, "Survey of robust and imperceptible watermarking," *Multimed. Tools Appl.*, vol. 78, no. 7, pp. 8603–8633, Apr. 2019, doi: 10.1007/s11042-018-7128-5.
- [6] B. M. Irany, X. C. Guo, and D. Hatzinakos, "A high capacity reversible multiple watermarking scheme for medical images," in *2011 17th International Conference on Digital Signal Processing (DSP)*, Jul. 2011, pp. 1–6. doi: 10.1109/ICDSP.2011.6004968.
- [7] A. K. Singh, "Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image," *Multimed. Tools Appl.*, vol. 78, no. 21, pp. 30523–30533, 2019.
- [8] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "Multiple image watermarking applied to health information management," *IEEE Trans. Inf. Technol. Biomed.*, vol. 10, no. 4, pp. 722–732, 2006.
- [9] 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, 2017.
- [10] A. K. Singh, B. Kumar, G. Singh, and A. Mohan, *Medical image watermarking: techniques and applications*. Springer, 2017.
- [11] V. H. Vallabha, "Multiresolution watermark based on wavelet transform for digital images," *Cranes Softw. Int. Ltd.*, 2003.
- [12] S. Sood *et al.*, "What is telemedicine? A collection of 104 peer-reviewed perspectives and theoretical underpinnings," *Telemed. E-Health*, vol. 13, no. 5, pp. 573–590, 2007.
- [13] C. Chakraborty, A. Banerjee, M. H. Kolekar, L. Garg, and B. Chakraborty, *Internet of Things for Healthcare Technologies*. Springer, 2021.
- [14] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A Privacy-Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 11, pp. 2594–2608, Nov. 2016, doi: 10.1109/TIFS.2016.2590944.
- [15] J. Kumar, A. K. Singh, A. Mohan, and R. Buyya, *Machine Learning for Cloud Management*. Boca Raton: Chapman and Hall/CRC, 2021. doi: 10.1201/9781003110101.
- [16] A. Vacavant, "A novel definition of robustness for image processing algorithms," in *International Workshop on Reproducible Research in Pattern Recognition*, 2016, pp. 75–87.

- [17] A. S. Kulkarni and S. S. Lokhande, "Imperceptible and Robust Digital Image Watermarking Techniques in Frequency Domain," vol. 3, p. 4, 2013.
- [18] S. P. Mohanty, *Nanoelectronic mixed-signal system design*. McGraw-Hill Education, 2015.
- [19] A. K. Singh, M. Dave, and A. Mohan, "Wavelet Based Image Watermarking: Futuristic Concepts in Information Security," *Proc. Natl. Acad. Sci. India Sect. Phys. Sci.*, vol. 84, no. 3, pp. 345–359, Sep. 2014, doi: 10.1007/s40010-014-0140-x.
- [20] S. Kumar and A. Dutta, "Performance analysis of spatial domain digital watermarking techniques," in *2016 International conference on information communication and embedded systems (ICICES)*, 2016, pp. 1–4.
- [21] F. Y. Shih, *Digital watermarking and steganography: fundamentals and techniques*. CRC press, 2017.
- [22] N. Agarwal and P. K. Singh, "Robust and Secure Watermarking for Propagation of Digital Multimedia by Paillier Homomorphic Cryptosystem With Arnold Transformation:," *Int. J. E-Health Med. Commun.*, vol. 12, no. 4, pp. 17–31, Jul. 2021, doi: 10.4018/IJEHMC.20210701.0a2.
- [23] H.-H. Tsai, Y.-J. Jhuang, and Y.-S. Lai, "An SVD-based image watermarking in wavelet domain using SVR and PSO," *Appl. Soft Comput.*, vol. 12, no. 8, pp. 2442–2453, Aug. 2012, doi: 10.1016/j.asoc.2012.02.021.
- [24] B. Mathon, F. Cayre, P. Bas, and B. Macq, "Optimal Transport for Secure Spread-Spectrum Watermarking of Still Images," *IEEE Trans. Image Process.*, vol. 23, no. 4, pp. 1694–1705, Apr. 2014, doi: 10.1109/TIP.2014.2305873.
- [25] 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.
- [26] P. Niu, L. Wang, J. Tian, S. Zhang, and X. Wang, "A Statistical Color Image Watermarking Scheme Using Local QPCET and Cauchy–Rayleigh Distribution," *Circuits Syst. Signal Process.*, pp. 1–30, 2021.
- [27] S. B. B. Ahmadi, G. Zhang, M. Rabbani, L. Boukela, and H. Jelodar, "An intelligent and blind dual color image watermarking for authentication and copyright protection," *Appl. Intell.*, vol. 51, no. 3, pp. 1701–1732, 2021.
- [28] Y. Wu, J. P. Noonan, and S. Aghaian, "NPCR and UACI randomness tests for image encryption," *Cyber J. Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun. JSAT*, vol. 1, no. 2, pp. 31–38, 2011.
- [29] M. Khan and F. Masood, "A novel chaotic image encryption technique based on multiple discrete dynamical maps," *Multimed. Tools Appl.*, vol. 78, no. 18, pp. 26203–26222, 2019.
- [30] D. S. Sherekar, D. V. M. Thakare, and D. S. Jain, "Attacks and Countermeasures on Digital Watermarks: Classification, Implications, Benchmarks," vol. 4, no. 2, p. 9, 2011.
- [31] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, "Attacks on digital watermarks: classification, estimation based attacks, and benchmarks," *IEEE Commun. Mag.*, vol. 39, no. 8, pp. 118–126, 2001.
- [32] S. P. Mohanty, "Digital watermarking: A tutorial review," URL [Httpwww Csee Usf Edu~ SmohantyresearchReportsWMSurvey1999Mohanty Pdf](http://www.csee.usf.edu/~SmohantyresearchReportsWMSurvey1999MohantyPdf), 1999.
- [33] P. Bas, J.-M. Chassery, and B. Macq, "Geometrically invariant watermarking using feature points," *IEEE Trans. Image Process.*, vol. 11, no. 9, pp. 1014–1028, 2002.
- [34] C.-W. Tang and H.-M. Hang, "A feature-based robust digital image watermarking scheme," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 950–959, 2003.

- [35] J. S. Seo and C. D. Yoo, "Localized image watermarking based on feature points of scale-space representation," *Pattern Recognit.*, vol. 37, no. 7, pp. 1365–1375, 2004.
- [36] J.-S. Tsai, W.-B. Huang, Y.-H. Kuo, and M.-F. Horng, "Joint robustness and security enhancement for feature-based image watermarking using invariant feature regions," *Signal Process.*, vol. 92, no. 6, pp. 1431–1445, Jun. 2012, doi: 10.1016/j.sigpro.2011.11.033.
- [37] X. Wang, J. Wu, and P. Niu, "A new digital image watermarking algorithm resilient to desynchronization attacks," *IEEE Trans. Inf. Forensics Secur.*, vol. 2, no. 4, pp. 655–663, 2007.
- [38] C. Deng, X. Gao, X. Li, and D. Tao, "Local histogram based geometric invariant image watermarking," *Signal Process.*, vol. 90, no. 12, pp. 3256–3264, 2010.
- [39] J.-J. Shen and P.-W. Hsu, "A Fragile Associative Watermarking on 2D Barcode for Data Authentication," p. 9, 2008.
- [40] V. Sachnev, Hyoung Joong Kim, Jeho Nam, S. Suresh, and Yun Qing Shi, "Reversible Watermarking Algorithm Using Sorting and Prediction," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009, doi: 10.1109/TCSVT.2009.2020257.
- [41] L. Kamstra and H. J. Heijmans, "Reversible data embedding into images using wavelet techniques and sorting," *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2082–2090, 2005.
- [42] D. M. Thodi and J. J. Rodríguez, "Reversible watermarking by prediction-error expansion," in *6th IEEE Southwest Symposium on Image Analysis and Interpretation, 2004.*, 2004, pp. 21–25.
- [43] D. M. Thodi and J. J. Rodríguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, 2007.
- [44] S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," *IEEE Trans. Inf. Forensics Secur.*, vol. 2, no. 3, pp. 321–330, 2007.
- [45] Soo-Chang Pei and Jing-Ming Guo, "Hybrid pixel-based data hiding and block-based watermarking for error-diffused halftone images," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 867–884, Aug. 2003, doi: 10.1109/TCSVT.2003.815943.
- [46] H. Z. Hel-Or, "Watermarking and copyright labeling of printed images," *J. Electron. Imaging*, vol. 10, no. 3, pp. 794–803, 2001.
- [47] C.-Y. Lin, "A reversible data transform algorithm using integer transform for privacy-preserving data mining," *J. Syst. Softw.*, vol. 117, pp. 104–112, Jul. 2016, doi: 10.1016/j.jss.2016.02.005.
- [48] T.-S. Chen, W.-B. Lee, J. Chen, Y.-H. Kao, and P.-W. Hou, "Reversible privacy preserving data mining: a combination of difference expansion and privacy preserving," *J. Supercomput.*, vol. 66, no. 2, pp. 907–917, 2013.
- [49] B. C. Fung, K. Wang, and S. Y. Philip, "Anonymizing classification data for privacy preservation," *IEEE Trans. Knowl. Data Eng.*, vol. 19, no. 5, pp. 711–725, 2007.
- [50] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, "The WEKA data mining software: an update," *ACM SIGKDD Explor. Newsl.*, vol. 11, no. 1, pp. 10–18, 2009.
- [51] D. Kirovski and H. S. Malvar, "Spread-spectrum watermarking of audio signals," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 1020–1033, Apr. 2003, doi: 10.1109/TSP.2003.809384.

- [52] W. Hong, T.-S. Chen, and C.-W. Shiu, "Reversible data hiding for high quality images using modification of prediction errors," *J. Syst. Softw.*, vol. 82, no. 11, pp. 1833–1842, Nov. 2009, doi: 10.1016/j.jss.2009.05.051.
- [53] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, 2006.
- [54] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, 2003.
- [55] G. Xuan, Y. Q. Shi, P. Chai, X. Cui, Z. Ni, and X. Tong, "Optimum histogram pair based image lossless data embedding," in *International Workshop on Digital Watermarking*, 2007, pp. 264–278.
- [56] J.-J. Shen and J.-M. Ren, "A robust associative watermarking technique based on vector quantization," *Digit. Signal Process.*, vol. 20, no. 5, pp. 1408–1423, Sep. 2010, doi: 10.1016/j.dsp.2009.10.015.
- [57] H.-C. Wu and C.-C. Chang, "A novel digital image watermarking scheme based on the vector quantization technique," *Comput. Secur.*, vol. 24, no. 6, pp. 460–471, 2005.
- [58] D. Singh and S. K. Singh, "DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection," *Multimed. Tools Appl.*, vol. 76, no. 11, pp. 13001–13024, 2017.
- [59] G. Bhatnagar, Q. J. Wu, and B. Raman, "A new robust adjustable logo watermarking scheme," *Comput. Secur.*, vol. 31, no. 1, pp. 40–58, 2012.
- [60] E. Ganic and A. M. Eskicioglu, "Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition," *J. Electron. Imaging*, vol. 14, no. 4, p. 043004, 2005.
- [61] A. K. Gupta and M. S. Raval, "A robust and secure watermarking scheme based on singular values replacement," *Sadhana*, vol. 37, no. 4, pp. 425–440, 2012.
- [62] C.-C. Lai and C.-C. Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 11, pp. 3060–3063, Nov. 2010, doi: 10.1109/TIM.2010.2066770.
- [63] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. Multimed.*, vol. 4, no. 1, pp. 121–128, 2002.
- [64] A. Noore, N. Tungala, and M. M. Houck, "Embedding biometric identifiers in 2D barcodes for improved security," *Comput. Secur.*, vol. 23, no. 8, pp. 679–686, Dec. 2004, doi: 10.1016/j.cose.2004.09.007.
- [65] Z. Wang and A. C. Bovik, "A universal image quality index," *IEEE Signal Process. Lett.*, vol. 9, no. 3, pp. 81–84, 2002.
- [66] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, 2004.
- [67] D. Van der Weken, M. Nachtgael, and E. E. Kerre, "A new similarity measure for image processing," *J. Comput. Methods Sci. Eng.*, vol. 3, no. 2, pp. 209–222, 2003.
- [68] J. Dittmann, L. C. Ferri, and C. Vielhauer, "Hologram watermarks for document authentications," in *Proceedings International Conference on Information Technology: Coding and Computing*, Las Vegas, NV, USA, 2001, pp. 60–64. doi: 10.1109/ITCC.2001.918766.
- [69] C.-C. Chang, T.-S. Chen, and L.-Z. Chung, "A steganographic method based upon JPEG and quantization table modification," *Inf. Sci.*, vol. 141, no. 1–2, pp. 123–138, Mar. 2002, doi: 10.1016/S0020-0255(01)00194-3.

- [70] M. Kamran and M. Farooq, "A Formal Usability Constraints Model for Watermarking of Outsourced Datasets," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 6, pp. 1061–1072, Jun. 2013, doi: 10.1109/TIFS.2013.2259234.
- [71] M. Kamran and M. Farooq, "An information-preserving watermarking scheme for right protection of EMR systems," *IEEE Trans. Knowl. Data Eng.*, vol. 24, no. 11, pp. 1950–1962, 2011.
- [72] T. V. Nguyen and J. C. Patra, "A simple ICA-based digital image watermarking scheme," *Digit. Signal Process.*, vol. 18, no. 5, pp. 762–776, Sep. 2008, doi: 10.1016/j.dsp.2007.10.004.
- [73] P. Meerwald, "Digital image watermarking in the wavelet transform domain," *Masters Thesis Dep. Sci. Comput. Univ. Salzburg.*, 2001.
- [74] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, 1997.
- [75] E. Koch and J. Zhao, "Towards robust and hidden image copyright labeling," in *IEEE Workshop on Nonlinear Signal and Image Processing*, 1995, vol. 1, pp. 123–132.
- [76] G. C. Langelaar, J. C. van der Lubbe, and R. L. Lagendijk, "Robust labeling methods for copy protection of images," in *Storage and retrieval for Image and Video databases V*, 1997, vol. 3022, pp. 298–309.
- [77] M. Kutter, F. D. Jordan, and F. Bossen, "Digital signature of color images using amplitude modulation [3022-51]," in *PROCEEDINGS-SPIE THE INTERNATIONAL SOCIETY FOR OPTICAL ENGINEERING*, 1997, pp. 518–526.
- [78] D. Kundur and D. Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition," in *Proceedings of the 1998 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP'98 (Cat. No. 98CH36181)*, 1998, vol. 5, pp. 2969–2972.
- [79] H.-J. M. Wang, P.-C. Su, and C.-C. J. Kuo, "Wavelet-based digital image watermarking," *Opt. Express*, vol. 3, no. 12, pp. 491–496, 1998.
- [80] F.-M. Yang, "One-dimensional neighborhood forming strategy for fragile watermarking," *J. Electron. Imaging*, vol. 12, no. 2, p. 284, Apr. 2003, doi: 10.1117/1.1557156.
- [81] A. Zear, A. K. Singh, and P. Kumar, "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine," *Multimed. Tools Appl.*, vol. 77, no. 4, pp. 4863–4882, Feb. 2018, doi: 10.1007/s11042-016-3862-8.
- [82] 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.
- [83] E. Ganic and A. M. Eskicioglu, "Robust DWT-SVD domain image watermarking: embedding data in all frequencies," in *Proceedings of the 2004 Workshop on Multimedia and Security*, 2004, pp. 166–174.
- [84] J. F. Delaigle, C. De Vleeschouwer, and B. Macq, "Watermarking algorithm based on a human visual model," *Signal Process.*, vol. 66, no. 3, pp. 319–335, May 1998, doi: 10.1016/S0165-1684(98)00013-9.
- [85] G. Coatrieux, C. Le Guillou, J.-M. Cauvin, and C. Roux, "Reversible Watermarking for Knowledge Digest Embedding and Reliability Control in Medical Images," *IEEE Trans. Inf. Technol. Biomed.*, vol. 13, no. 2, pp. 158–165, Mar. 2009, doi: 10.1109/TITB.2008.2007199.
- [86] Y. Zhi-qiang, H. H.-S. Ip, and L. F. Kowk, "Robust watermarking of 3D polygonal models based on vertex scrambling," in *Proceedings Computer Graphics International 2003*, 2003, pp. 254–257.

- [87] M. U. Celik, A. N. Lemma, S. Katzenbeisser, and M. van der Veen, "Secure Embedding of Spread Spectrum Watermarks using Look-up-Tables," in *2007 IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP '07*, Honolulu, HI, USA, 2007, p. II-153-II-156. doi: 10.1109/ICASSP.2007.366195.
- [88] Suk-Hawn Lee, Tae-Su Kim, Byung-Ju Kim, Seong-Geun Kwon, Ki-Ryong Kwon, and Kuhn-II Lee, "3D polygonal meshes watermarking using normal vector distributions," in *2003 International Conference on Multimedia and Expo. ICME '03. Proceedings (Cat. No.03TH8698)*, Baltimore, MD, USA, 2003, p. III-105. doi: 10.1109/ICME.2003.1221259.
- [89] A. K. Singh, M. Dave, and A. Mohan, "Multilevel Encrypted Text Watermarking on Medical Images Using Spread-Spectrum in DWT Domain," *Wirel. Pers. Commun.*, vol. 83, no. 3, pp. 2133-2150, Aug. 2015, doi: 10.1007/s11277-015-2505-0.
- [90] X. Rolland-Neviere, G. Doerr, and P. Alliez, "Spread transform and roughness-based shaping to improve 3D watermarking based on quadratic programming," in *2014 IEEE International Conference on Image Processing (ICIP)*, Paris, France, Oct. 2014, pp. 4777-4781. doi: 10.1109/ICIP.2014.7025968.
- [91] Y. AL-Nabhani, H. A. Jalab, A. Wahid, and R. M. Noor, "Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 27, no. 4, pp. 393-401, Oct. 2015, doi: 10.1016/j.jksuci.2015.02.002.
- [92] A. Najih, S. A. R. Al-Haddad, A. R. Ramli, S. J. Hashim, and M. A. Nematollahi, "Digital image watermarking based on angle quantization in discrete contourlet transform," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 29, no. 3, pp. 288-294, Jul. 2017, doi: 10.1016/j.jksuci.2016.02.005.
- [93] L. P. Feng, L. B. Zheng, and P. Cao, "A DWT-DCT based blind watermarking algorithm for copyright protection," in *2010 3rd International Conference on Computer Science and Information Technology*, 2010, vol. 7, pp. 455-458.
- [94] C. Kumar, A. K. Singh, and P. Kumar, "Improved wavelet-based image watermarking through SPIHT," *Multimed. Tools Appl.*, vol. 79, no. 15-16, pp. 11069-11082, Apr. 2020, doi: 10.1007/s11042-018-6177-0.
- [95] J. L. D. Shivani and R. K. Senapati, "Robust Image Embedded Watermarking Using DCT and Listless SPIHT," *Future Internet*, vol. 9, no. 3, Art. no. 3, Sep. 2017, doi: 10.3390/fi9030033.
- [96] A. Said and W. A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 6, no. 3, pp. 243-250, Jun. 1996, doi: 10.1109/76.499834.
- [97] R. K. Senapati, U. C. Pati, and K. K. Mahapatra, "Reduced memory, low complexity embedded image compression algorithm using hierarchical listless discrete Tchebichef transform," *IET Image Process.*, vol. 8, no. 4, pp. 213-238, 2014.
- [98] A. K. Singh, M. Dave, and A. Mohan, "Hybrid Technique for Robust and Imperceptible Image Watermarking in DWT-DCT-SVD Domain," *Natl. Acad. Sci. Lett.*, vol. 37, no. 4, pp. 351-358, Aug. 2014, doi: 10.1007/s40009-014-0241-8.
- [99] M. I. Khan, M. M. Rahman, and M. I. H. Sarker, "Digital Watermarking for Image Authentication Based on Combined DCT, DWT and SVD Transformation," *ArXiv13076328 Cs*, Jul. 2013, Accessed: Nov. 14, 2021. [Online]. Available: <http://arxiv.org/abs/1307.6328>
- [100] H. N J, *Hybrid Robust Watermarking Technique Based on DWT, DCT and SVD*. 2013.

- [101] R. Mehta, N. Rajpal, and V. P. Vishwakarma, "LWT- QR decomposition based robust and efficient image watermarking scheme using Lagrangian SVR," *Multimed. Tools Appl.*, vol. 75, no. 7, pp. 4129–4150, Apr. 2016, doi: 10.1007/s11042-015-3084-5.
- [102] Y. Naderahmadian and S. Hosseini-Khayat, "Fast Watermarking Based on QR Decomposition in Wavelet Domain," in *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Oct. 2010, pp. 127–130. doi: 10.1109/IIHMSP.2010.39.
- [103] H. Peng, J. Wang, and W. Wang, "Image watermarking method in multiwavelet domain based on support vector machines," *J. Syst. Softw.*, vol. 83, no. 8, pp. 1470–1477, Aug. 2010, doi: 10.1016/j.jss.2010.03.006.
- [104] W. Song, J. Hou, Z. Li, and L. Huang, "Chaotic system and QR factorization based robust digital image watermarking algorithm," *J. Cent. South Univ. Technol.*, vol. 18, no. 1, pp. 116–124, Feb. 2011, doi: 10.1007/s11771-011-0668-8.
- [105] J. Li, C. Yu, B. B. Gupta, and X. Ren, "Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition," *Multimed. Tools Appl.*, vol. 77, no. 4, pp. 4545–4561, Feb. 2018, doi: 10.1007/s11042-017-4452-0.
- [106] Q. Su, Y. Niu, Q. Wang, and G. Sheng, "A blind color image watermarking based on DC component in the spatial domain," *Optik*, vol. 124, no. 23, pp. 6255–6260, Dec. 2013, doi: 10.1016/j.ijleo.2013.05.013.
- [107] A. Shehab *et al.*, "Secure and Robust Fragile Watermarking Scheme for Medical Images," *IEEE Access*, vol. 6, pp. 10269–10278, 2018, doi: 10.1109/ACCESS.2018.2799240.
- [108] R. O. Preda, "Self-recovery of unauthentic images using a new digital watermarking approach in the wavelet domain," in *2014 10th International Conference on Communications (COMM)*, May 2014, pp. 1–4. doi: 10.1109/ICComm.2014.6866744.
- [109] M. El'arbi and C. B. Amar, "Image authentication algorithm with recovery capabilities based on neural networks in the DCT domain," *IET Image Process.*, vol. 8, no. 11, pp. 619–626, 2014.
- [110] V. S. Dhole and N. N. Patil, "Self Embedding Fragile Watermarking for Image Tampering Detection and Image Recovery Using Self Recovery Blocks," in *2015 International Conference on Computing Communication Control and Automation*, Feb. 2015, pp. 752–757. doi: 10.1109/ICCUBEA.2015.150.
- [111] B. Patra and J. C. Patra, "CRT-based fragile self-recovery watermarking scheme for image authentication and recovery," in *2012 International Symposium on Intelligent Signal Processing and Communications Systems*, Nov. 2012, pp. 430–435. doi: 10.1109/ISPACS.2012.6473528.
- [112] S. Iftikhar, M. Kamran, E. U. Munir, and S. U. Khan, "A Reversible Watermarking Technique for Social Network Data Sets for Enabling Data Trust in Cyber, Physical, and Social Computing," *IEEE Syst. J.*, vol. 11, no. 1, pp. 197–206, Mar. 2017, doi: 10.1109/JSYST.2015.2416131.
- [113] M. Andalibi and D. M. Chandler, "Digital Image Watermarking via Adaptive Logo Texturization," *IEEE Trans. Image Process.*, vol. 24, no. 12, pp. 5060–5073, Dec. 2015, doi: 10.1109/TIP.2015.2476961.
- [114] X. Wu and Z.-H. Guan, "A novel digital watermark algorithm based on chaotic maps," *Phys. Lett. A*, vol. 365, no. 5–6, pp. 403–406, 2007.
- [115] V. Reddy and V. Sourirajan, "An Effective Wavelet-Based Watermarking Scheme Using Human Visual System for Protecting Copyrights of Digital Images," *Int. J. Comput. Electr. Eng.*, pp. 32–40, Jan. 2010, doi: 10.7763/IJCEE.2010.V2.109.

- [116] C. Jin, F. Tao, and Y. Fu, "Image Watermarking Based HVS Characteristic of Wavelet Transform," in *2006 International Conference on Intelligent Information Hiding and Multimedia*, Dec. 2006, pp. 71–74. doi: 10.1109/IIH-MSP.2006.264957.
- [117] E. First and X. Qi, "A Composite Approach for Blind Grayscale Logo Watermarking," in *2007 IEEE International Conference on Image Processing*, Sep. 2007, vol. 3, p. III-265-III-268. doi: 10.1109/ICIP.2007.4379297.
- [118] D. S. Chauhan, A. K. Singh, A. Adarsh, B. Kumar, and J. P. Saini, "Combining Mexican hat wavelet and spread spectrum for adaptive watermarking and its statistical detection using medical images," *Multimed. Tools Appl.*, vol. 78, no. 10, pp. 12647–12661, 2019.
- [119] X. Zhou, H. Zhang, and C. Wang, "A Robust Image Watermarking Technique Based on DWT, APDCBT, and SVD," *Symmetry*, vol. 10, no. 3, p. 77, Mar. 2018, doi: 10.3390/sym10030077.
- [120] S. Fazli and M. Moeini, "A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks," *Optik*, vol. 127, no. 2, pp. 964–972, Jan. 2016, doi: 10.1016/j.ijleo.2015.09.205.
- [121] E. E. D. Hemdan, N. El Fishawy, G. Attiya, and F. A. El-Samie, "An efficient image watermarking approach based on wavelet fusion and singular value decomposition in wavelet domain," in *Proceeding of 3rd International Conference on Advanced Control Circuits And Systems (ACCS'013)*, 2013, no. 1–10.
- [122] A. K. Singh, "Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images," *Multimed. Tools Appl.*, vol. 76, no. 6, pp. 8881–8900, Mar. 2017, doi: 10.1007/s11042-016-3514-z.
- [123] D. Rosiyadi, S.-J. Horng, P. Fan, X. Wang, M. K. Khan, and Y. Pan, "Copyright protection for e-government document images," *IEEE Multimed.*, vol. 19, no. 3, pp. 62–73, 2011.
- [124] A. Singh and A. Tayal, "Choice of Wavelet from Wavelet Families for DWT-DCT-SVD Image Watermarking," *Int. J. Comput. Appl.*, vol. 48, no. 17, pp. 9–14, Jun. 2012, doi: 10.5120/7439-0375.
- [125] A. Srivastava and P. Saxena, "DWT-DCT-SVD based semiblind image watermarking using middle frequency band," *IOSR J Comput Eng*, vol. 12, no. 2, pp. 63–66, 2013.
- [126] S. Thakur, A. K. Singh, S. P. Ghrera, and A. Mohan, "Chaotic based secure watermarking approach for medical images," *Multimed. Tools Appl.*, vol. 79, no. 7–8, pp. 4263–4276, Feb. 2020, doi: 10.1007/s11042-018-6691-0.
- [127] D. Bouslimi, G. Coatrieux, and C. Roux, "A joint watermarking/encryption algorithm for verifying medical image integrity and authenticity in both encrypted and spatial domains," in *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Boston, MA, Aug. 2011, pp. 8066–8069. doi: 10.1109/IEMBS.2011.6091989.
- [128] F. N. Thakkar and V. K. Srivastava, "A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications," *Multimed. Tools Appl.*, vol. 76, no. 3, pp. 3669–3697, Feb. 2017, doi: 10.1007/s11042-016-3928-7.
- [129] A. K. Singh, B. Kumar, M. Dave, and A. Mohan, "Multiple Watermarking on Medical Images Using Selective Discrete Wavelet Transform Coefficients," *J. Med. Imaging Health Inform.*, vol. 5, no. 3, pp. 607–614, Jun. 2015, doi: 10.1166/jmihi.2015.1432.

- [130] S. A. Parah, J. A. Sheikh, F. Ahad, N. A. Loan, and G. M. Bhat, "Information hiding in medical images: a robust medical image watermarking system for E-healthcare," *Multimed. Tools Appl.*, vol. 76, no. 8, pp. 10599–10633, Apr. 2017, doi: 10.1007/s11042-015-3127-y.
- [131] Y. Liu, L. Ju, M. Hu, X. Ma, and H. Zhao, "A robust reversible data hiding scheme for H.264 without distortion drift," *Neurocomputing*, vol. 151, pp. 1053–1062, Mar. 2015, doi: 10.1016/j.neucom.2014.03.088.
- [132] Y. Liu, Z. Li, and X. Ma, "Reversible Data Hiding Scheme Based On H. 264/AVC without Distortion Drift.," *J Softw*, vol. 7, no. 5, pp. 1059–1065, 2012.
- [133] A. K. Singh, B. Kumar, S. K. Singh, S. P. Ghrera, and A. Mohan, "Multiple watermarking technique for securing online social network contents using Back Propagation Neural Network," *Future Gener. Comput. Syst.*, vol. 86, pp. 926–939, Sep. 2018, doi: 10.1016/j.future.2016.11.023.
- [134] Y. Xing and J. Tan, "A Color Image Watermarking Scheme Resistant against Geometrical Attacks," vol. 19, no. 1, p. 6, 2010.
- [135] A. Ghafoor and M. Imran, "A Non-blind Color Image Watermarking Scheme Resistent Against Geometric Attacks," vol. 21, no. 4, p. 6, 2012.
- [136] V. Santhi and A. Thangavelu, "DC Coefficients Based Watermarking Techniquefor color Images Using Singular ValueDecomposition," *Int. J. Comput. Electr. Eng.*, vol. 3, pp. 8–16, Jan. 2011, doi: 10.7763/IJCEE.2011.V3.285.
- [137] M. Zhao and Y. Dang, "Color image copyright protection digital watermarking algorithm based on DWT & DCT," in *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*, 2008, pp. 1–4.
- [138] X. Xiong, "A new robust color image watermarking scheme based on 3D-DCT," *World J. Eng. Technol.*, vol. 3, no. 03, p. 177, 2015.
- [139] H. Shi, F. Lv, and Y. Cao, "A Blind Watermarking Technique for Color Image based on SVD with Circulation.," *J Softw*, vol. 9, no. 7, pp. 1749–1756, 2014.
- [140] T. P. Duy, D. Tran, and W. Ma, "An intelligent learning-based watermarking scheme for outsourced biomedical time series data," in *2017 International Joint Conference on Neural Networks (IJCNN)*, Anchorage, AK, USA, May 2017, pp. 4408–4415. doi: 10.1109/IJCNN.2017.7966414.
- [141] T. D. Pham, D. Tran, and W. Ma, "A proposed blind DWT-SVD watermarking scheme for EEG data," in *International Conference on Neural Information Processing*, 2015, pp. 69–76.
- [142] P. Ramu and R. Swaminathan, "Imperceptibility—robustness tradeoff studies for ECG steganography using continuous ant colony optimization," *Expert Syst. Appl.*, vol. 49, pp. 123–135, 2016.
- [143] S. E. Jero, P. Ramu, and S. Ramakrishnan, "Discrete wavelet transform and singular value decomposition based ECG steganography for secured patient information transmission," *J. Med. Syst.*, vol. 38, no. 10, pp. 1–11, 2014.
- [144] V. Aslantas, "A singular-value decomposition-based image watermarking using genetic algorithm," *AEU - Int. J. Electron. Commun.*, vol. 62, no. 5, pp. 386–394, May 2008, doi: 10.1016/j.aeu.2007.02.010.
- [145] K. Loukhaoukha, M. Nabti, and K. Zebbiche, "A robust SVD-based image watermarking using a multi-objective particle swarm optimization," *Opto-Electron. Rev.*, vol. 22, no. 1, Jan. 2014, doi: 10.2478/s11772-014-0177-z.

- [146] M. Ali and C. W. Ahn, "An optimal image watermarking approach through cuckoo search algorithm in wavelet domain," *Int. J. Syst. Assur. Eng. Manag.*, vol. 9, no. 3, pp. 602–611, Jun. 2018, doi: 10.1007/s13198-014-0288-4.
- [147] S. Iftikhar, M. Kamran, and Z. Anwar, "RRW—A Robust and Reversible Watermarking Technique for Relational Data," *IEEE Trans. Knowl. Data Eng.*, vol. 27, no. 4, pp. 1132–1145, Apr. 2015, doi: 10.1109/TKDE.2014.2349911.
- [148] Z. Zheng, N. Saxena, K. K. Mishra, and A. K. Sangaiah, "Guided dynamic particle swarm optimization for optimizing digital image watermarking in industry applications," *Future Gener. Comput. Syst.*, vol. 88, pp. 92–106, Nov. 2018, doi: 10.1016/j.future.2018.05.027.
- [149] M. Sharma and J. K. Chhabra, "An efficient hybrid PSO polygamous crossover based clustering algorithm," *Evol. Intell.*, vol. 14, no. 3, pp. 1213–1231, Sep. 2021, doi: 10.1007/s12065-019-00235-4.
- [150] P. Kapoor, K. K. Sharma, S. S. Bedi, and A. Kumar, "Colored image watermarking technique based on HVS using HSV color model," in *Proceedings of International Conference on Advances in Computer Engineering*, 2011, pp. 20–24.
- [151] B. L. Gunjal, "Wavelet based color image watermarking scheme giving high robustness and exact correlation," *Int. J. Emerg. Trends Eng. Technol. IJETET*, vol. 1, no. 1, pp. 21–30, 2011.
- [152] N. V. Dharwadkar, G. K. Kulkarni, T. Y. Melligeri, and B. B. Amberker, "The image watermarking scheme using edge information in YCbCr color space," *Int. Proc. Comput. Sci. Inf. Technol.*, vol. 56, p. 127, 2012.
- [153] E. L. Lydia, J. S. Raj, R. Pandi Selvam, M. Elhoseny, and K. Shankar, "Application of discrete transforms with selective coefficients for blind image watermarking," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 2, p. e3771, 2021.
- [154] S. P. Vaidya and P. C. Mouli, "Adaptive digital watermarking for copyright protection of digital images in wavelet domain," *Procedia Comput. Sci.*, vol. 58, pp. 233–240, 2015.
- [155] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," *Signal Process.*, vol. 66, no. 3, pp. 385–403, 1998.
- [156] O. Bruyndonckx, "Spatial method for copyright labelling of digital images," in *Proc. of 1995 IEEE Nonlinear signal Processing Workshop*, 1995, pp. 456–459.
- [157] S. D. Lin and C.-F. Chen, "A robust DCT-based watermarking for copyright protection," *IEEE Trans. Consum. Electron.*, vol. 46, no. 3, pp. 415–421, 2000.
- [158] A. Mishra, C. Agarwal, A. Sharma, and P. Bedi, "Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm," *Expert Syst. Appl.*, vol. 41, no. 17, pp. 7858–7867, 2014.
- [159] F. A. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems," in *International workshop on information hiding*, 1998, pp. 218–238.
- [160] R. v Totla and K. S. Bapat, "Comparative Analysis of Watermarking in Digital Images Using DCT & DWT," *Int. J. Sci. Res. Publ.*, vol. 3, no. 2, p. 1, 2013.
- [161] S. D. Daphal, P. K. Aher, S. B. Galande, and S. K. Jagtap, "Comparison of key transform domain watermarking methods based on performance measures," in *2018 International Conference on Communication information and Computing Technology (ICCICT)*, 2018, pp. 1–6.
- [162] M. Begum and M. S. Uddin, "Digital image watermarking techniques: a review," *Information*, vol. 11, no. 2, p. 110, 2020.

- [163] P. Khare and V. K. Srivastava, "A Novel Dual Image Watermarking Technique Using Homomorphic Transform and DWT," *J. Intell. Syst.*, vol. 30, no. 1, pp. 297–311, Jan. 2021, doi: 10.1515/jisys-2019-0046.
- [164] M. K. H. Kolekar, G. L. Raja, and S. Sengupta, "An Introduction to Wavelet-Based Image Processing and Its Applications," *Computer Vision: Concepts, Methodologies, Tools, and Applications*, 2018. <https://www.igi-global.com/chapter/an-introduction-to-wavelet-based-image-processing-and-its-applications/www.igi-global.com/chapter/an-introduction-to-wavelet-based-image-processing-and-its-applications/196952> (accessed Mar. 04, 2022).
- [165] S. Priya, R. Varatharajan, G. Manogaran, R. Sundarasekar, and P. M. Kumar, "Paillier homomorphic cryptosystem with poker shuffling transformation based water marking method for the secured transmission of digital medical images," *Pers. Ubiquitous Comput.*, vol. 22, no. 5, pp. 1141–1151, 2018.
- [166] C. K. Jha and M. H. Kolekar, "Electrocardiogram Data Compression Techniques for Cardiac Healthcare Systems: A Methodological Review," *IRBM*, p. S1959031821000750, Jun. 2021, doi: 10.1016/j.irbm.2021.06.007.
- [167] S. D. Lin, S.-C. Shie, and J. Y. Guo, "Improving the robustness of DCT-based image watermarking against JPEG compression," *Comput. Stand. Interfaces*, vol. 32, no. 1–2, pp. 54–60, 2010.
- [168] C.-C. Chang, P. Tsai, and C.-C. Lin, "SVD-based digital image watermarking scheme," *Pattern Recognit. Lett.*, vol. 26, no. 10, pp. 1577–1586, 2005.
- [169] M.-Q. Fan, H.-X. Wang, and S.-K. Li, "Restudy on SVD-based watermarking scheme," *Appl. Math. Comput.*, vol. 203, no. 2, pp. 926–930, 2008.
- [170] C. Saha, Md. F. Hossain, and Md. A. Rahman, "NSCT-based robust image watermarking in DC components of APDCBT using singular value decomposition," *Iran J. Comput. Sci.*, vol. 4, no. 3, pp. 133–145, Sep. 2021, doi: 10.1007/s42044-020-00070-2.
- [171] K. Prabha, M. J. Vaishnavi, and I. S. Sam, "Quaternion Hadamard transform and QR decomposition based robust color image watermarking," in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, 2019, pp. 101–106.
- [172] E. Candes, L. Demanet, D. Donoho, and L. Ying, "Fast discrete curvelet transforms," *Multiscale Model. Simul.*, vol. 5, no. 3, pp. 861–899, 2006.
- [173] S. E. Jero, P. Ramu, and S. Ramakrishnan, "ECG steganography using curvelet transform," *Biomed. Signal Process. Control*, vol. 22, pp. 161–169, 2015.
- [174] M. Mittal *et al.*, "Image watermarking in curvelet domain using edge surface blocks," *Symmetry*, vol. 12, no. 5, p. 822, 2020.
- [175] C. Zhang, L. L. Cheng, Z. Qiu, and L.-M. Cheng, "Multipurpose watermarking based on multiscale curvelet transform," *IEEE Trans. Inf. Forensics Secur.*, vol. 3, no. 4, pp. 611–619, 2008.
- [176] M. N. Do and M. Vetterli, "The contourlet transform: an efficient directional multiresolution image representation," *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2091–2106, 2005.
- [177] M. Rabizadeh, M. Amirmazlaghani, and M. Ahmadian-Attari, "A new detector for contourlet domain multiplicative image watermarking using Bessel K form distribution," *J. Vis. Commun. Image Represent.*, vol. 40, pp. 324–334, 2016.
- [178] A. K. Singh, B. Kumar, G. Singh, and A. Mohan, *Medical image watermarking: techniques and applications*. Springer, 2017.

- [179] I. J. Cox, M. L. Miller, J. A. Bloom, and C. Honsinger, *Digital watermarking*, vol. 53. Springer, 2002.
- [180] Y. Liu, S. Tang, R. Liu, L. Zhang, and Z. Ma, “Secure and robust digital image watermarking scheme using logistic and RSA encryption,” *Expert Syst. Appl.*, vol. 97, pp. 95–105, May 2018, doi: 10.1016/j.eswa.2017.12.003.
- [181] M. Boussif, N. Aloui, and A. Cherif, “Secured cloud computing for medical data based on watermarking and encryption,” *IET Netw.*, vol. 7, no. 5, pp. 294–298, 2018.
- [182] T.-Y. Seong, K.-C. Kwon, S.-H. Lee, K.-S. Moon, and K.-R. Kwon, “DCT and Homomorphic Encryption based Watermarking Scheme in Buyer-seller Watermarking Protocol,” *J. Korea Multimed. Soc.*, vol. 17, no. 12, pp. 1402–1411, 2014, doi: 10.9717/kmms.2014.17.12.1402.
- [183] C. Jost, H. Lam, A. Maximov, and B. Smeets, “Encryption performance improvements of the paillier cryptosystem,” *Cryptol. EPrint Arch.*, 2015.
- [184] H. A. Abdallah *et al.*, “Homomorphic image watermarking with a singular value decomposition algorithm,” *Inf. Process. Manag.*, vol. 50, no. 6, pp. 909–923, Nov. 2014, doi: 10.1016/j.ipm.2014.07.001.
- [185] R. Gupta, A. Mishra, and S. Jain, “Secure Image Watermarking in a Compressed SPIHT Domain Using Paillier Cryptosystem,” *Int. J. Inf. Syst. Model. Des. IJISMD*, vol. 10, no. 4, pp. 51–70, Oct. 2019, doi: 10.4018/IJISMD.2019100103.
- [186] M. O’Keeffe, “The Paillier cryptosystem: a look into the cryptosystem and its potential application,” *Coll. N. J.*, 2008.
- [187] Z. Zhang, C. Wang, and X. Zhou, “Image watermarking scheme based on Arnold transform and DWT-DCT-SVD,” in *2016 IEEE 13th International Conference on Signal Processing (ICSP)*, Nov. 2016, pp. 805–810. doi: 10.1109/ICSP.2016.7877942.
- [188] L. Min, L. Ting, and H. Yu-jie, “Arnold Transform Based Image Scrambling Method:,” presented at the 3rd International Conference on Multimedia Technology(ICMT-13), Guangzhou, China, 2013. doi: 10.2991/icmt-13.2013.160.
- [189] Q. Su and B. Chen, “Robust color image watermarking technique in the spatial domain,” *Soft Comput.*, vol. 22, no. 1, pp. 91–106, Jan. 2018, doi: 10.1007/s00500-017-2489-7.
- [190] C. Das, S. Panigrahi, V. K. Sharma, and K. K. Mahapatra, “A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation,” *AEU-Int. J. Electron. Commun.*, vol. 68, no. 3, pp. 244–253, 2014.
- [191] M. Ishtiaq, M. A. Jaffar, M. A. Khan, Z. Jan, and A. M. Mirza, “Robust and Imperceptible Watermarking of Video Streams for Low Power Devices,” in *Signal Processing, Image Processing and Pattern Recognition*, Berlin, Heidelberg, 2009, pp. 177–184. doi: 10.1007/978-3-642-10546-3_22.
- [192] B. Sikander, M. Ishtiaq, M. A. Jaffar, M. Tariq, and A. M. Mirza, “Adaptive Digital Watermarking of Images Using Genetic Algorithm,” in *2010 International Conference on Information Science and Applications*, Apr. 2010, pp. 1–8. doi: 10.1109/ICISA.2010.5480367.
- [193] S. Verma, A. Chug, and A. P. Singh, “Prediction Models for Identification and Diagnosis of Tomato Plant Diseases,” in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Bangalore, Sep. 2018, pp. 1557–1563. doi: 10.1109/ICACCI.2018.8554842.

- [194] C. Agarwal, A. Mishra, and A. Sharma, "Gray-scale image watermarking using GA-BPN hybrid network," *J. Vis. Commun. Image Represent.*, vol. 24, no. 7, pp. 1135–1146, Oct. 2013, doi: 10.1016/j.jvcir.2013.07.007.
- [195] C.-H. Huang and J.-L. Wu, "Watermark optimization technique based on genetic algorithms," in *Security and Watermarking of Multimedia Contents II*, 2000, vol. 3971, pp. 516–523.
- [196] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Opt. Lasers Eng.*, vol. 56, pp. 83–93, May 2014, doi: 10.1016/j.optlaseng.2013.12.003.
- [197] E. M. El Houbay and N. I. Yassin, "Wavelet-Hadamard based blind image watermarking using genetic algorithm and decision tree," *Multimed. Tools Appl.*, vol. 79, no. 37, pp. 28453–28474, 2020.
- [198] "Comparison of multiple watermarking techniques using genetic algorithms - ScienceDirect." <https://www.sciencedirect.com/science/article/pii/S231471721630006X> (accessed Nov. 18, 2021).
- [199] W.-C. Hong, Y. Dong, W. Y. Zhang, L.-Y. Chen, and B. K. Panigrahi, "Cyclic electric load forecasting by seasonal SVR with chaotic genetic algorithm," *Int. J. Electr. Power Energy Syst.*, vol. 44, no. 1, pp. 604–614, Jan. 2013, doi: 10.1016/j.ijepes.2012.08.010.
- [200] A. Bajaj and O. P. Sangwan, "A Systematic Literature Review of Test Case Prioritization Using Genetic Algorithms," *IEEE Access*, vol. 7, pp. 126355–126375, 2019, doi: 10.1109/ACCESS.2019.2938260.
- [201] W.-C. Hong, Y. Dong, L.-Y. Chen, and S.-Y. Wei, "SVR with hybrid chaotic genetic algorithms for tourism demand forecasting," *Appl. Soft Comput.*, vol. 11, no. 2, pp. 1881–1890, Mar. 2011, doi: 10.1016/j.asoc.2010.06.003.
- [202] R. Mehta, N. Rajpal, and V. P. Vishwakarma, "Robust image watermarking scheme in lifting wavelet domain using GA-LSVR hybridization," *Int. J. Mach. Learn. Cybern.*, vol. 9, no. 1, pp. 145–161, Jan. 2018, doi: 10.1007/s13042-015-0329-6.
- [203] S. Katoch, S. S. Chauhan, and V. Kumar, "A review on genetic algorithm: past, present, and future," *Multimed. Tools Appl.*, vol. 80, no. 5, pp. 8091–8126, Feb. 2021, doi: 10.1007/s11042-020-10139-6.
- [204] M. Sadeghzadeh and M. Taherbaghal, "A new method for watermarking using genetic algorithms," in *International Conference on Machine Learning, Electrical and Mechanical Engineering (ICMLEME'2014) Jan*, 2014, pp. 8–9.
- [205] H. M. Pandey, M. Trovati, and N. Bessis, "Statistical exploratory analysis of mask-fill reproduction operators of Genetic Algorithms," *Appl. Soft Comput.*, vol. 102, p. 107087, Apr. 2021, doi: 10.1016/j.asoc.2021.107087.
- [206] C.-S. Shieh, H.-C. Huang, F.-H. Wang, and J.-S. Pan, "Genetic watermarking based on transform-domain techniques," *Pattern Recognit.*, vol. 37, no. 3, pp. 555–565, 2004.
- [207] N. Arya and A. P. Singh, "A fault avoidance approach with test set generation in combinational circuits using genetic algorithm," in *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, Jan. 2018, pp. 1439–1445. doi: 10.1109/ICISC.2018.8399045.
- [208] R. Mehta, K. Gupta, and A. K. Yadav, "An adaptive framework to image watermarking based on the twin support vector regression and genetic algorithm in lifting wavelet transform domain.," *Multimed. Tools Appl.*, vol. 79, 2020.

- [209] X. Zhou, C. Cao, J. Ma, and L. Wang, “Adaptive Digital Watermarking Scheme Based on Support Vector Machines and Optimized Genetic Algorithm,” *Math. Probl. Eng.*, vol. 2018, p. e2685739, Mar. 2018, doi: 10.1155/2018/2685739.
- [210] R. Chaturvedi, A. Sharma, U. Dwivedi, S. Kumar, and A. Praveen, “Security Enhanced Image Watermarking using Mid-Band DCT Coefficient in YCbCr Space,” p. 8.
- [211] A. Ray and S. Roy, “Recent trends in image watermarking techniques for copyright protection: a survey,” *Int. J. Multimed. Inf. Retr.*, vol. 9, no. 4, pp. 249–270, Dec. 2020, doi: 10.1007/s13735-020-00197-9.
- [212] S.-J. Horng, D. Rosiyadi, P. Fan, X. Wang, and M. K. Khan, “An adaptive watermarking scheme for e-government document images,” *Multimed. Tools Appl.*, vol. 72, no. 3, pp. 3085–3103, Oct. 2014, doi: 10.1007/s11042-013-1579-5.
- [213] E. E. Hemdan, N. El-Fishawy, G. Attiya, and F. A. El-samie, “C11. Hybrid Digital Image Watermarking Technique for Data Hiding,” in *2013 30th National Radio Science Conference (NRSC)*, Apr. 2013, pp. 220–227. doi: 10.1109/NRSC.2013.6587920.
- [214] P. Khare and V. K. Srivastava, “Robust Digital Image Watermarking Scheme Based on RDWT-DCT-SVD,” in *2018 5th International Conference on Signal Processing and Integrated Networks (SPIN)*, Feb. 2018, pp. 88–93. doi: 10.1109/SPIN.2018.8474125.
- [215] S. Gaur and V. Kumar, “A RDWT and Block-SVD based Dual Watermarking Scheme for Digital Images,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 4, 2017, doi: 10.14569/IJACSA.2017.080430.
- [216] I. Mehra and N. K. Nishchal, “Image fusion using wavelet transform and its application to asymmetric cryptosystem and hiding,” *Opt. Express*, vol. 22, no. 5, pp. 5474–5482, Mar. 2014, doi: 10.1364/OE.22.005474.