

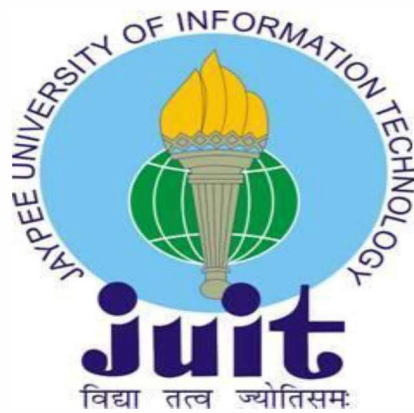
ROBUST AND SECURE WATERMARKING SCHEME FOR MULTIMEDIA DATA AGAINST VARIOUS ATTACKS

Thesis submitted in fulfillment of the requirement of the Degree of

Doctor of Philosophy

By

LAXMANIKA



Department of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology

Waknaghat, Solan-173234, Himachal Pradesh,

May 2024

@Copyright JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY WAKNAGHAT

MAY 2024

ALL RIGHTS RESERVED

DECLARATION BY THE SCHOLAR

I hereby declare that the work reported in the PhD thesis entitled "**Robust and Secure Watermarking Scheme for Multimedia Data against Various Attacks**" submitted at **Jaypee University of Information Technology, Wagnaghat**, India is an authentic record of my work carried out under the supervision of **Dr. Jagpreet Sidhu** 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 PhD Thesis.

A handwritten signature in blue ink, appearing to read 'Laxmanika', written over a horizontal line.

(Signature of the Scholar)

(Laxmanika)

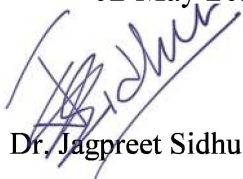
Department of Computer Science & Engineering and Information Technology,
JUIT, Wagnaghat, Solan -173234, India.

Date: 02 May 2024

SUPERVISOR'S CERTIFICATE

This is to certify that the work in the thesis entitled “**Robust and Secure Watermarking Scheme for Multimedia Data against Various Attacks**” submitted by **Laxmanika** is a record of an original research work carried out by him under our supervision and guidance in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy in Computer Science and Engineering in the Department of Computer Science and Engineering, **Jaypee University of Information Technology, Waknaghat, India**. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Date: 02 May 2024



Dr. Jagpreet Sidhu,

Associate Professor

Department of Computer Engineering

NMIMS Deemed University, Chandigarh-160014, India



Dr. Pradeep Kumar Singh

Associate Professor

Department of Computer Science and Engineering (CSE)

Central University of Jammu, J&K-181143, India

ACKNOWLEDGEMENT

First and foremost, thanks to **GOD**, the Almighty, to whom I owe my very existence. I would like to thank Him, who gave me the grace and privilege to pursue this programme and successfully complete it in spite of the many challenges I faced.

With an overwhelming sense of legitimate pride and a genuine obligation, which gives me exuberant pleasure and privilege, I reiterate my indebtedness to prudent, speculative and dignified supervisors **Dr. Jagpreet Sidhu**, Associate Professor (NMIMS University) and **Dr. Pradeep Kumar Singh**, Associate Professor (Central University of Jammu) for their incessant guidance, eternal encouragements, painstaking efforts and keen interest during the investigation and finally scanning the manuscript in a meticulous way.

I am also grateful to **Prof. (Dr.) Vivek Kumar Sehgal**, Head, Department of Computer Science and Engineering & IT, for his insightful comments and administrative help on various occasions. I extend my sincere thanks to my DPMC members **Dr. Yugal Kumar, Dr. Pardeep Kumar and Dr. Gopal Singh Bisht** for their stimulating questions and valuable feedback. I owe my thanks to the other faculty members of the department for their valuable feedback and support.

A formal acknowledgement of my emotions to convey the depth of my love and affection to my reverend parents **Sh. Harmendra Singh** and **Smt. Shashi** for their prudent persuasion, selfless sacrifice and heartfelt blessings, which have enabled me to translate their dreams into reality.

In spite of all these, I am grateful to my husband **Dr. Naman Garg**, for having patience and giving priority to my research work. In fact, I have no words to express my gratitude towards him. He made me concentrate on my work while taking very good care of all other things.

A special thanks to my Brother, Sister and Sister in law, **Shivanshu Singh, Nalnika Kairot and Anu Singh** for their encouragement and never-ending help during the entire course of study. And I can never forget to mention my adorable niece and nephew, **Manya Kairot and Krishiv (Govind)**, for their love and affection, which give me constant strength to go on throughout the span of my studies.

This note of acknowledgement will always be incomplete without the mention of my Brother in law, Sister in law and Mother in law **Mr. Shubham Garg, Dr. Lalima Garg and Smt. Sadhna Garg** for their love and affection which always gives me moral support and strength. Lastly, I would like to thank each and every one of them who helped me directly or indirectly during this wonderful and lots of experience-gaining journey. I once again bow my head before the almighty to facilitate me at every stage of my dream to accomplish this task.

Needless to say, errors and omissions are solely mine.

Date: 02 May 2024


(LAXMANIKA)

ABSTRACT

The widespread adoption of digital technology has become prevalent in various domains. Concurrently, the internet began reshaping the world into a closely interconnected global community. While digital data offered numerous advantages over analog inputs, including ease of storage and transmission, many providers of multimedia content expressed reservations. They were concerned that the high-quality replication made possible by digital files might infringe upon their copyrights. Since necessity is the creator of innovation, watermarking methods were developed to address this issue. A hidden and undetectable piece of data is inserted into the digital file during watermarking. Such confidential information might be a logo or another piece of information that helps users identify the content source or creator. By obtaining concealed information from the digital data, the source owner might readily establish his ownership in the event of a dispute. The current work focuses on imaging watermarking to provide the confirmed authenticity of transferred multimedia files. This is done in light of the abovementioned and recognizing the broad applications of multimedia as well as its associated security issues. The thesis proposes several enhanced methods of multimedia image watermarking that give superior robustness and show the positive quality, greater embedding capacity, and confidentiality of the watermark after evaluating the present techniques for multimedia image watermarking.

In this thesis, four kinds of problems have been proposed related to watermarking techniques for multimedia data. The first is concerned with a method for watermarking images utilizing the discrete cosine transform (DCT), bi-dimensional empirical mode decomposition (BEMD), and particle swarm optimization (PSO). DCT coefficient is utilized on the initial image during the encoding process, and then the watermark image is divided apart using BEMD decomposition. Particle swarm optimization (PSO) is employed to optimize complicated and multidimensional searches. The security key is used to embed the scaling and embedding factors. IDCT and IBEMD are used during the process, and a recovery procedure is also utilized to extract the watermark image.

The second deals with introducing robust image watermarking using SVD (singular value decomposition), BEMD, DCT, PSO, and DWT (discrete wavelet transform). Second-level DWT

is employed throughout the embedding procedure to deconstruct the cover image and watermark the image into sub-bands. Moreover, BEMD decomposition is implemented at the chosen DWT frequency. For optimization, PSO is employed for complicated as well as multidimensional searches. Moreover, DCT, as well as SVD, are implemented on the selected band. The embedding and the scaling factor are encoded with the aid of a security key. This technique is followed by ISVD, IDCT, IDWT, and IBEMD. The suggested method produces watermarked images with superior visual clarity and robustness against various attacks such as speckle, median filter, shearing, salt and pepper, gamma correction, scaling, Gaussian filter, and rotation for greyscale images.

The third issue relates to an improved watermarking method using DWT, SVD, and BEMD where the watermark image is scrambled with Arnold transform to enhance the algorithm's security. The BEMD disintegrates the input image in this instance to provide the multi-scale demonstration in the form of IMFs and residue. The suggested algorithm offers greater robustness and imperceptibility against several geometrical and non-geometric attacks.

The last issue addressed in this study pertained to a watermarking method that combined DWT and BEMD for ownership verification, aiming to provide markedly improved visual quality compared to alternative decomposition techniques. BEMD can identify the image from the lowest fragile frequencies to the most robust frequencies. Also, the performance comparison with other competitive methodologies provides superior outcomes for various attacks.

Table of Content

CONTENT	PAGE NO.
DECLARATION BY STUDENT	iii
SUPERVISOR'S CERTIFICATE	iv
ACKNOWLEDGEMENT	v
ABSTRACT	vi-vii
LIST OF FIGURES	xi-xii
LIST OF TABLES	xiii-xiv
LIST OF ABBREVIATION	xv-xvi
CHAPTER 1: INTRODUCTION	1-11
1.1 Types of digital watermarks	2
1.2 Watermarking Attacks	4
1.3 Current applications for digital watermarking	5
1.4 Watermark Encoding and Recovery procedure	6
1.5 Performance measures for digital watermarking	8-9
1.6 Significant contribution of the work	10
1.7 Thesis organization	10-11
CHAPTER 2: STUDY OF LITERATURE	12-23
2.1 Digital Image Watermarking	12
2.1.1 Spatial domain based watermarking system	13
2.1.2 Frequency domain based watermarking system	13
2.2 BEMD based watermarking system	14
2.3 Robust hybrid watermarking system	14
2.4 Optimization based watermarking system	16
2.5 Arnold based watermarking system	17
2.6 Deep Learning based watermarking system	18
2.7 Research gaps	22
2.8 Research objectives	22

2.9 Research procedure	23
CHAPTER 3: IMPROVED ROBUSTNESS THROUGH BI-EMPIRICAL MODE AND DISCRETE COSINE TRANSFORM USING PSO	24-32
3.1 Introduction	24
3.2 Watermarking scheme	25
3.2.1 Watermarking embedding and extraction process	25
3.3 Experimental result	26
CHAPTER 4: IMPROVED ROBUST AND IMPERCEPTIBLE IMAGE WATERMARKING THROUGH BEMD, DCT, SVD USING PSO IN WAVELET DOMAIN	33-52
4.1 Introduction	33
4.2 The proposed method	39
4.2.1 Algorithm for watermark embedding	39
4.2.2 Watermark recovery algorithm	42
4.3 Experimental results and analysis	42
CHAPTER 5: ROBUST AND SECURE WATERMARKING THROUGH ARNOLD TRANSFORM IN BEMD, SVD AND DWT DOMAIN	53-66
5.1 Introduction	53
5.2 Proposed technique	55
5.2.1 Algorithm for watermarks embedding	56
5.2.2 Algorithm for watermarks recovery	57
5.3 Experimental results and analysis	58
CHAPTER 6: ROBUST WATERMARKING APPROACH USING BEMD IN WAVELET DOMAIN	67-81
6.1 Introduction	67
6.2 Proposed technique	70
6.2.1 Algorithm for watermarks embedding	72
6.2.2 Algorithm for watermarks recovery	73
6.3 Experimental results and analysis	73

CHAPTER 7: CONCLUSION AND FUTURE DIRECTIONS	82-83
REFERENCES	84-92
LIST OF PUBLICATION	93-94

LIST OF FIGURES

1.1	Features of digital watermarks	2
1.2	Key Watermark attacks	4
1.3	Application of digital watermarking	5
1.4	Frequency domain and spatial domain watermarking technique	6
1.5	Watermarking (a) encoding Process (b) recovery Procedure	7
1.6	Secured Watermarking method	10
3.1	BEMD founded watermark (i) Embedding and (ii) Recovery Procedure	26
3.2	The standard input image of (i) Baboon (ii) Lena (iii) Cameraman (iv) Barbara (v) Man (vi) Tank (vii) the watermark image	27
3.3	PSNR Value at numerous gain coefficients as represented on a graph	30
3.4	PSNR Value for different Images	31
4.1	BEMD using watermark (i) Embedding and (ii) Recovery Process	41
4.2	PSNR value using various gain factors	48
4.3	Graph for comparing PSNR values	48
4.4	PSNR value at various NC values	49
4.5	PSNR values	49
5.1	Arnold transformation-based watermark (i)encoding process (ii) recovery process	57-58
5.2	The input image of (i) Barbara (ii) Baboon (iii) Cameraman (iv) Lena (v) Boat (vi) the watermark image	59
5.3	PSNR value against the unique gain value	63
5.4	Compared PSNR values	64
6.1	Lena's cover image divided into DWT's sub-bands	68

6.2	BEMD based watermark (a) Encoding and (b) Recovery Process	71
6.3	(1) Host image “Lena” (2) Watermarked image (3) Watermark image against “salt and pepper attack” (4) the watermark image against “Gaussian attack” (5) the watermark image against “2° rotation attack” (6) the watermark image against “shearing attack”	73-74
6.4	The host image of (A) “Lena” (B) “Barbara” (C) “Baboon” (D) “Tank” (E) “cameraman” (F) the “watermark image”	74
6.5	PSNR value at distinct gain factor	79
6.6	Comparative analysis of NC	79
6.7	Comparative analysis of PSNR	80
6.8	Pictures (a) Host (b) Watermark (c) Watermarked and (d) Recovered watermark	80-81

LIST OF TABLES

1.1	Resemblance among watermarking and additional comparable privacy approaches	1-2
1.2	Fundamental features and accompanying applications of digital watermarks	3-4
1.3	Types of Attack in watermarking system	5
2.1	An overview of a few known efficient watermarking methods	20-22
3.1	PSNR and NC achieved at several gain value using the proposed technique	28
3.2	The outcomes of the suggested approach with a different gain factor in respect of PSNR and NC values	28
3.3	PSNR and NC readings from the suggested approach at several gain parameters	29
3.4	PSNR values of proposed work compared with other technique	30
4.1	The suggested method resulted in varied gain rates for PSNR and NC measurements	43
4.2	PSNR and NC values obtained using the method provided for different pictures	44
4.3	PSNR and NC values obtained using suggested technique at different attacks	45
4.4	Results of comparing NC values under various attacks	46
4.5	PSNR value under various attacks is compared	47
4.6	PSNR value comparing for the same image	47
4.7	PSNR comparison results for the identical image	47
4.8	The NC value determined from many watermark attacks and watermark recovery	50
4.9	Comparing characteristics existing systems	51
5.1	PSNR, SSIM, NC, NPCR and UACI values at distinct gain factor	59-60

5.2	PSNR, SSIM, NC, NPCR and UACI values at distinct Images	60
5.3	The PSNR and NC acquired against several attacks	60-61
5.4	NC values in comparison to previous methods	61-62
5.5	NC values compared to other techniques	62
5.6	PSNR values in comparison to other methods	62
5.7	Visibility of watermarked images subjectively by applying a certain gain factor	63
5.8	NC value recorded from separate watermark images that have been attacked and extracted images	64-65
6.1	Values of PSNR and NC at various gain factors	75
6.2	PSNR and NC values for distinct input images throughout the watermarking procedure	75
6.3	Values of PSNR and NC acquired using various non-geometric attacks	75-76
6.4	PSNR and NC values acquired from various attacks	76-77
6.5	PSNR and NC values for various bands at various gain factors	77
6.6	NC values are compared at various noise densities	78
6.7	Comparative analysis of PSNR values	78

LIST OF ABBREVIATIONS

LSB	Least Significant Bit
DWT	Discrete Wavelet Transform
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
KLT	Karhunen- Loeve Transform
SVD	Singular Value Decomposition
JND	Just Noticeable Difference
PSNR	Peak Signal to Noise Ratio
MSE	Mean Square Error
NC	Normalized Correlation
SSIM	Structural Similarity Index Measure
NPCR	Number of Changing Pixel Rate
UACI	Unified Averaged Changed Intensity
BEMD	Bi- Empirical Mode Decomposition
PSO	Particle Swarm Optimization
AMBTC	Absolute Moment Block Truncation Coding
ECG	ElectroCardioGram
LWT	Lifting Wavelet Transform
IMF	Intrinsic Mode Function
BER	Bit Error Rate
FNR	False Negative Rate

FPR	False Positive Rate
ABC	Artificial Bee Colony
ECC	Error Correcting Code
BCR	Bit Correcting Code
DPSO	Dynamic Particle Swarm Optimization
GA	Genetic Algorithm
IWT	Integer Wavelet Transform
LZW	Lempel–Ziv–Welch
RSA	Rivest-Shamir-Adleman
FrFT	Fractional Fourier Transform
ATT	Arnold Transform technique
NCST	Non Subsampled Contour let Transform
RDWT	Redundant Discrete Wavelet Transforms
SPIHT	Set Partitioning In Hierarchical Tree
CDMA	Code Division Multiple Access
SS	Spread Sprectrum
BPNN	Back Propagation Neural Network
CNN	Convolutional Neural Network
DFT	Discrete Fourier transforms
DFrFT	Discrete fractional Fourier transform

CHAPTER 1

INTRODUCTION

Digital imaging and communication technologies have recently been used to disseminate and distribute digital information through open networks, offering a critical and efficient method in a variety of applications [1]. Digital health, patent defence, securing data in the cloud and dispersed systems, finger and thumb printing, distance learning, etc., are all included in the system. Sensitive data must still be transmitted, stored, and shared through insecure communication networks, which requires high level of security and privacy [1, 2]. Sensitive data and information can be protected with high levels of secrecy, integrity, availability, and authenticity using watermarking and encryption techniques. Other benefits of potential watermarking systems include proprietary rights, avoiding detaching, safety from tampering, accessible command, not-renunciation, inventory and effective logging, and lowering storage and capacity demands [1, 2].

Table 1.1 lists the distinguishing features between watermarking and other comparable security measures [3, 4]. Watermarking methods are either spatial or transformation domain-specific. The study came to the conclusion that transform-based techniques are more reliable than spatial area watermarking procedures, including LSB, patchwork, correlation-supported, and spread-spectrum. Some potential examples of transform-based approaches include DWT, SVD, DCT, DFT, and KLT [1].

Table 1.1: Resemblance among watermarking and additional comparable privacy approaches

Characteristic	Watermarking	Cryptography	Steganography	Fingerprinting	Digital Signature
Definition	Watermarking is the process of adding a mark to any image, video, or document to protect the data.	Digital data is secured through encryption over a channel, which is accomplished by cryptography.	The data is encrypted using steganography so that only the sender and the intended recipient can decode the encoded message.	The process of fingerprinting involves making a clone of each original piece of data and then making it specific to the user.	A method for validating the integrity of digital data can be done by digital signature.
Objective (s)	For the preservation of copyright, robustness is essential.	Data protection requires robustness.	Capacity is key to private communication.	Patrimony Data is required to protect the data.	Data protection requires content unity.
Secret data and key	A multimedia file contains a watermark.	For the encryption and decryption processes, a secret key is used.	Any digital asset that has a payload can be used to encrypt the message and embed it.	It has a unique identification to protect the data.	It serves to verify the validity of digital documents.
Choosing of source	Limitations on the source image.	Selecting a source is not required.	Any source may be picked because it is cover writing.	Choosing a cover may or may not be required.	Choosing a cover is not required.

Relationship between source and message	There is a connection between the source and the message.	Not any connection between the cover and the message.	Not any connection between the cover and the message.	There is a connection between the cover and the message.	There is a connection between the cover and the message.
Different Attacks	Dynamic, inactive, Imitation, connivance	Edge-Channel attacks, Error investing, Searching attacks	Brute-force attack, digital attack	Trafficking finger and thumb printing	Birthday attack, Fake attack
Variety of communication	One-to-many	One-to-many	One-to-one	One-to-many	One-to-one

The continuation of the work is structured in this way: The fundamentals and types of the digital watermark(s) are given in Section 1.1. Section 1.2 describes two types of watermarking attacks: Authorized action-specific attacks and System attacks. The current application of digital watermarking is discussed in section 1.3. In section 1.4, the basic idea of watermark encoding and recovery procedure is demonstrated. Section 1.5 describes the necessary performance measure of watermarking techniques, and section 1.6 discusses the aim and significant contribution of the work. In the last, the organization of the thesis is discussed in section 1.7.

1.1 Types of The Digital Watermarks

The fundamental properties of watermarks include strength, protection, content payload, visible quality, infirmity, encoding bandwidth, calculating the budget, and important constraints [1, 5]. The fundamental attributes of digital watermarks are shown in Figure 1.1. It also describes which significant applications matches with the fundamental attributes of the watermark. Table 1.2 provides a brief summary of the key features and associated applications of digital watermarks.

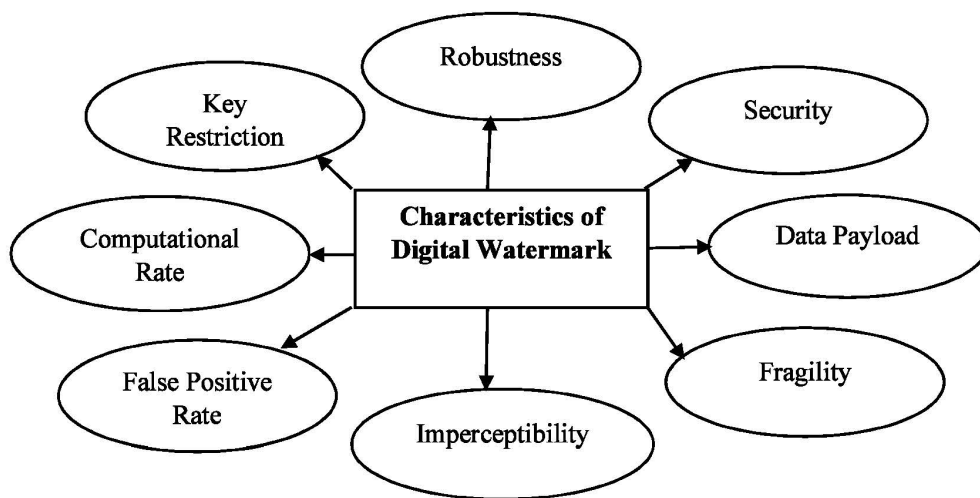


Figure 1.1: Features of digital watermarks [5]

Watermarks may be employed in people or application-specific areas, as well as in many multimedia file types [7]. The watermark may be utilized in both the frequency as well as spatial domains. Frequency domain watermarking surpasses spatial domain in terms of robustness. Image, video, text, and audio files belong to the types of digital documents that are frequently watermarked. According to human understanding, there are two different forms of classification: visible and non-visible. Therefore, the various components of visible watermarks are both strong and vulnerable. Strong watermarking is further divided into public and private watermarks. Public watermarks are typically not protected, while private watermarks are safe and may only be obtained using a special key. For the purpose of developing more effective watermarking systems, feasible researchers are combining strong as well as weak watermarks on a single input media. Application-based watermarking is divided into categories based on source and destination.

Authentication is the goal of source-based watermarking. However, in the instance of unauthorized resale, the customer's location is determined using destination-based watermarking. A comprehensive explanation of all available watermarking methods is found in [7]. Moreover, various watermarks for compressed data are defined in [8].

Table 1.2: Fundamental features [1, 6] and accompanying applications of digital watermark

Basic Characteristics	Definition	Applications
Robustness	Extracting embedded data from attacks. Ensure that copyrights are protected.	Copyright protection, Forensic applications, Digital image processing, graphics, telemedicine etc.
Security	Without damaging the cover image, the watermark should be difficult to change or remove.	Telemedicine, Military, Multimedia, Digital imaging, Computer chip hardware etc.
Data Payload	The amount of information a watermark may hold depending on its entire data payload.	Video, Network based Communication, Digital Imaging Computer Chip Hardware etc,
Imperceptibility	It displays the image's visual quality following the watermark's insertion.	Digital Imaging, Telemedicine, Digital Documents, claim of ownership, Network patrolling, Meta level etc.
Fragility	Pay attention to content authentication.	E- governance, Law enforcement, Digital Signal, Defense,

		Commerce, Journalism, Telemedicine etc.
Capacity	The term “capacity” refers to the simultaneous embedding of numerous watermarks in a document.	Tele-medicine, Secure media distortion, thumbnail embedding for authentication, auxiliary data embedding etc.

1.2 Watermarking Attacks

An understanding of watermarking mechanisms is required to classify watermarking threats. A successful attack is one that exceeds the acceptable limitations of watermark distortion while preserving the visible quality of the attacked data. It can essentially be classified into two categories such as intentional and accidental attacks. In the first type, malicious attackers make an effort to prevent the watermark(s) from serving their goals, as in the case of geometric, cryptographic, and protocol attacks. The next category includes signal processing attacks, where the attacker has no malicious purpose behind blocking the watermark's operational capability. Whereas exploiting watermarks' vulnerabilities results in unlawful activities, such as targeted attacks.

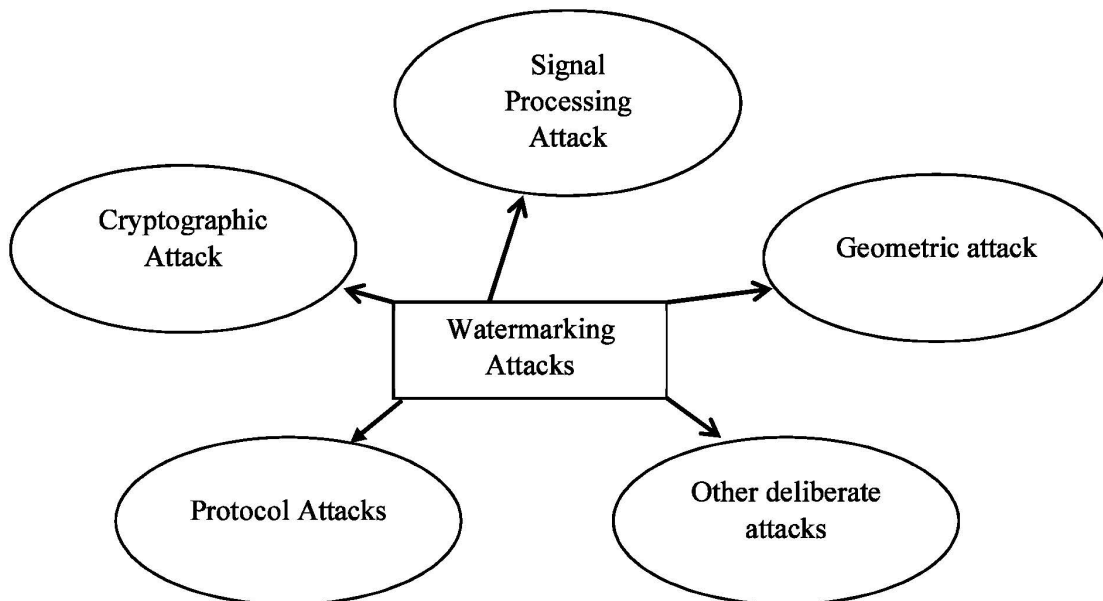


Figure 1.2: Key Watermark attacks

Figure 1.2 depicts a categorization of watermarking attacks [9]. In addition, table 1.3 describes several important attacks, description and their examples. These attacks like signal processing attack, cryptographic attack, protocol attack, and geometric attacks highlight the various strategies applied by adversaries to compromise the security and robustness of the images.

Table 1.3 Types of Attack in Watermarking System

S.No.	Type of attacks	Description	Important example
1.	Signal Processing Attack	They can be classified as unintended attacks because they weren't intended.	Filtering, JPEG compression
2.	Cryptographic Attacks	This type of attack disables the defence mechanisms from defending the watermark. Because of their higher operating costs, they are used less frequently.	Key and algorithm attack, Ciphertext-only attack, Chosen plaintext attack, Brute force attack
3.	Protocol Attacks	Instead of altering or removing the watermark, the main goal of these attacks is to obtain an indication of it. The attacker then claims ownership of the cover and watermarked image as a result.	Session Attack, copy attack, DDoS attack
4.	Geometric Attacks	These attacks aim to visibly degrade digital information rather than eliminate secret data.	Shearing, random bending attack, Cropping, affine transformations, Projections
5.	Other deliberate attacks	These are attacks that are intended to compromise the integrity of ownership data.	Forgery attack, Re-watermarking, Printing attack

1.3 Current Applications of digital watermarking

Technologies for watermarking are being used in literature. Some of the important applications like Hardware and microchip level security, intellectual property infringement, voting

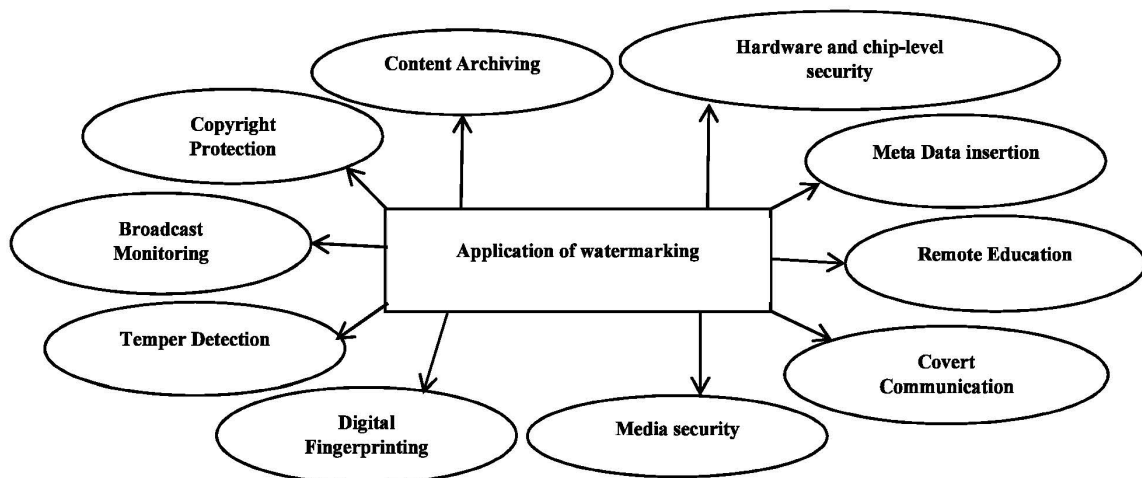


Figure 1.3: Applications of watermarking

machine, sound/display, automation, multimedia cyber security in smart areas, remote training, digital forensics, defence, and media surveillance are covered in figure.1.3 [1, 2].

1.4 Watermark Encoding and Recovery Procedure

Spatial domain and Frequency domain watermarking techniques are shown in Figure 1.4. Spatial domain watermarking techniques such as patchwork, co-relation, spread spectrum etc. embed a hidden signal directly into the pixel values of a host image, making it simple but potentially less robust to attacks.

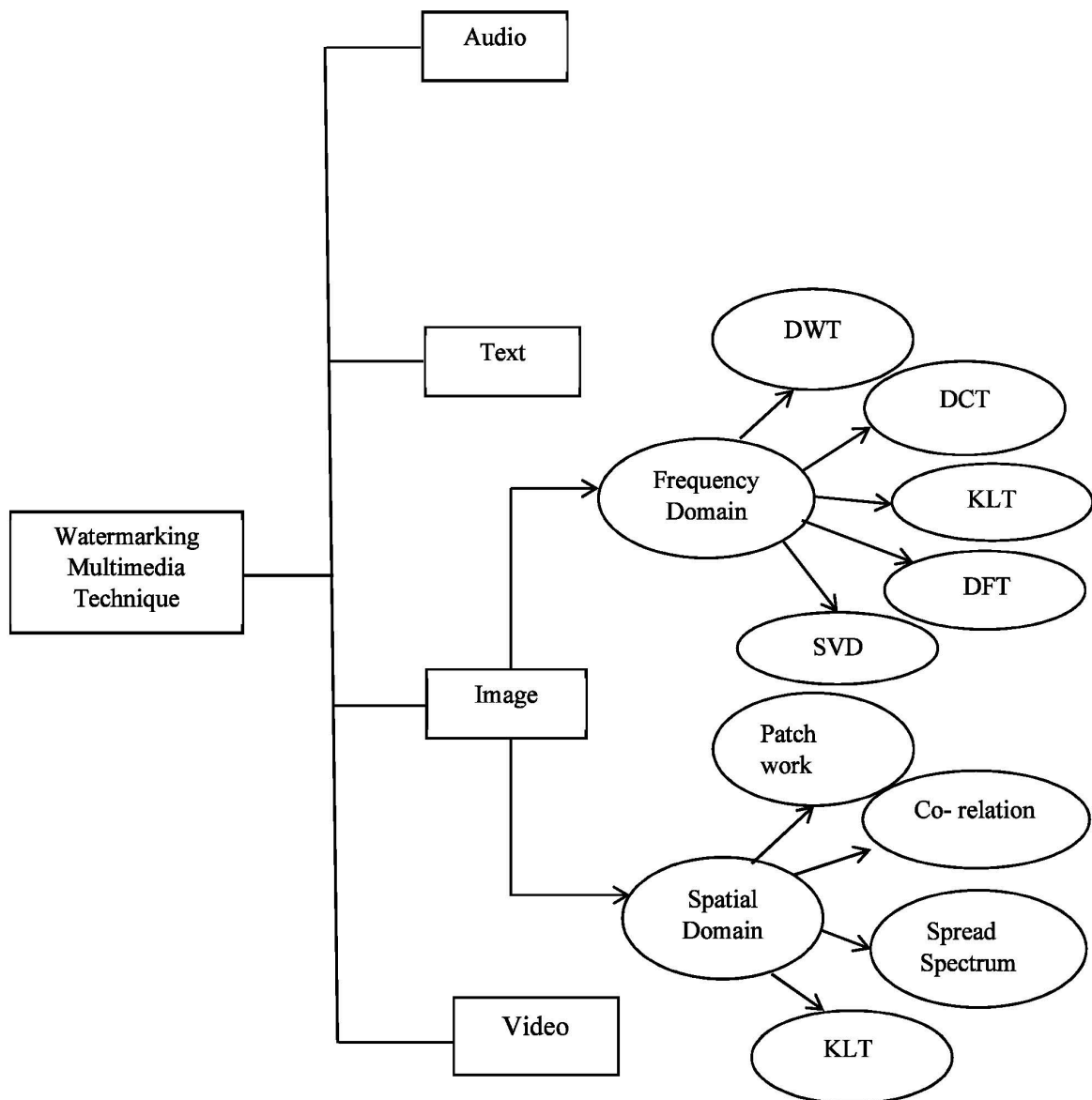


Figure 1.4: Frequency domain and spatial domain watermarking technique

Frequency domain watermarking transforms the host image into a frequency representation using techniques like DCT, DWT, SVD or DFT and then embeds the watermark into specific frequency coefficients, offering greater resilience to common image processing operations. The choice between them depends on factors like security, robustness, and the visual quality of the watermarked image.

The encoding and extracting of the watermark are depicted in Figure 1.5(a-b). The functionalities of the input, watermark, and additional security key are used in the watermark encoding procedure. The watermarked image is the result of the embedding procedure. The watermark recovery method relies on the watermarked image or input information, an additional secret key, and on the test information, each of which has a specific role in the process. Many researchers nowadays frequently utilize both objective and subjective analysis methods to assess the effectiveness of any watermarking technology. The accurate value is based on the mathematical evaluation that represents the transparency of the digital image and is evaluated through objective evaluation techniques, including Just Noticeable Difference (JND), Structural Similarity Index Measure (SSIM), and Peak Signal to Noise Ratio (PSNR)[4].

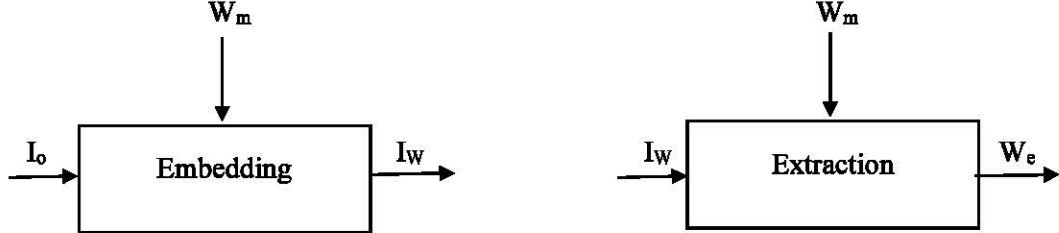


Figure 1.5: Watermarking (a) Encoding Process (b) Recovery Procedure

The encoding takes two inputs, such as a cover image (I_o) and a watermark (W_m). The result of the function $E(I_o, W_m)$ produces the watermarked image (I_w).

$$I_w = E(I_o, W_m) \quad (1.1)$$

Likewise, the decoding takes the test image (W_m) and original image (I_w) as input and produces the output in the form of a recovered watermark (W_e). Therefore, the result of the function $E(W_m, I_w)$ is obtained in the form of the extracted watermark (s).

$$W_e = E(W_m, I_w) \quad (1.2)$$

1.5 Performance Measures for digital watermarking

There are various parameters for calculating the performance of digital watermarking procedures. A few key metrics are explained as follows:

Peak Signal-to-Noise Ratio (PSNR) and Normalized Cross-Correlation (NC) are commonly used metrics in the field of image processing to evaluate the quality, robustness, and imperceptibility of image transformations. However, it is important to note that the choice of metrics depends on the specific goals and characteristics of the task at hand. PSNR is a metric that measures the quality of a reconstructed image by comparing it to the original image. It is widely used in image compression, restoration, and watermarking applications. On the other hand, Normalized Cross-Correlation is used to assess the similarity between two images. In image processing, it is often employed to evaluate the similarity between the original and transformed images.

i. Peak Signal to noise ratio (PSNR)

The peak signal-to-noise ratio (in dB) is calculated between two inputs. This proportion is employed to compare the characteristics of unique and watermarked images [10]. This watermarking method is suitable with PSNR values up to 28 dB. Hence, a higher PSNR value denotes higher imperceptibility or similarity to the cover image.

$$PSNR(P, Q) = 10 \times \log_{10} \frac{(255)^2}{MSE(P, Q)} \quad (1.3)$$

The mean square error (MSE) is measured as

$$MSE(P, Q) = \frac{1}{XY} \sum_{k=1}^X \sum_{l=1}^Y (P_{kl} - Q_{kl})^2 \quad (1.4)$$

Where (P, Q) = examined images, X×Y = Dimension of the source image / watermarked image.

ii. Normalized correlation (NC)

The similarity between the recoverable watermark image and the unique watermark is determined using the Normalized correlation (NC). Therefore, the range of NC value is 0 to 1, and it ought to be 1, preferably. NC levels of 0.7 are regarded as acceptable [10]. It is described as:

$$NC = \frac{\sum_{n=0}^{N-1} x(n)y(n)}{\sqrt{\sum_{n=0}^{N-1} x^2(n) \cdot \sum_{n=0}^{N-1} y^2(n)}} \quad (1.5)$$

Where x=original watermark pixel and y=extracted watermark pixel.

iii. Structural similarity index measure (SSIM)

It is one of the new performance measures that allow the comparison of two images' visual quality. The range of SSIM values is -1 to +1, where 1 indicates that the watermarked image and source image are identical [11, 12].

$$SSIM(i, j) = p(i, j) q(i, j) r(i, j) \quad (1.6)$$

$$p(i, j) = \frac{2\mu_i \mu_j + CT_1}{\mu_i^2 + \mu_j^2 + CT_1} \quad (1.7)$$

$$q(i, j) = \frac{2\sigma_i \sigma_j + C_2}{\sigma_i^2 + \sigma_j^2 + CT_2} \quad (1.8)$$

$$r(i, j) = \frac{\sigma_{ij} + CT_3}{\sigma_i \sigma_j + CT_3} \quad (1.9)$$

The terms "luminance," discrepancy, and "structure comparing tasks" refer to the variables $p(i, j)$, $q(i, j)$, and $r(i, j)$, respectively. Moreover, the constants CT_1 , CT_2 , and CT_3 have positive values.

iv. Number of changing pixel rate (NPCR) and Unified Averaged Changed Intensity (UACI)

It is employed to measure robustness against differential attacks of image encryption techniques/cyphers.

Consider the symbols "C1" and "C2" to be two cypher text images.

$$NPCR = \frac{\sum_{i=1}^M \sum_{j=1}^N D(i, j) \times 100\%}{M \times N} \quad (1.10)$$

$D(i, j)$ defined as

$$D(i, j) = \begin{cases} 0, & \text{if } C1 = C2 \\ 1, & \text{if } C1 \neq C2 \end{cases} \quad (1.11)$$

$$UACI = \frac{\sum_{i=1}^N \sum_{j=1}^M (C1(i, j) - C2(i, j))}{255 \times M \times N} \times 100\% \quad (1.12)$$

Where M and N are the height and width, respectively, for the image.

1.6 Significant contribution of the work

The primary assessment methods for watermarking technologies includes robustness, imperceptibility, bandwidth, privacy, and computation time. With any given watermarking algorithm, it can be challenging to keep these assessments balancing method. Secured watermarking solutions can be accomplished using encryption, chaotic logistic map(s), hashing, frequency spectrum, fingerprinting, identification, Hessenberg matrices, digitized signing, and so forth, as explained in subsection 1.1. Secure watermarking methods involve embedding hidden information into digital media in a way that ensures the watermark's robustness to various attacks and distortions. These techniques often employ cryptographic principles, robust embedding schemes, and advanced algorithms to protect the integrity and authenticity of the embedded watermark, making it challenging for unauthorized users to alter or remove it without the appropriate decryption keys. Some of these techniques are shown in Figure 1.6.

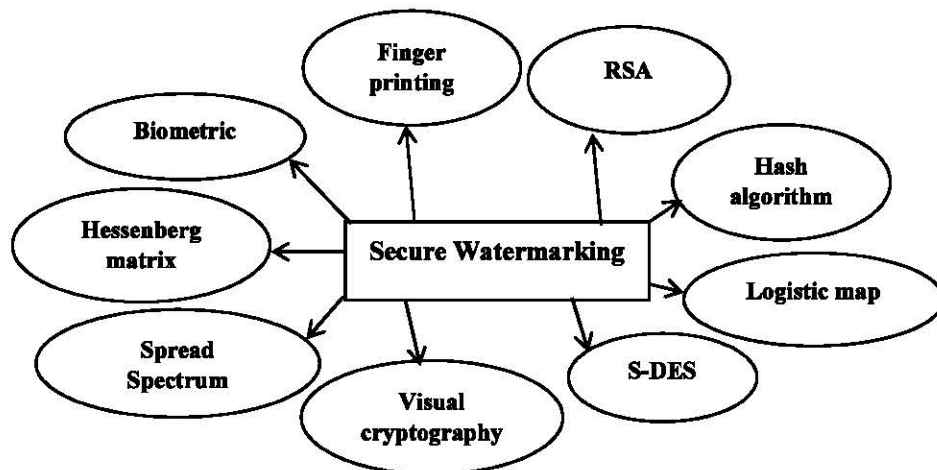


Figure 1.6: Secured Watermarking method [9]

In the context of some interesting challenges presented, this study aims to propose secure watermarking solutions for protecting and preserving multimedia data.

1.7 Thesis organization

This thesis is divided into seven chapters: The fundamentals of embedding and extracting watermarks, contemporary applications, important evaluation indicators, and all of the important watermarking attacks along with the novel properties of digital watermarks discussed in Chapter 1. A literature review of existing watermarking techniques in spatial and frequency

domains is discussed in Chapter 2. BEMD as well as Discrete Cosine Domain watermarking techniques based on PSO described in Chapter 3. A strong and undetectable image watermarking method established with SVD, DCT, BEMD, and PSO in the wavelet domain is covered in Chapter 4. Chapter 5 suggested secured watermarking scheme established with the Arnold transform, SVD, and BEMD in the wavelet domain. A Robust Image Watermarking Using Bi-empirical Mode Decomposition and Discrete Wavelet Domain is presented in Chapter 6. Finally, Chapter 7 discusses with conclusion and future work.

CHAPTER 2

STUDY OF LITERATURE

In this chapter, the different existing watermarking methods have been discussed. Section 2.1 provides a summary of the digital watermarking methods. The classification of watermarking techniques according to several criteria, along with the techniques associated with each classification. It also offers the reasoning behind the chosen classification for the watermarking scheme. Section 2.1.1 presents the watermarking techniques in the spatial domain, and section 2.1.2 presents the transform domain-based watermarking techniques. Section 2.2 describes the existing BEMD techniques using different transform techniques and section 2.3 presents robust hybrid technique. Section 2.4 provides literature optimization of the digital data using PSO. In section 2.5, the encryption using Arnold transform-based literature has been presented in brief. Research Gap have been discussed in section 2.6. Section 2.7 focuses on the research objective of the work. Finally, section 2.8 summarizes the research methodology used in this work.

2.1 Digital Image Watermarking

The distribution of digital data has become more efficient as a result of the networked multimedia systems exponential growth. This has made it simpler to distribute unauthorized copies without losing the quality of the original data. Hence, when information is exchanged over the internet, the owner's authentication as well as the data must be provided to stop unauthorized dissemination. Digital watermarking was developed for this reason which is the type of copyright that is put in a noise-tolerant signal like image, audio, and video files and used to make a statement about the image. Digital watermarking techniques are categorized into two groups based on their performance: imperceptibility and robust. The spatial domain and frequency domain are the two kinds of embedding techniques used in image watermarking. Both approaches need a relatively small amount of computational resources and are easy to implement. Spatial domain watermarking is inferior to transform domain watermarking in terms of robustness [13]. Watermark information could be introduced to the wavelet domain of the input image using a discrete cosine transform (DCT). In order to increase robustness, a novel transform range method, for example, bi-dimensional empirical mode decomposition (BEMD) is advised for image watermarking.

2.1.1 Spatial domain-based watermarking system

In [14], Blind watermark data can be integrated into the spatial domain of the input image. This technique separates the binary watermark into 4 smaller watermarks. The embedding process incorporates the blue portion of an RGB color image into the sub-watermark. Furthermore, the watermark is blindly recovered using key-based quantization. The findings showed that this technique is secure and robust under several attacks. Moreover, this strategy yields more acceptable outcomes than different comparable methods [15, 16]. Watermarking methods are either spatial or transformation domain-specific. This research concluded that transform-based techniques are more robust than spatial area watermarking approaches, including LSB, patch task, correlation-founded, and broad spectrum. Some potential examples of transform-based approaches include DWT, SVD, DCT, DFT as well as KLT [1]. In [17], a lossy compression watermarking methodology was presented. In this method, using AMBTC compression technique, the cover image is divided into three distinct blocks. Then, include the watermark into these blocks employing a number of methods. The method's payload, HPSNR, and MSSIM values are higher than other approaches [18, 19, 20, 21]. The author developed a medical industries Internet - of - things monitoring platform that protects patient information and identity using watermarking in [22]. The DWT-SVD technique is used to introduce the watermark into the Electrocardiogram. This techniques evaluation demonstrates that it is invisible and robust against various attacks. Moreover, the technique is also stronger and more invisible than DWT-DCT methods [23].

2.1.2 Frequency domain-based watermarking system

In view of robustness and improved visual quality, frequency region watermarking is better than spatial area watermarking [24]. Employing discrete wavelet transforms (DWT) or discrete cosine transforms (DCT), using the aforementioned frequency region in the frequency zone of the source image, watermark analytics could be generated. Algebraic properties are frequently recovered from an image using the statistical approach of singular value decomposition (SVD). Combining DWT-SVD-DCT-based watermarking has been recommended in [25] to improve strength with better visual transparency and poor inclusion ratio. DWT, DCT, SVD, and BEMD using frequency-based transform techniques are discussed in the literature review.

2.2 BEMD-based watermarking system

Abbas et al. [27] provide lifting wavelet transformation (LWT) for the accomplishment of copyright protection with watermarking using bi-empirical mode decomposition (BEMD). The LWT boosts both the velocity as well as the computational complexity of the recoverable watermark. The BEMD transformation was implemented to split the image into a variety of periodicity bands. Thus, LWT, as well as BEMD, are used to deconstruct input images into the uppermost strength and lowest susceptible frequency groups for the purpose of maintaining the integrity of the recovered watermark. According to observational findings, visual characteristics would be preserved, and this technique would be sufficiently strong under statistical and non-statistical attacks. The author advocated watermarking images by employing a BEMD approach. During the embedding process, the source image is divided into n sub-images, generating a set of 2D IMFs. Additionally, the extraction method makes use of the assembling approach, local lined configuration, and affine uniformity. Experimental results demonstrate that this method exhibits both high robustness and effective imperceptibility.

A digitized image watermarking method using BEMD was developed in [28]. The first four intrinsic mode functions (IMFs) of the BEMD are taken into account for the binary matrix throughout the embedding phase. Moreover, BEMD is more effective than other methods, such as Fourier and wavelet, as regards obtaining an intrinsic factor. The BEMD methodology is used by the authors to propose a robust watermarking method [29, 30, 31, 32, 33]. BEMD is employed to divide the images and provide accurate frequency coefficients. To achieve better results, fusion quality matrices and other transform techniques are computed for the performance evaluation.

2.3 Robust Hybrid Watermarking System

Hybrid watermarking techniques are those that uses more than one transform throughout the watermarking process. In a hybrid watermarking system, a watermarking algorithm in the encrypted domain was proposed by Guo et al. [34]. Before the embedding process, the algorithm encrypts the cover image using a homomorphic cryptosystem. The chosen sub-region of the DWT input image is then subjected to DCT. The hidden watermark is recovered using a method that is robust to attacks.

The BER result demonstrates that the technique is superior to [35] in terms of measuring channel noise distortion. However, the performance balance between BER and PSNR is poor. A combined compression and watermarking technique for medical applications was offered by Haddad et al. [36]. The algorithm combines the JPEG-LS compression technique with bit substitution watermarking modulation. The proposed approach is examined for several medical ultrasound images. When embedding capacity is excellent, the PSNR value is attractive. Moreover, use lossless compression to reduce the complexity and identify the tempered area. Results from the technique are superior to those from [37, 38].

In [39], the SVD-based watermarking technique and contourlet transform are proposed. According to this method, a watermark is the patient detail(s) encrypted within a 2D rapid response (QR) code. The modified cover image is also incorporating the scrambled encoded watermark. The performance demonstrates the improvements in security as well as strength. Experiment outcomes showed that the offered technique achieved previous similar documented techniques in respect of security, adaptability, and complexity [40, 41, 42, 43]. A secure method for watermarking colored images by visible cryptography and adjustable sequence dithering in the wavelet domain is described in [44]. According to experimental findings, when the watermark is incorporated, there is no noticeable dissimilarity between the input image and the input image after the watermark making the approach robust to many forms of attacks. Secret sharing and wavelet transform also provide more security against multiple attacks than other techniques currently in use [45]. It was suggested to employ a logistic mapping through a Hamming code-using image watermarking system by [46]. The watermark encoding technique is blocked, autonomous and resistant to vector quantization (VQ) attacks. Compared to other similarly described techniques, the strategy yields excellent outcomes in terms of false negative rate (FNR) and false positive rate (FPR) aspects [47, 48].

A secure and fragile watermarking technique was introduced by Rawat and Raman [49] using a chaotic map. Originally, The host image is transformed by the Arnold algorithm and then a binary chaotic watermark is added to the transformed image. Execution measure is evaluated against various attacks. A safe watermark-based approach for cloud applications was developed by Xia et al. [49]. Here, the cover image is utilised to hide private data. The authors considered two main security challenges, with the first being the problem of data privacy and the second being the issue of copyright. The security of the method is examined against various attack models. Moreover, the watermark-based approach preserves copyright protection and

provides superior outcomes [51]. Su and Chen proposed a Hessenberg transform-based blind colour image watermarking [52]. Arnold and the hash pseudo-random technique offer security and robustness, respectively. The scrambled color watermark is encoded via a quantization system into the Hessenberg matrix's biggest energy element. This method takes less time to embed and retrieve data than other methods currently in use [53, 54, 55, 56]. The use of watermarking for content authentication and copyright protection was first described in [60]. An effective way of data hiding is provided by the methodology, which combines the wavelet transform, chaotic method as well as artificial bee colony (ABC) algorithm.

In [61], a secure semi-blind watermarking method based on elliptical curve cryptography (ECC) is proposed. The outcomes were contrasted with the author's previous findings, which was published in [62, 63, 69] and were discovered to be better with respect of PSNR, SSIM, and bit correction rate (BCR). In addition, the author claims that ECC is a faster encryption technique than two other well-known ones. Patra et al. presented copyright protection watermarking technology with the DCT domain [65]. Chinese remainder theorem also provides evidence of the authenticity of the algorithm (CRT). According to the authors' findings, the CRT-DCT-based method offers better protection against potential attacks and faster embedding and extraction of the watermark than the CRT-SVD method [66, 67].

2.4 Optimization-based watermarking system

An image classification method that uses SVM-PSO to derive the properties of persistent rotational image patterns from the SVD as well as DWT domains is observed in [68]. SVD is employed to improve image structure. According to Saxena et al. [69], watermarking for color images should be done by integrating the watermark into the input image using DWT, dynamic PSO, and SVD. Toward giving the necessary variation as well as a great likelihood of recovering from enlargement, active PSO (DPSO) is utilized. When the execution of DWT-SVD and DPSO is evaluated with that of other PSO versions, it is clear that it is better than other all-encompassing approaches.

In [70] provided an IWT, standardized SVD, Genetic algorithm (GA), and PSO for image watermarking. In addition, the proposed method improves robustness as well as imperceptibility compared to other attacks. In addition, normalization is employed to determine the invariant characteristic, and the invariant characteristic that is discovered are then focused on the IWT and NSVD. The results of this technology show that it offers a higher level of robustness against different attacks and is superior to conventional ways. In [71], the author

discussed SVD and ageing leader-founded PSO as a successful image watermarking method. Moreover, ageing leader-founded PSO, as well as SVD, are employed to speed up and increase the security of watermarking then the Arnold transform is employed to scramble the watermark to enhance security. Furthermore, this proposed approach is contrasted with current techniques based on mean rotational distortion, relative MSE, PSNR, core MSE, and standardized cross-correlation.

In [72], the author proposed a dual-encoded watermarking technique combining SVD-DCT-DWT as well as PSO. As a result, the watermark is encoded using the Arnold transformation, and both the minor frequency and upper-frequency regions of input images are significant. PSO is also used to increase the embedding aspect matrix. Hence, the outcomes of this method demonstrate great bandwidth, high strength, and visible impact with respect to the majority of attacks. Such method for lossless image compression using PSO optimization, DWT, LZW compression, RSA encryption, as well as DWT is discussed in [73]. As a result, Pseudo-random sequence & series and RSA encryption are both utilized for encoding the estimation and precise sub-bands, respectively. Moreover, explained sub-bands already have fewer data. PSO algorithm optimization results in good compression performance.

In [74], DWT and PSO using watermarking method optimization are presented. In order to insert the data, a low-frequency area is employed. The encoding and decoding processes are utilized to enhance gbest and pbest and produce the most effective outcomes. The experimental results designate that there is very little disparity between the source and watermarked image. In [75], in this hybrid domain, an invisible and strong image watermarking approach founded on fusing logistic maps as well as PSO is offered. First, the input image is divided by DWT and the insensitive LH as well as HL sub-bands is subjected to DCT using a human visual model. With the DCT, an ideal frequency spectrum is selected to increase the watermark's transparency and robustness. Moreover, PSO is employed in multi-dimensional optimization to choose the best DCT coefficients. Security is provided by an interconnected logistical network. The results of this method demonstrate its great imperceptibility and good robustness.

2.5 Arnold-based watermarking system

In [76], the authors explain digital image watermarking founded on the Arnold map employing DCT, SVD, and DWT. Therefore, DCT and SVD in the wavelet domain are utilized for improved robustness as well as imperceptibility. Much memory space is preserved by this method. A strong image watermarking method utilizing SVD, DWT, as well as Arnold map is

addressed in [77]. SVD, along with Arnold's map of the method, can thus preserve security and copyright protection, respectively. The outcome demonstrates that the suggested procedure can produce images of good quality. Author [78] establishes a successful chaotic image encryption method using a generalized Arnold map. This paper describes this method as consisting of the two phases of substitution and distribution. In the substitution step, conventional frequent position substitution is used. A huge key space and high key sensitivity make this area of the section persistent and effective encryption.

In [79], on the basis of SVD and the Arnold transform, a fractional domain image encoding technique is suggested. In this study, an original image is transformed using FrFT into a fractional domain and divided into three portions using SVD. Moreover, the Arnold transform secures all three of these portions. In [80], it offers a digital watermarking method that makes use of the DWT, DCT, SVD, and Arnold transforms. Therefore, the watermark is made more secure by using the Arnold transform. Additionally, the image may be colored, and the suggested technique may be applied to tapes. The study's findings demonstrated strong robustness and maximum security levels.

In [81], the use of SPIHT in the wavelet domain for image watermarking is discussed. High-energy compaction properties use DCT and SVD. As a result, the Arnold transform is used for improved confidentiality, while SPHIT is a method for compressing bit strings as well as offers precise rate control. In contradiction of multiple attacks, the offered method's output is robust and imperceptible. In order to watermark multiple images, RDWT, NSCT, SPHIT, and SVD are combined [82]. As a result, the NSCT achieves shift variance and increased directionality assets. The SPHIT also achieves compression on the watermark image. The result demonstrates excellent robustness and privacy against various attacks. Author [83] suggests circular embedding using the Arnold transform and BEMD as an increase to blind image watermarking. As a result, to expand the method's security, the watermark image is randomized through the Arnold transform. Moreover, the input image is disintegrated using the BEMD approach to produce the IMFs and residue. The paper's conclusion shows increased robustness and imperceptibility. The paper's conclusion shows increased robustness and imperceptibility.

2.6 Deep Learning based watermarking system

In [84], Author introduces a pioneering approach to digital watermarking by leveraging deep neural networks (DNNs). This method involves constructing a DNN specifically tailored to the

challenges of protecting digital content, particularly images, and training it on a curated set of images. The experimental results on test images not only highlight the potential of this method but also showcase its practicality and efficiency through both subjective and objective assessment.

The proposed neural network-driven digital watermarking solution integrates a DCT- DWT hybrid algorithm, embedding visible and invisible watermarks into an original image is proposed in [85]. Neural networks are then employed in later stages to extract the watermark independently of the original, enhancing security and copyright protection. This comprehensive approach plays a significant role in ensuring secure and efficient digital watermarking. In [86], the author introduces a novel dual watermarking scheme designed to address the dual objectives of image authentication and copyright protection. This method employs the discrete wavelet transform (DWT) to simultaneously embed a fragile watermark and a robust watermark is generated using a specific visual cryptography technique. Moreover, the incorporation of visual cryptography and chaotic transformation enhance security and the blind watermark extraction feature eliminates the need for host image information during extraction, contributing to the scheme's comprehensive and competitive performance.

In [87], the proposed method integrated the Deep Belief Network (DBN) trained by the Bear Smell Search Algorithm (BSSA) in the initial phase. Moreover, the embedding phase leverages a hybrid transform domain involving Discrete Wavelet Transform and Singular Value Decomposition (DWT-SVD). Extraction is executed through a Back Propagation Neural Network (BPNN). The robustness of the proposed DBN-BPNN topology is further demonstrated against a spectrum of attacks, including noises and distortions. Moreover, the experimental results underscore the comprehensive and competitive performance of the proposed watermarking technique.

In [88], the author addresses the issues by first reviewing the utility of digital watermarking technologies in safeguarding the copyright of DNNs. A comparative study of the latest techniques is then presented along with the proposal of several optimizers aimed at enhancing accuracy against fine-tuning attacks. Experiments conducted in black-box settings, employing various optimizers, are compared with the widely used SGD optimizer. DNNs, pervasive across fields like marketing, healthcare and natural language processing, necessitate robust copyright protection. Experiments conducted on MNIST and CIFAR10-CNN datasets underscore the practical insights derived from this comprehensive study.

As computer security advances, a single watermarking technique may fall short, and the potential emergence of anti-watermarking methods adds complexity. This gap in knowledge poses significant challenges for information security engineer and software designers. In [89], author addresses this challenge by proposing two innovative methods that leverage deep learning and shallow learning models based on state-of-the-art watermarking techniques. Various ML algorithms are applied to model watermarked data from diverse spectrum and domains, encompassing speeches, audio, images, and videos. The experimental setup, utilizing Amazon Sagemaker for ML modeling, demonstrates the effectiveness of the proposed methods in resolving ambiguities within a general watermarking process. Despite the focus on novel watermarking methods, the method highlights the underexplored realm of anti-watermarking and watermark-removal methods. Moreover, the results indicate improvements when the original data is utilized in the training process.

Table 2.1 Comparison of various methods

Ref. No.	Objectives	Blind/ Fragile/Non-blind Technique	Achieve Objective through	Results	Important Note	Size of watermark/ Cover watermark
[14]	Robust and Imperceptibility	Blind	DCT	Capacity = 0.0013 bpp	Based on the idea "first to select the optimum sub-watermark from 4 sub-watermarks, then combine the sub-watermarks to the final watermark"	32×32/ 512×512 (both color images)
[15]	Robustness	Blind	DCT, Inter-block correlation	Max PSNR= 41.78 dB,	The lower the Tamper Assessment Function the better is the watermark extraction.	Cover Image= 512× 512 and watermark Image= m×n
[16]	Robustness	Robust/ Fragile	DWT, DCT, Error correction code	Max PSNR= 40.68 dB, Max NC=1	Reduce the error uses error correction code	Original/Water mark image size is converted to 1024×1024.
[17]	Capacity and image quality	Blind	Block truncation coding (BTC), Direct binary search (DBS)	Max Payload= 16380	Two advantage: i) Increase Security ii) Reduced Image size	Image size= 400×400

[18]	Improve hiding Capacity	Robust	Reversible data hiding, Block truncation coding, Histogram shifting, Predictive coding	average accumulated hiding capacities= 3471.167 and 6111.333	The best basic element for the block-based linear interpolation is exploited.	Image size= 512×512
[19]	Improved Payload	NA	Data hiding, AMBTC, Steganography, Payload, Compressed bitstreams	Max PSNR = 34.19 dB Max Payload= 16774	Computation is easy.	Image Size= m×n
[20]	Improved Security	NA	AMBTC Compression Technique	Max capacity= 16384 Max PSNR= 34.50 dB	Goal of AMBTC is to preserve the mean and the first absolute central moment of image blocks.	Image Size= 512× 512
[21]	High Payload, improved image quality	NA	Steganography, Smooth block , Minimum distortion, High payload Absolute moment block truncation coding	PSNR value= 32.67 dB	Low computation complexity Easy to implement	Image Size= 512× 512
[22]	Imperceptibility and robustness	Robust	Internet of Things (IoT), cloud assisted system	PSNR= 64.35 dB SNR= 50.12	Describes a cloud-integrated HealthIoT monitoring framework	Image Size= I× J
[23]	Robustness, improved computational complexity	Robust	DCT	Mean frequency mask= 20.77	Higher bit rate and comparatively costly	Audio watermarking
[24]	Robustness, Imperceptibility, less execution time	Blind	Discrete Hartley Transform (DHT), DCT	Max PSNR= 44.4928, SSIM= 0.9889, NC= 1	Higher real time performance	Watermark Image size= 32×32/ Original Image= 512×512
[25]	Robustness	Robust	DWT, DCT and SVD	Max PSNR= 51.148, CC= 0.9999	It has a flaw positive detection.	Image Size= 512×512
[26]	Improved visual Quality	Robust	LWT and BEMD	Max NC= 1 Max PSNR of watermark image= 60.34	It can resist the high distortion caused by motion blurring.	Watermark size= 256×256/ original Image= 512×512

[27]	Imperceptibility and Robustness	Blind	BEMD	Max PSNR= 42 dB	Limitation is insufficiency against geometric distortion.	Watermark Image= 64×64/ Original Image Size= 512×512
[28]	Robustness	Robust	BEMD	Max NC= 1 PSNR= 39.50 dB	Robust against different attacks.	Image size= 512×512
[30]	Robustness and visibility of image	Robust	BEMD	Shearing Attack by 75%.	Improve the validity of the watermark.	Original Image size= 256×256

Table 2.1 describes the comparison of different methods based on objectives, techniques, achieved objectives, results and size of watermark/ cover watermark. Therefore, various watermarking methods differ in their objectives, with some prioritizing robustness against attacks, others emphasizing invisibility, and some focusing on security.

2.7 Research Gaps

After extensive research review following gaps were found:

- Several transforms are applied in watermarking methods. Most of these methods apply an optimized embedding and extraction factor with a single gain factor value for each Image's pixel block. So, there is a lack of providing a trade-off between robustness and imperceptibility against common watermarking attacks.
- Binary watermark has been employed in almost all watermarking methods. The researchers are still facing significant difficulties in their efforts to embed a color or grey-scale watermark in the image.
- With robust image-adaptive data hiding methods using erasure and error correction, the identification of watermarks is reduced to errors even though side information about the locations where data is hidden is not provided. Many embedding techniques can be used to provide security [26, 29, 72, 96] to the algorithm for the hidden data.

2.8 Research Objectives

This work aims to provide a complete watermarking mechanism to improve robustness, imperceptibility, and security for grey-scale images. Objectives framed are given below:

- To develop a watermarking technique for enhancing robustness and imperceptibility.
- To design a transformation technique for embedding the data in image files.

- To design an efficient watermarking technique for enhancing data security.
- To examine the robustness of the watermarking method using distinct kinds of malicious and non-malicious attacks.

2.9 Research Methodology

In the first method, robust, secure, and transparent watermarking is proposed for grayscale images. In order to do this, it is suggested to use a transform domain using watermarking. The suggested method seamlessly integrates into the host image using BEMD, DCT, and PSO. Moreover, the secret key is used to enhance the privacy of digital information. Both subjective and objective methods are used to establish the method's effectiveness and significance. Additionally, experimental testing suggested that the system is strong and secure to various assaults and it also originates enhanced presentation than former techniques. The next contribution of this thesis is to design a transformation method for encoding the information into image files. The proposed work aims to provide robustness and imperceptibility. However, the PSO is used for optimization to get a better association between visible quality and strength. A comprehensive assessment of this technique has demonstrated that it is more secure, reliable, and imperceptible than other former methods. Further, an improved DWT-SVD and BEMD approach is developed in the next contribution. However, Arnold Transform provides the privacy of the offered methodology. The target of the proposed work is to produce security and imperceptibility.

CHAPTER 3

IMPROVED ROBUSTNESS USING BEMD WITH DISCRETE COSINE TRANSFORM USING PSO

This chapter proposes reliable image watermarking with BEMD (bi-dimensional empirical mode decomposition), DCT (discrete cosine transform), and PSO (particle swarm optimization). During the embedding procedure, the input image is given with DCT coefficient and the watermark image is divided using BEMD decomposition. PSO is utilized for multidimensional and complicated discovery during optimization. A security key is used to embed the scaling and embedding factors. The Inverse DCT and Inverse BEMD go along with such a technique. The image of the watermark is recovered by a recovery method. The proposed results of this algorithm demonstrate how robust the suggested technique is in the presence of various attacks. In comparison to previous methods, the suggested method is potential for the visibility of the watermark image and enhances the imperceptibility.

3.1 Introduction

The embedding and extraction of watermarking using BEMD, DCT as well as PSO is used to improve the robustness and imperceptibility. A discussion of embedding and extraction is shown in section 3.2. To preserve security, visual quality, and authenticity are the several complicated concerns. To protect the integrity and privacy of information from illegitimate approach, it is vital to create robust and secured watermarking techniques. The suggested method may be effective in resolving the complicated challenges of strength, privacy as well and legitimacy for the images. Here, 256×256 Grey-scale watermark image and 512×512 Grey-scale original image are used for the experiment analysis. The estimated PSNR and NC values are calculated to measure the experiment works.

In this chapter, an effective image watermarking approach found on BEMD, PSO as well as DCT is suggested. The following is an outline of the work's primary responsibilities:

- The watermarking image is decomposed using BEMD in order to enhance image quality and generate effective frequency parameters for the input image.
- The original image, as well as the watermark image, is converted using DCT, which increases the visual quality of the algorithm.
- To conduct a dynamical assessment, the BEMD approach identifies inferior and optimal frequency bands and PSO optimization is used to provide a dynamic scale factor matrix.
- In this method, the embedding and extraction of digital content use a cypher key for authentication purposes.

3.2 Watermarking System

This chapter introduces the watermarking technique in which the BEMD, DCT, and PSO have been used to represent the embedding and recovery process of digital watermarking.

3.2.1 Process of Watermarking Embedding and Recovery Procedure

The block diagram of watermark embedding is presented in Figure 3.1. In this demonstrated efficient watermarking system, the input image is decomposed into 512×512 non-imbrication blocks. The composition of BEMD, DCT and PSO is employed to provide imperceptibility and robustness using a digital image. Initially, cover image 'Lena' is divided by the DCT coefficient in the embedding process to obtain the 8×8 block of pixels and watermark mark image 'baboon' is decomposed by BEMD decomposition to get the residue and IMFs of the watermark image. After that, the DCT coefficient and residue of BEMD are used to calculate the embedding factor. Here, PSO is employed to get the optimal solution of the algorithm. Subsequently, the watermark picture is scrambled and encoded into the cover picture. A reverse embedding approach is employed to achieve the watermark recovery. An extracted watermark is obtained via the reverse embedding method.

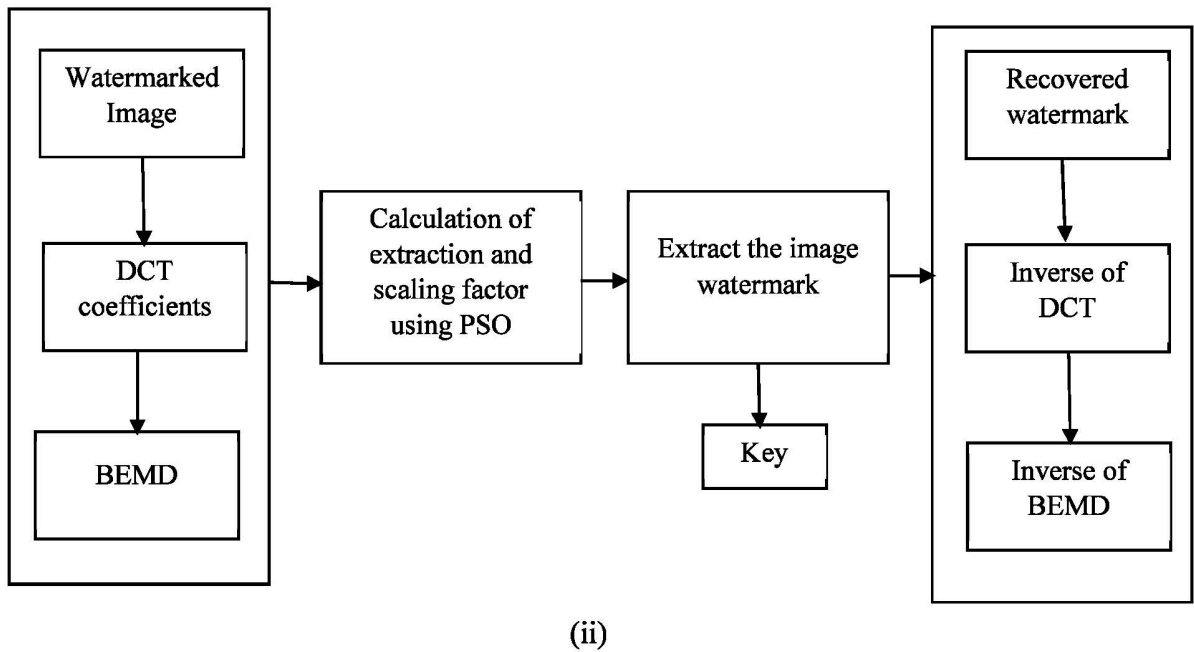
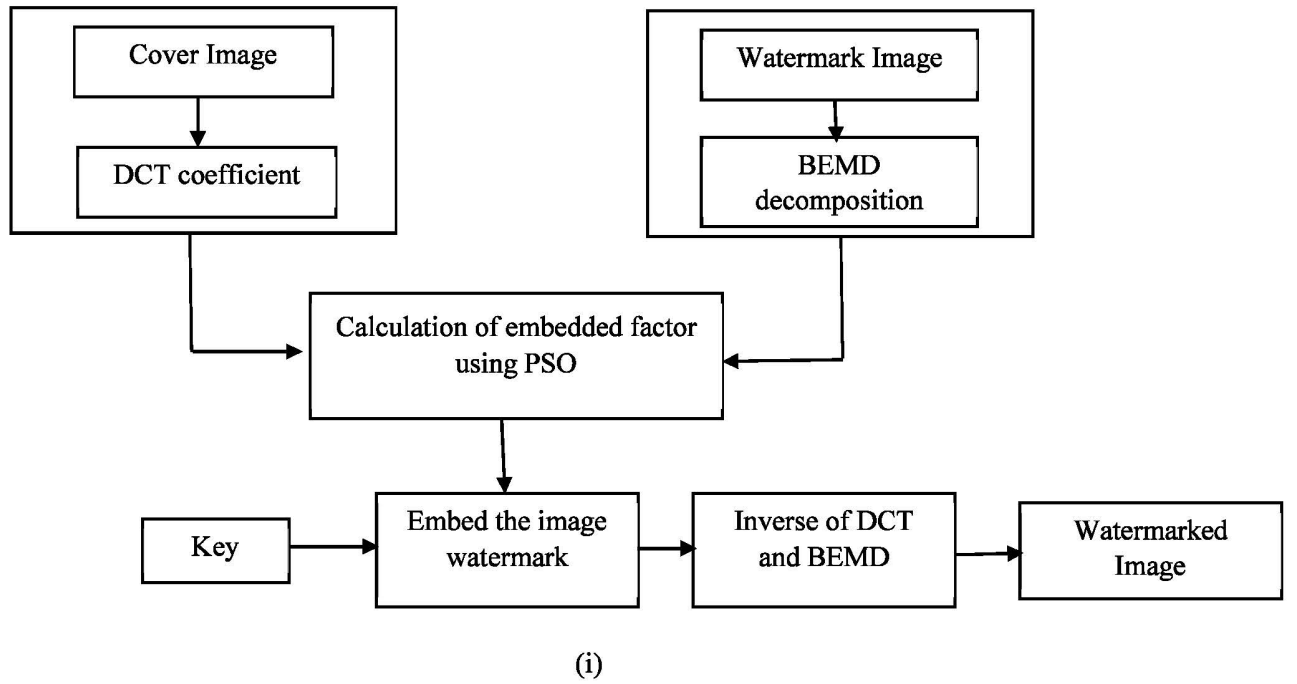


Figure 3.1: BEMD founded watermark (i) Embedding and (ii) Recovery Procedure

3.3 Experimental Results

For experimental results, 256×256 Grey-scale watermark image and 512×512 Grey-scale original image are used for the experiment analysis. The experimental outcome relies on the values of PSNR

as well as NC. Fig.3.1 describes a brief explanation of the embedding and extraction processes. Figure 3.2 demonstrates the standard images of (i) baboon, (ii) Lena, (iii) cameraman, (iv) Barbara, (v) man, (vi) tank, and (vii) baboon as watermarked image.

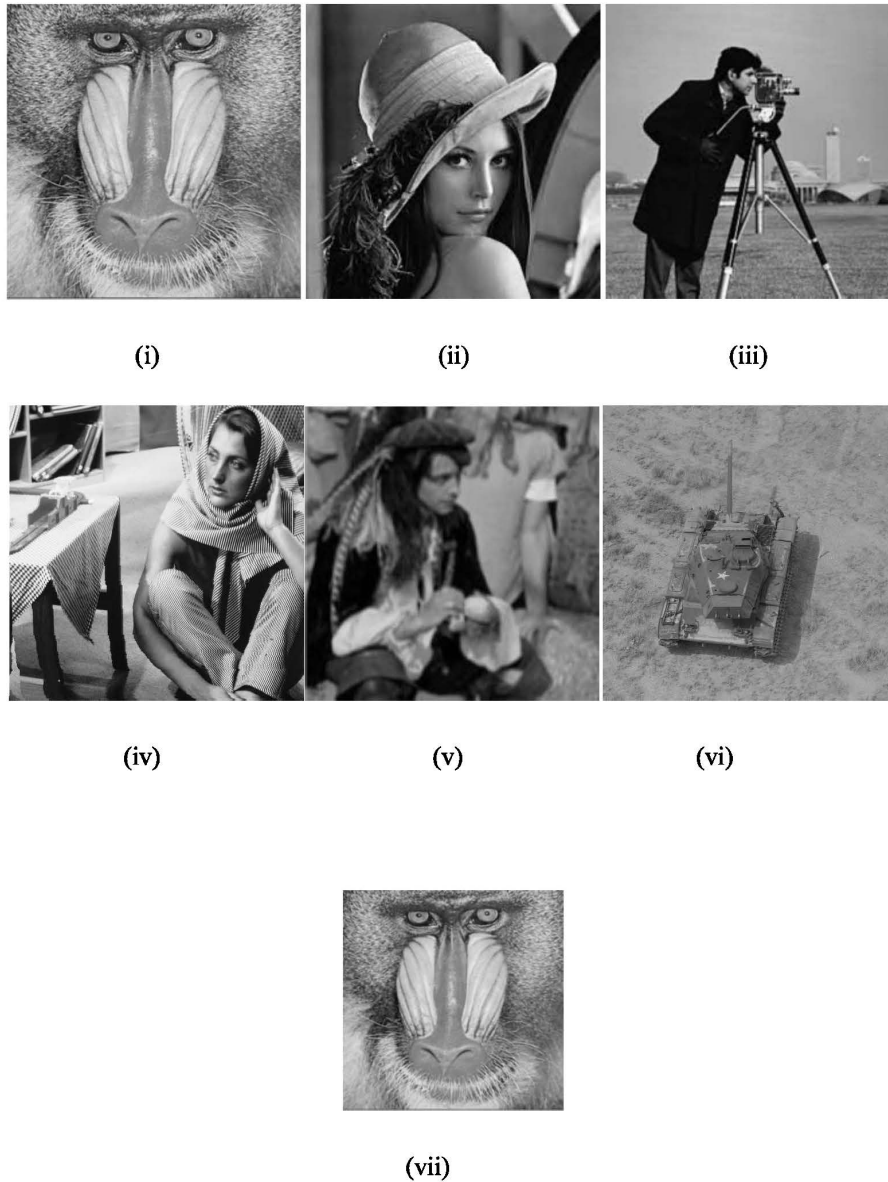


Figure 3.2 The standard input image of (i) Baboon (ii) Lena (iii) Cameraman (iv) Barbara (v) Man (vi) Tank (vii) the watermark image

The performance of the proposed technique is measured using standard measures like PSNR and NC. Chapter 1 presents the fundamentals of the metric under consideration.

Table 3.1: PSNR and NC achieved several gain values using the proposed technique.

Different Gain value	PSNR value	NC value
0.001	49.4254	0.999
0.005	48.4754	0.998
0.01	44.6497	0.997
0.05	43.2497	0.996
0.1	42.7497	0.993

Tables 3.1–3.4 show the results in terms of standard metrics. Table 3.1 demonstrates the PSNR and NC values of our approach at various gains and indicates that the PSNR and NC values are above 42.7497 dB and 0.993, respectively, without several attacks. Table 3.2 displays the PSNR and NC results for several images at gain factor value=0.01. It is evident that the greatest PSNR and NC results are observed as 49.4254 and 0.9998, respectively. However, PSNR and NC values for Barbara's image are less.

Table 3.2: The outcomes of the suggested approach with a different gain factor with respect to PSNR and NC values.

Distinct Image	PSNR (in dB) value	NC value
Baboon	44.6268	0.9997
Barbara	41.7053	0.9993
Cameraman	49.4254	0.9998
Lena	43.1863	0.9996
Man	43.4886	0.9994
Tank	45.3862	0.9998

Thus, the results of PSNR and NC under numerous attacks are displayed in Table 3.3. For salt and pepper at various gain factors of 0.0001, it can be seen that the maximum PSNR and NC values are above 41.291 dB and 0.9898, respectively. However, PSNR, as well as NC values, are poor for Gaussian attack and rotation, respectively.

Table 3.3: PSNR and NC values against different attacks

Dissimilar Attacks	Noise Density	PSNR (in dB)	NC
Salt & Pepper	0.0001	41.2915	0.9894
	0.0005	41.0871	0.9894
	0.01	40.2060	0.9897
	0.1	39.3139	0.9897
	0.5	39.0049	0.9898
Rotation	1°	39.7589	0.9850
	3°	39.2328	0.9861
	5°	39.8937	0.9749
Gaussian Attack	0.0001	40.3916	0.9850
	0.01	40.3963	0.9850
	0.05	39.1709	0.9867
	0.1	38.4890	0.9867
Speckle		39.3916	0.9819

Table 3.4: PSNR values of proposed work compared with other techniques [90]

Various Image	NC	PSNR (in dB) value [90]	PSNR (in dB) value by the offered technique
Lena	0.9996	38.5334	43.1863
Man	0.9994	37.6545	43.4886
Baboon	0.9997	37.5343	44.6268

Table 3.4 represents the better performance of our method as demonstrated by contrasting its outcome in respect of PSNR values with that of the former approach [90]. The highest PSNR result offered by the approach [90] is 44.6268 for a baboon. However, our method maintains the standard value for PSNR (i.e. greater than 28 dB) for all images, including Lena, Man and Baboon.

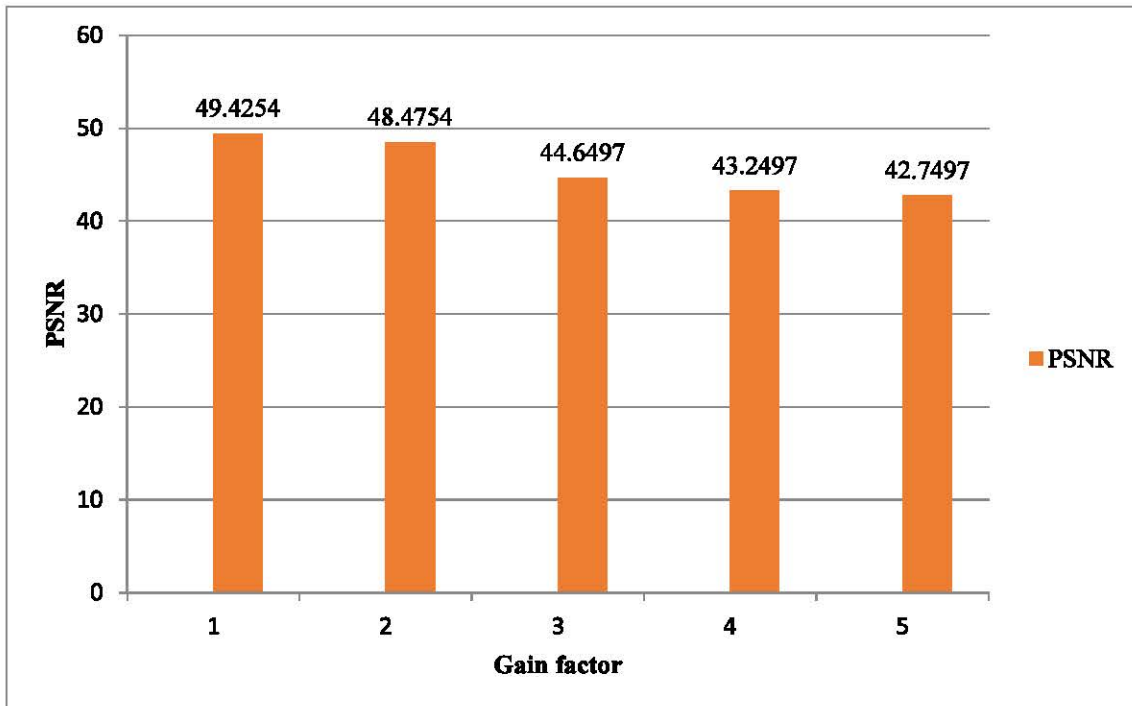


Figure 3.3: PSNR Value at numerous gain coefficients as represented on a graph

It can be noticed from PSNR value that the offered technique provides improved imperceptibility compared to the compared technique [90]. This method offers the highest level of robustness in contrast to the most severe attacks; including speckle, salt and pepper, rotation, and Gaussian noise attacks of the image as well as other widely used operations in processing as per the source of evaluation from the offered technique.

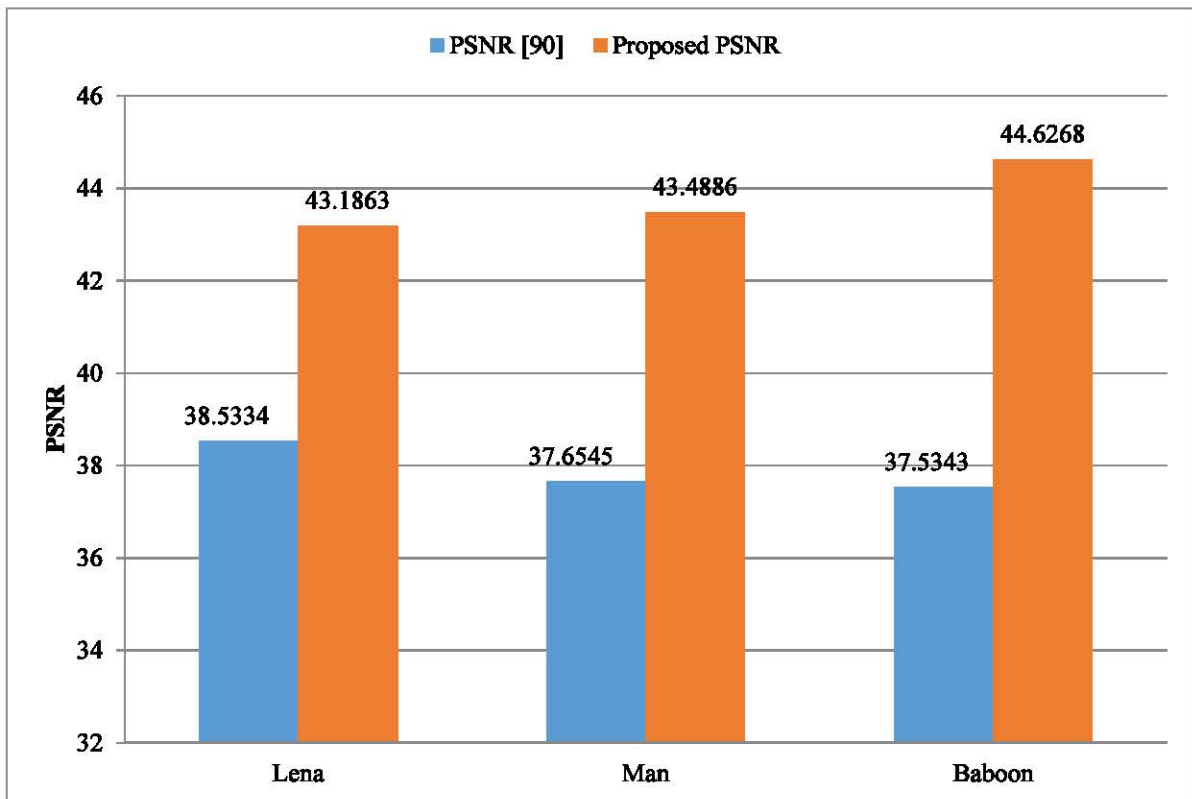


Figure 3.4 PSNR Value for different Images

Figure 3.3 shows a visual depiction of the PSNR values obtained using the DCT-PSO and BEMD methods at various gain factors. Figure 3.4 compares the PSNR values between the proposed method and the currently used method [90].

In this chapter, the embedding and extraction of watermarks using BEMD, PSO, and DCT domains were covered. In this method, the watermarking process was carried out using DCT and BEMD techniques, and PSO optimization was applied to increase robustness. Moreover, the cipher key is utilized to increase the protection of the algorithm using DCT-BEMD and PSO optimization.

Extensive assessment with respect to PSNR and NC confirmed that the technique is robust as well as imperceptible against distinct types of attack. This approach attains a PSNR of 40 dB or higher without the use of any attacks. The results also confirmed that our technique is superior to former schemes.

In addition, how to adapt the proposed framework to solve the robustness and visual quality efficiently for medical images will also be investigated in future work.

L Singh and P. K. Singh, "An Efficient Image Watermarking Through BEMD and Discrete Cosine Domain Based on PSO" *Innovations in Information and Communication Technologies (IICT-2020) Proceedings of International Conference on ICRIHE-2020, Delhi, India: IICT-2020* (pp. 469-474). Springer International Publishing.

CHAPTER 4

IMPROVED ROBUST AND IMPERCEPTIBLE IMAGE WATERMARKING THROUGH BEMD, DCT, SVD USING PSO IN THE WAVELET DOMAIN

In this chapter, an enhanced DWT-SVD- BEMD- PSO using the watermarking system in the wavelet domain is presented. The technique collectively uses DWT, DCT, and PSO to provide robustness and optimization, respectively. The technique employs DWT to deconstruct the input image during the embedding phase of the image. Secondly, DCT is used to convert the chosen DWT component. An image watermark details first decomposed by BEMD and the IMFs and residue after decomposition. Moreover, the DCT coefficient and residue of BEMD are imperceptibly embedded into the SVD decomposition to obtain the singular value matrix. An extraction procedure is executed in reverse order. Digital watermark testing on five different cover images and under several attacks shows that the presented method provides better robustness with less distortion than competing approaches.

4.1 Introduction

Currently, Data processing has made it easier for digitalized data to be distorted and disseminated, which has increased the need for secure ownership of digital facts [10]. However, the major problem is the secured transportation of digital data. The best method for ensuring the ownership and integrity of digital data in this aspect is image watermarking [91]. A method for positioning the tempered area of the host image and for ownership protection is defined by virtual image watermarking. Fragile watermarking allows the manipulation of the image, whereas robust watermarking protects ownership and copyright [92]. The embedding process and the extraction procedure are the two fundamental steps in the watermarking approach. There are two different kinds of embedding methods for image watermarking: spatial region and frequency region. Both applications require a very small number of computation resources and are simple to implement. The spatial watermarking is inferior to the frequency region in positions of good visual quality and robustness [24]. It has been suggested to use DWT-SVD-DCT oriented watermarking to increase

strength with higher perceptive clarity and poor insertion proportion [25]. Moreover, fragmentation of the DWT results in four transmissions of the DWT transform, referred to as low-low, low-high, high-low, and high-high [93]. This low-low frequency shows an image's properties, while the high-high band signifies its noise. Also, a new transform region approach is proposed for image watermarking that incorporates BEMD to improve robustness. Therefore, the frequency band is divided by BEMD transform from strongest frequency to weakest bands. On the contrary, for complex and multidimensional searches, the PSO optimization strategy is used [84].

Now, watermarking techniques are widely used and are shown in this way: Taghia et al. [27] recommended watermarking images using a BEMD methodology. The input image is distributed in n -residual image throughout the embedding process, producing several 2D-IMFs. Additionally, the extraction method involves the use of the locally linear structure, affine symmetry as well as the clustering approach. Therefore, the experiment's findings indicate that this approach is very robust and imperceptible.

In [28], Sabri et al. provides an image watermarking method using BEMD. The first four intrinsic mode functions (IMFs) of the BEMD are taken into consideration for the binary matrix as well as the watermarking method throughout the embedding phase. Moreover, BEMD is more effective than other methods, such as Fourier and wavelet domain, to obtain an intrinsic feature.

In [94], a BEMD-based digital image watermarking technique is proposed. In this, the encoding and decoding processes uses the CDMA (code division multiple access) and SS (spread spectrum) techniques. The results of the experiments show that this technology is far more resistant to attacks and there is no noticeable difference between watermarked and digital images. The BEMD method is used by the author to offer a robust watermarking approach in [29, 30, 31, 32]. Accordingly, the BEMD transform is used to decompose the image into different frequency components and obtain the orthogonal characteristics. Moreover, this method improved robustness against geometric attacks. Arnold map-based SVD and DWT image watermarking were designed to be robust by Kamble et al. [77]. In order to protect the algorithm's copyright protection and ensure its security, SVD, as well as Arnold map, are used, respectively. The experiment's findings confirm that the suggested system has high image quality. In the SVD and DWT domains, SVM-PSO is utilized as a component of an image categorization procedure to extract properties of an image texture with a constant cycle [68]. As a result, SVD is employed to improve image texture.

In [95, 26], a hybrid LWT and Arnold transform-based multipurpose watermarking technique is introduced. To preserve the retrieved watermark's authenticity and separate the image into frequency bands using, LWT and BEMD have been used with the highest robustness and lowest vulnerability, respectively.

Saxena et al. [69] suggested strategy based on the watermark in the input image using DWT, DPSO, and SVD for color images. To offer the required variance and good possibility to increase from enlargement, dynamic PSO (DPSO) is employed. DWT-SVD, along with DPSO performance, is evaluated in comparison to other PSO variants, it is obvious that the outcome of the suggested technique is better than another encompassing approach. Zear et al. [96] presented a variety of watermarking techniques using DWT, SVD, as well as DCT for medical applications. A host image is utilized to deconstruct to various bands of three levels of DWT during the embedding phase, and one of those bands is then exposed to DCT in order to produce matrices that can be scrambled using the Arnold algorithm. According to the suggested method, a back propagation neural network (BPNN) is used to increase signal robustness as well as minimize the effect of noise on the watermarked picture. This proposed scheme presents the power and visual characteristics of the watermarked picture at various gain levels. The author proposes DWT-DCT along with SVD approaches for color image watermarking in digital images [97]. As a result, the RGB to YUV color space of the cover image is converted. Moreover, the lower band is then divided into blocks using DCT, SVD, as well as DWT. After that, luminance component Y is implemented using DWT. This approach demonstrates improved robustness and increased visibility.

A logistic chaotic map-based invisible image watermarking methodology found on DCT-DWT and SVD with a modified least squares curve is shown in [98]. Here, the source image is deconstructed into 4 sub-bands employing the DWT procedure. Afterwards, each block is subjected to DCT and a number of specific medium periodicity DCT factors are retrieved to generate a modified matrix. Also, the experiment's findings demonstrate improved perceptual quality and excellent security using the chaotic map. The author describes an unseen as well as persistent watermarking system Using IWT and a confidential key matrix [99]. This approach also increased the grey scale image's robustness and preserved its copyright protection. Furthermore, IWT is employed to maintain the strength strategy, and a confidential key matrix is employed to enhance the encoding methodology's privacy. The results of the proposed procedure show that BER and NC have low and high values,

respectively. For image watermarking, [70] provided an IWT, standardized SVD, Genetic algorithm (GA) as well as PSO. In addition, this strategy improves robustness and invisibility compared to other attacks. Furthermore, it uses normalization to identify the invariance and the invariant features that are discovered. After that, IWT is used first, then the NSVD. The results of the proposed technology show that it is better than conventional ways and has a high level of robustness against numerous attacks.

The authors describe SVD and ageing leader-basis PSO as an effective image watermarking method [71]. Additionally, the watermark is encrypted using the Arnold transform for security, and ageing leader-based PSO, as well as SVD are applied to quicken and improve the security of watermarking. Furthermore, this proposed approach is contrasted with current approaches based on absolute Mean Square Error (MSE), PSNR, root MSE, standardized cross-correlation, as well as mean angular deformation. The author suggests a double-embedded watermarking technique using SVD-DCT-DWT as well as PSO is discussed in [72]. As a result, the Arnold transformation is used to encode the watermark, and also the low-frequency region and greater-frequency regions of the input images are also relevant. Additionally, the embedding parameter vector is improved using PSO. As a result, these methodology findings demonstrate strong capacity, great robustness, and visual impact against the majority of attacks.

An innovative CNN-based scenario for creating image watermarks with security guarantees for usage in smart city applications is proposed in [100]. A grey watermarking image is included as a watermark signal using DCT. Rapid R-CNN also converts a dual point from a signal input. The three main criteria for judging an image watermark's quality are transparency, robustness, and security. The proposed classification method has classification accuracy for the image data of over 93.75%. A strong hybrid-based invisible digital image watermarking is discussed in [101]. Hence, this process involves the inner and outer watermarking schemes that are utilized as visible and invisible watermarking schemes, respectively. The mitigation of false-negative errors, except for any attacks, is referred to as the fusion of blind and non-blind approaches. For improved outcomes, it is modified by employing DWT as well as SVD. Also, this approach is robust to attacks like speckle, rotation, Gaussian noise, Poisson, salt and pepper, and JPEG compression. In [92], the use of DWT and SVD in a 2D SVD-based blind picture watermarking approach is suggested. As a

result, the two-level authentication technique is used to secure this method. The experimental outcome presents that the robustness, capacity, and imperceptibility of this approach have all been improved.

In [102], strong and blind watermarking methods using DWT, DCT, and SVD are discussed. In this, three grey watermark images and a color host image are used in the embedding and recovery procedure. IDWT and IDCT are also employed to obtain the latest color factor. The results of the proposed technique demonstrate that the technique has high imperceptibility and good robustness. A method for lossless image compression using PSO improvement, DWT, LZW compression, RSA encryption as well and DWT is discussed in [73]. Therefore, randomly generated numbers, sequencing, and RSA encryption are used to encrypt by approximating and comprehensive sub-bands, respectively. Additionally, described sub-regions already have fewer details. PSO algorithm optimization results in good compression performance.

An improved image watermarking technique founded on HD, DWT as well and SVD is presented in [103]. In order to find the right balance between invisibility and strength, the fruit fly optimization method is utilized to choose a flexible as well as optimum correction aspect. A weak and reliable image watermarking method founded on sequential LSB bit substitutions is discussed in [104] for the purpose of protecting digital images. In order to insert a fragile watermark, randomized insertion is employed to detect tampering. A privacy key is additionally employed to protect information from unwanted authority. The results of the proposed technique demonstrate that it offers a variety of features, including quick tamper detection, ownership protection, and high embedding capacity. An improvement to the watermarking method using DWT and PSO is proposed in [74].

In order to insert the data, a small frequency area is employed. The greatest response is given by the upgraded gbest and pbest for the encoding and recovery procedure. An application of homomorphic transform (HT), Arnold transforms, DWT as well as SVD to watermark images is examined in [105]. In order to deconstruct the input image by DWT into multiple sub-bands, and HL sub-band is again converted into radiance and reflectivity factors by HT. Furthermore, SVD, as well as DWT, enhance performance and strength, respectively. The proposed results demonstrate its excellent imperceptibility and robustness. The use of circular embedding, the

Arnold transformation, and the Hilbert curve with BEMD to watermark images are detailed in [33]. The cover image is broken up IMFs and residue using BEMD to get a multi-scale depiction. In addition, the Arnold transformation is used to enhance the privacy of the method then the Hilbert curve reduces it to a dimensional signal. The technique's results demonstrate its excellent visual quality and strength.

In [106], the author proposes empirical mode decomposition in the wavelet domain using an ECG data reduction technique. Thus, the compression approach solves the issues of storage and transmission. To assess the compression performance, 48 ECG data points from the MIT-BIH arrhythmia database were used. According to the experiment results, the suggested approach offers greater compression performance with opposing main signal characteristics. In [75], A blind and strong image watermarking technique using combining logistic maps with PSO is presented in the composite area. Initially, the cover image is deconstructed using DWT, and the insensitive LH and HL sub-bands are processed to DCT using a human visual model. With the DCT, an ideal frequency spectrum is selected to increase the watermark's transparency and robustness. Moreover, PSO is employed in multi-dimensional optimization to choose the best DCT coefficients. Security is provided by a logistical network that is interconnected. The results of this method demonstrate its great imperceptibility and good resilience.

In [107], the author presents a deep neural network-based automatic and robust watermarking method. Further, Domain expertise is not as necessary with the utilization of deep learning neural networks. Furthermore, to avoid human intervention and explanation, image watermarking uses an unsupervised deep learning framework. The results of the proposed method show great strength in the absence of the need for previous awareness of potential deformation. Numerous image watermarking are proposed in [82] employing amalgamation of SVD, Non-sub sampled contourlet transform (NSCT), and redundant discrete wavelet transforms (RDWT), set partitioning in the hierarchical tree (SPHIT) addition with NSCT. To improve shifting variance and major directive characteristics, NSCT is applied. Moreover, the watermark image is used with the SPHIT approach for compression. The efficiency of the method demonstrates greater robustness and security against attacks.

In this chapter, A robust image watermarking method using PSO, BEMD as well as DCT is discussed. The approach employs the fusion of DWT along with SVD to embed watermarks into a

single cover. The effectiveness of the suggested strategy is assessed in the context of its robustness and visual appearance. The key role of the work is recognized as follows:

1. The original image and watermark image are transformed using SVD with DWT and DCT, which increases the capacity and imperceptibility of the algorithm.
2. In order to enhance image quality and produce appropriate frequency factors for the input image, the watermarking image is disintegrated using BEMD.
3. For multiple-scale assessment, the BEMD procedure separates deficient as well as higher frequency bands, and PSO optimization is utilized to provide a flexible scale factor matrix.
4. In this method, the embedding and extraction of digital content uses a secret key for authentication purposes.

4.2 The Proposed Method

In this work, the proposed procedure is prepared from DWT, BEMD, DCT, SVD and PSO. The watermark image (size: 256×256) is embedded into the input image (512×512). DCT is employed on a certain band obtained by the application of second-level DWT on the input image. However, the watermark image is produced by BEMD. Moreover, by BEMD breakdown with distinct frequency analysis, IMFs and residue are produced. Finally, inverse SVD, BEMD and DCT are applied to watermarked images, followed by the application of DWT to obtain the compressed watermarked image. However, in extraction, the whole process is applied in reverse order. The presented strategy is employed to increase the image's resistance against numerous attacks without lowering its quality.

4.2.1 Algorithm for watermark embedding

The following are the basic steps for imperceptibly encoding the watermarks algorithm:

1. Initially, 512×512 sizes original images and 256×256 size watermark images are obtained.
Cameraman (I): cover image
L Singh (I_w): 'logo' watermark
 α : Scale factor

2. The 2D DWT is employed to input image I and in order to obtain the second level sub-bands of the DWT (LL2, LH2, HL2, and HH2) to enhance the visual quality of an image.

$$[LL2, LH2, HL2, HH2] = \text{DWT}(I);$$

3. DCT coefficient is used to DWT's LL2 subband to give the algorithm accuracy.

$$D = \text{DCT}(LL_2);$$

4. EMD is carried out on the watermark image I_w in order to achieve the required frequency factors for the input photos.

$$I_w = \text{BEMD};$$

5. To obtain a flexible scale factor matrix, PSO is implemented in both the cover image and The watermark image.

$$\text{PSO} = (I, I_w);$$

6. To create the singular value orders S_y and S_w and store the left-hand and right-hand vectors, respectively, the singular factor of optimal value (SVD) is applied to calculate the singular factor of optimizing value.

$$[U_y S_y V_y^T] = \text{SVD}(I);$$

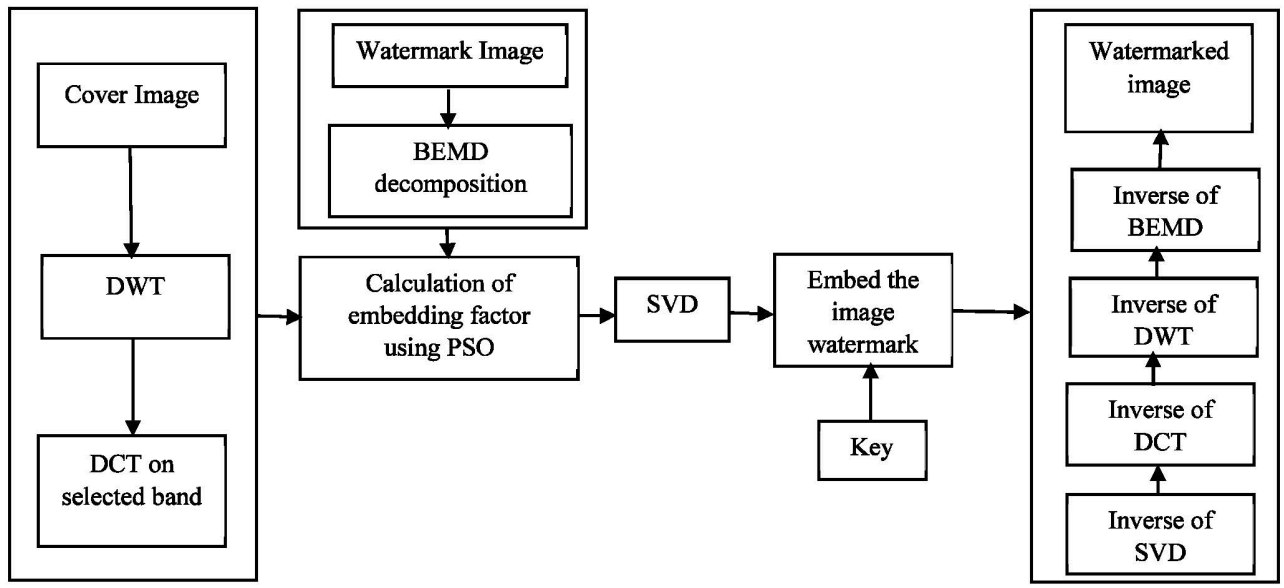
$$[U_w S_w V_w^T] = \text{SVD}(I_w);$$

7. The S_y of the cover image contains the S_w of the watermark image. Furthermore, PSO is employed to optimise the encoding factor matrices.

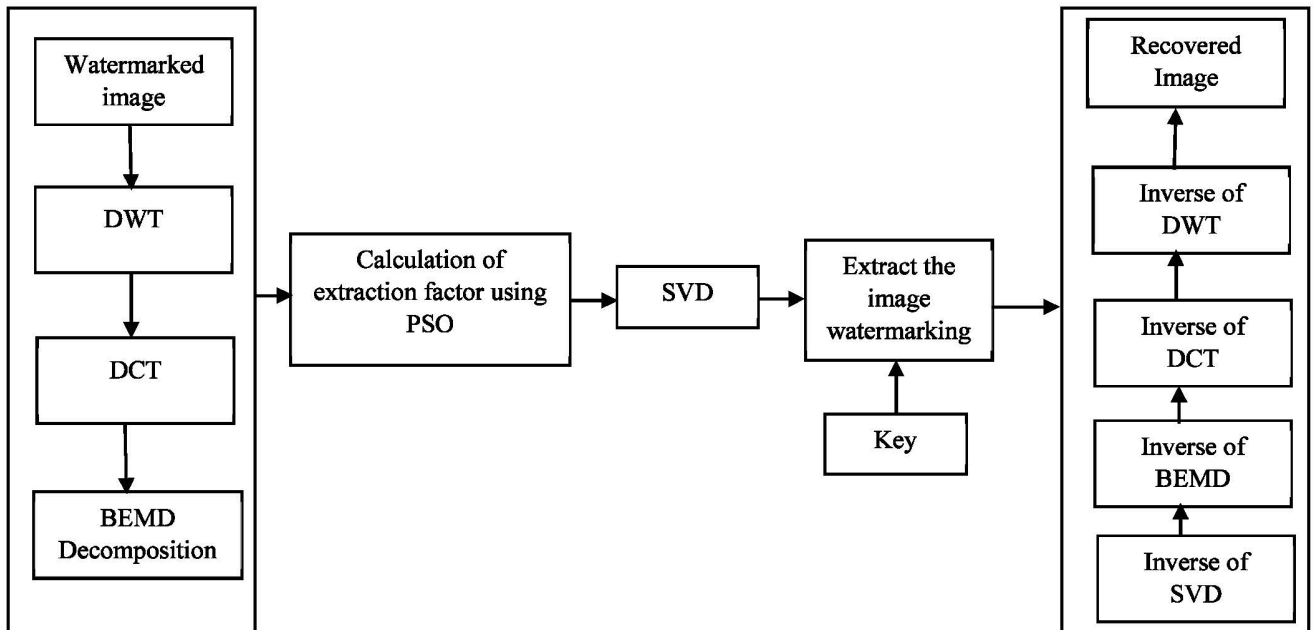
$$S_{\text{mark}} = S_y + \alpha \times S_w;$$

8. To obtain a watermarked image, ISVD, IDCT, IDWT, and IBEMD are used.

To increase the method's security, create the key using the X-OR cypher approach, Key = K.



(i)



(ii)

Figure 4.1: BEMD using watermark (i) Embedding and (ii) Recovery Process

4.2.2 Watermark Recovery Process

The following are the essential steps for efficiently extracting the hidden watermarks algorithm:

1. The watermarked image I_1 is applied to DWT to generate the different bands $LL1_w$, LH_w , HL_w , and HH_w .

$$[LL1_w, HL1_w, LH1_w, HH1_w] = DWT(I_1);$$

2. The $LL1_w$ subband of the deconstructed watermarked image is processed to DCT.

$$D_w = DCT(LL_WV);$$

3. The scaling factor matrix is calculated using PSO and BEMD, which are applied to the DCT coefficient D_w .

$$B_w = BEMD(D_w);$$

$$P_w = PSO(B_w);$$

4. The singular value matrices for P_w are obtained using SVD.

$$S_w = SVD(P_w);$$

5. The equation of extraction recovers the encrypted watermark.

$$S_{wrec} = (S_w - S_y) / \alpha;$$

6. To retrieve the watermark image, the ISVD, IBEMD, IDCT, and IDWT algorithms are used.

7. To increase the security of the extraction procedure, the secret key is used.

4.3 Experimental Results and Analysis

In this work, six different types of host images (with dimensions: 512×512), and one watermark, with dimensions '256×256' are considered for experiments. Grey-level images such as Barbara, baboon, cameraman, Lena, Tank, and Goldhill are used for experimental purposes. Peak-signal noise ratio (PSNR) and normalized correlation (NC) are utilized in this approach for testing. In this experiment, the "Haar wavelet" has been used because of its superior resolution.

Strength and visual quality are important metrics to evaluate the efficiency of watermarking systems. PSNR (peak signal-to-noise ratio) determines the value of the watermark. A higher PSNR value signifies a likeness between the input image and the watermark image. This finding allows us to conclude that watermark images have a high level of imperceptibility. When the value

of PSNR is greater, the watermark image's resolution will be improved. Usually, a watermarked image should have a PSNR value of at least 39 [10]. PSNR is calculated by this equation (4.1).

$$PSNR = 10 \log \frac{(255)^2}{MSE} \quad (4.1)$$

The mean square error (MSE) is calculated by following equation (4.2) [10]:

$$MSE = \frac{1}{M \times N} \sum_{x=1}^m \sum_{y=1}^n (Oxy - Wxy) \quad (4.2)$$

Where, Wxy of dimension $x \times y$ stands in for a watermark image pixel and Oxy indicates the pixels of the original image of size $x \times y$. Nevertheless, normalization correlation (NC) is employed to evaluate the strength of the technique [10]. The value of NC is measured by the similarity between the original and retrieved watermarks, which ranges from 0 to 1. The optimal value is 1, while a value of 0.7 is acceptable.

$$NC = \frac{\sum_{x=1}^m \sum_{y=1}^n (I_{originalxy} \times I_{recoveredxy})}{\sum_{x=1}^m \sum_{y=1}^n I^2_{originalxy}} \quad (4.3)$$

Where $I_{originalxy}$ stands for the pixels of the cover image with a dimension of $m \times n$, and $I_{recoveredxy}$ stands for the pixels of the watermarked image with a dimension of $m \times n$.

Table 4.1: PSNR and NC at distinct gain value

Different Gain value	PSNR (in dB) value	NC value
0.001	46.9565	0.995
0.01	44.6268	0.997
0.05	44.3971	0.997
0.1	44.0478	0.998
0.12	39.8901	0.998
0.5	38.5430	0.999
0.7	36.2527	0.999

Table 4.1 depicts the PSNR and NC value (without any attack) of our technique at a varying gain, and it has been found that the value of PSNR and NC is above 36.2527 dB and 0.995, respectively.

Table 4.2: PSNR and NC values for different images

Different Images	PSNR (dB)	NC
Barbara	41.7053	0.9993
Baboon	44.6268	0.9997
Lena	43.1863	0.9996
Cameraman	49.4254	0.9998
Goldhill	45.3862	0.9998
Tank	45.7331	0.9999

However, PSNR and NC results for different images are listed in Table 4.2. It can be seen that the highest NC and PSNR values are obtained as 0.9999 for Goldhill and 49.4254 dB for cameramen, respectively. Table 4.3 depicts PSNR and NC results for various attacks and different gain values, and it is found that the assessment of PSNR and NC are above 34 dB and 0.9364, respectively. It can be observed that the highest PSNR and NC assessment was 43.8946dB for salt & pepper and 0.9967 for the median filter, respectively. However, PSNR is poor under gamma correlation.

As clearly mentioned in table 4.4, our technique uses the fusion of DWT and DCT along with optimization-based PSO, BEMD, and SVD to provide better performance than former techniques [91, 96, 98].

Table 4.2 depicts PSNR and NC for distinct images and fixed gain values, and it is found that the assessment of PSNR and NC are above 40 dB and 0.9993, respectively.

Table 4.3: PSNR and NC values for various attacks

Different type of attacks	Noise Density	PSNR (in dB) value	NC value
Salt & Pepper	0.001	43.8946	0.9364
	0.005	43.5140	0.9364
	0.01	43.2210	0.9707
	0.1	43.1382	0.9707
	0.5	36.7922	0.9882
	0.7	35.3378	0.9906
Rotation	1°	40.5789	0.9823
	3°	40.2832	0.9852
	5°	39.8937	0.9879
Gaussian Attack	0.001	41.6021	0.9364
	0.005	41.5889	0.9371
	0.01	41.4358	0.9564
	0.05	41.3756	0.9767
	0.1	40.2033	0.9859
	0.5	36.5762	0.9878
Speckle	3×3	38.7537	0.9829
Median Filter		43.6371	0.9967
Gamma Correction		34.7651	0.9724
Scaling		41.6523	0.9598
Shearing		42.1212	0.9613

The highest NC and PSNR values reported by the suggested technique are 0.9967 and 43.8946 dB against the Median filter and salt & Pepper noise attack, respectively. However, the minimum NC value is reported as 0.9364 against a Gaussian attack. NC and PSNR values clearly prove the successful recovery of hidden watermarks.

Table 4.4: Comparing of NC values on various attacks

Various Attacks	Noise Density value	Singh AK et.al. [91]	Zear et. al. [96]	Kang et. al. [98]	Proposed method
Salt & Pepper	0.01	0.7552	0.7747	0.9609	0.9707
Gaussian Noise	0.5	0.6565	0.6576	0.6627	0.8878
Median Filter		0.9752	Not found	0.9953	0.9967

Table 4.4 represent the robustness of the proposed method in comparison to existing technique [98, 96, 91] in terms of NC and PSNR value.

It has been further noted that the highest reported NC value by the previous method [98] is 0.9953 against the median filter attack. However, the minimum reported NC value by the existing technique [91] is 0.6565 against a Gaussian noise attack.

Table 4.5 represents the imperceptibility of the proposed method and existing technique [108] for well-known attacks. The best PSNR value attained using the suggested method is 43.6371 dB against the median filter attack. Though, the lowest PSNR value is 34.7651 dB against a Gamma Correction attack. Therefore, it is clear that the suggested method offers greater imperceptibility than the earlier method [108].

Table 4.5: PSNR value for various attacks

Distinct Attacks	Noise Density value	PSNR[108] value	PSNR of proposed method
Gaussian Noise	0.2	26.6051	42.6397
Salt & Pepper	0.05	26.5243	43.2095
Gamma Correction	2	21.4030	34.7651
Median Filter	3	26.8223	43.6371

It is further seen that the highest reported PSNR value reported by existing approaches [96, 70, 91, 98] is 43.88 dB for the same image in table 4.6. However, the lowest reported PSNR value is 31.41.

Table 4.6: Comparison of PSNR

Scheme metrics	Zear et. al [96]	Rao. V et. al. [70]	Singh et.al. [91]	Kang et. al. [98]	Proposed Method
PSNR (in dB)	43.88	31.41	35.84	42.25	44.63

Table 4.7 demonstrates the imperceptibility of the suggested technique and former technique [96] for famous attacks. The high PSNR value achieved by the suggested technique is 44.6268 at a gain value of 0.01. Though, the highest PSNR assessment of the existing method is 43.88 at a gain factor of 0.01. Therefore, it is clear that the suggested technique offers better imperceptibility as compared to the former method [96].

Table 4.7: PSNR comparison on identical image

Gain Value	PSNR [96]	PSNR of the Proposed method
0.01	43.88	44.6268
0.05	36.53	44.3971
0.1	32.09	44.0478

The PSNR assessment of different gain factors is depicted graphically in Figure 4.2. The suggested method's optimum PSNR value is greater than the one currently in use at different noise densities, demonstrating the robustness of the offered process in figure 4.3.

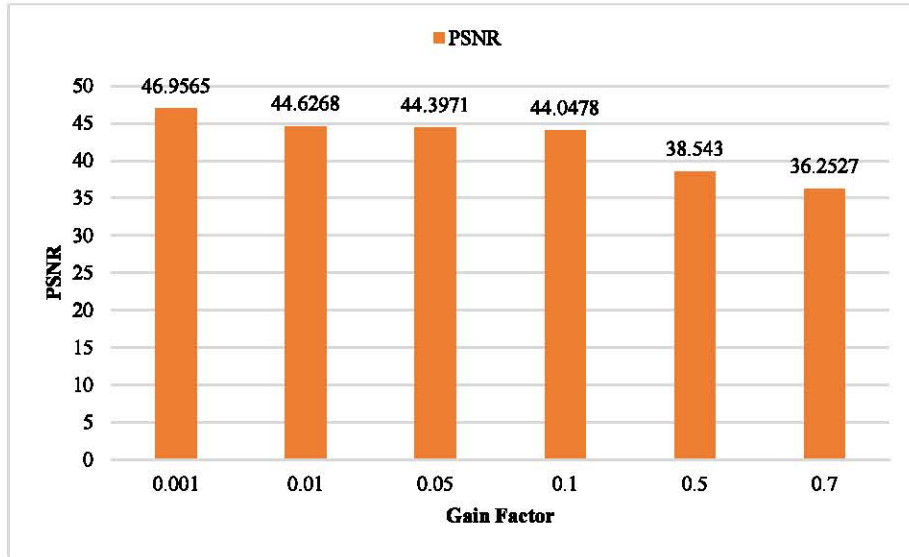


Figure 4.2 PSNR value using various gain factors

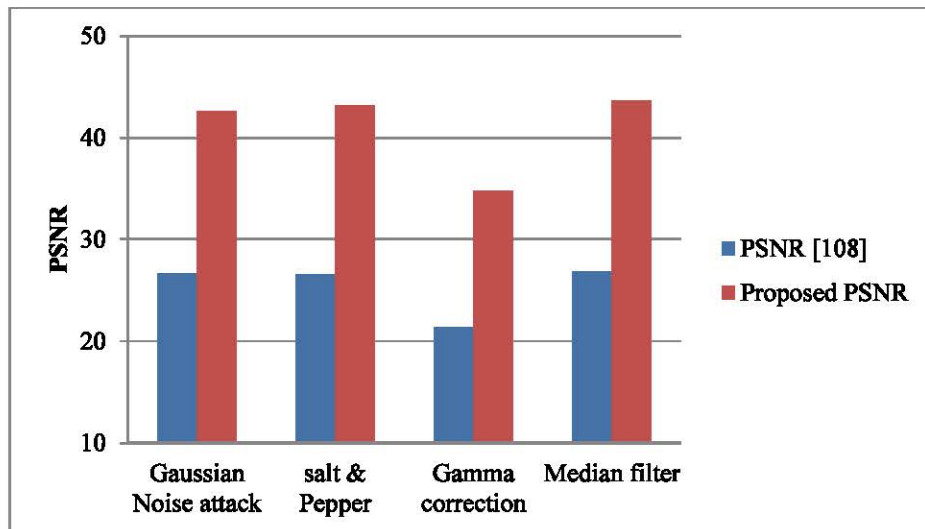


Figure 4.3 Graph for comparing PSNR values

Figure 4.4 demonstrates NC values for different types of attacks at different gain factors. As a result, as the value of NC increases, the PSNR value will decrease.

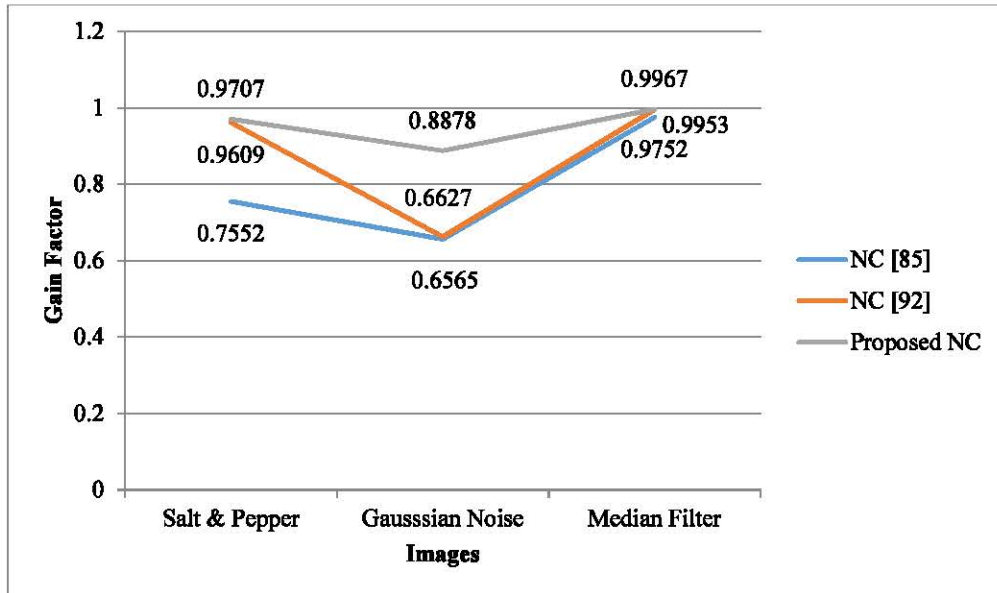


Figure 4.4 NC value at various Gain factor

Figure 4.5 shows the inconsistency between the suggested PSNR value as well as previously described methodologies [96] at various gain values.

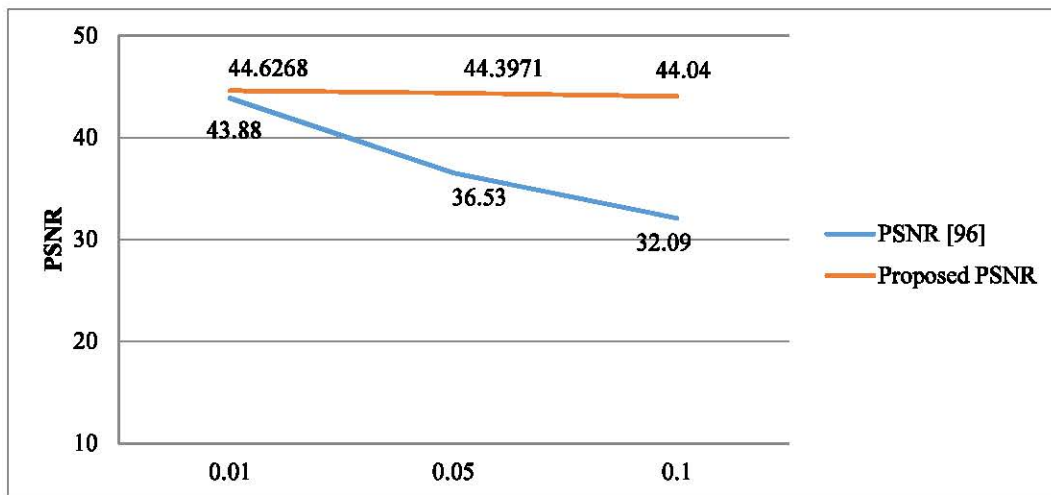



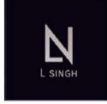









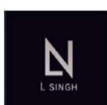

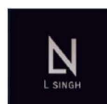


Figure 4.5 PSNR values

Table 4.8: The NC value for watermark attacks and watermark recovery

Attacks	Attacked image	Obtained NC value	Recovered watermark image
Salt and pepper (0.001)		0.9364	
Salt and pepper (0.01)		0.9707	
Gaussian attack (0.001)		0.9364	
Gaussian attack (0.01)		0.9564	
Median Filter (3×3)		0.9967	
Gamma correction		0.9724	
Shearing		0.9613	
Speckle		0.9829	

The NC values of various attacks and recovered watermarked images are shown in Table 4.8. The NC value suggests that the proposed technique is robust to attacks.

Table.4.9: Comparing characteristics of existing systems

S.no	Description	Existing Methods						Proposed method
		Zear et.al. [18]	Kang et.al. [20]	Zang et, al. [24]	Singh et. al.[45]	Srivastava et. al.[46]	Rao.V et.al. [47]	
1.	Nature of scheme	Robust	Blind	Robust	Robust	Non-blind	Robust	Robust
2.	Insertion domain	Transform	Transform	Transform	Transform	Transform	Transform	Transform
3.	Operation for insertion	DWT+ DCT+ SVD+ BPNN	DCT+DWT +SVD+ logistic caotic map +Least square curve fitting	DWT+ DCT+ SVD+ PSO	DWT+ DCT+ SVD+ encryption + steganography	DWT+ SVD+ PSO	DWT+ DCT+ SVD+ PSO	DWT+ SVD+ DCT+ BEMD + PSO + cipher key
4.	Host Image size	512×512	512×512	512×512	512×512	---	512×512	512×512
5.	Watermark image size	256×256	32×32	256×256	256×256	---	256×256	256×256
6.	Host type	Grey	Grey	Grey	Grey	Color	Grey	Grey
7.	Watermark image size	Binary	Binary	Gery	Binary	Color	Grey	Grey
8.	Robustness	✓✓	✓✓✓	✓✓	✓✓	✓	✓	✓✓✓
9.	Imperceptibility	✓✓	✓✓	✓✓	✓✓	---	✓	✓✓✓
10.	Security	✓✓	✓	✓✓	✓✓	----	---	✓✓
11.	Applications	Copyright protection, healthcare applications	Copyright protection	Copyright protection	Telemedicine and telediagnosis	Copyright protection and compression	Copyright protection	Image authentication, copyright protection

Based on various existing methods, method category, domain, inclusion process, cover and watermark image size, cover and watermark category, purpose(s), and applications are represented in Table 4.9. This proposed method is used because of its cheap computing, good encoding bandwidth, and multiple-scaled evaluation. On the contrary, the entire property has not been included in all the existing methods. As a result, it demonstrates that the suggested technique is superior to the existing technique for image analysis, image enhancement, and authentication. In evaluating robustness across different watermarking methods, a common notation is used, where a single tick (✓) represents lower robustness, and triple ticks (✓✓✓) indicate higher robustness, as observed in various research papers.

In this chapter, we developed an improved DWT- DCT-based watermarking method. In this technique, the suggested method offers a significant improvement in security, imperceptibility, and robustness over the previous methodologies. Furthermore, the cypher key utilized in the

embedding and extraction procedure improves the confidentiality of this method. Moreover, the tradeoff between robustness and transparency is better balanced with PSO optimization. The approach's outcomes demonstrate that the suggested approach satisfies the demands of strong watermarking in three areas: robustness, confidentiality as well as visual quality. The PSNR and NC values obtained are acceptable for attention. Also, the invisibility of the watermarked image is evaluated subjectively in order to determine its level of quality. This subjective review was used to determine whether the suggested technique could create an acceptable level of watermark quality at a specific gain factor. Therefore, the following are the main attributes of the suggested method: i. The DWT, DCT, as well as SVD combination offers superior performance as it relates to invisibility, robustness, and bandwidth. ii. For verification, a confidential key is utilized. iii. To enhance and obtain a flexible scale factor matrix, PSO is applied. iv. A subjective method is utilized to assess the watermarked image's visual quality. The recommended method may also be useful for texture segmentation and classification, remote sensing, image enhancement, and medical image analysis.

Laxmanika Singh and P. K., Singh, "Robust and imperceptible image watermarking technique based on SVD, DCT, BEMD and PSO in wavelet domain" *Multimedia Tools and Applications*, Springer, 81(16), 22001-22026, 2022.

CHAPTER 5

EFFICIENT AND SECURE WATERMARKING THROUGH ARNOLD TRANSFORM IN BEMD, SVD, AND DWT DOMAIN

In this chapter, an enhanced watermarking method is developed using the discrete wavelet transform (DWT), singular value decomposition (SVD) as well as bi-dimensional empirical mode decomposition (BEMD). The 1st level of DWT is used during the embedding procedure to divide the cover image into different sub-bands (LL, LH, HH, HL). Moreover, DWT sub-bands are decomposed into strong and weak bands using BEMD decomposition. SVD is used to calculate the singular factor on a specific band for an encoding procedure. “Haar wavelets” are used to implement the proposed technique. Additionally, this method uses an inverse DWT, SVD, and BEMD process to obtain the watermarked image. Moreover, the extraction procedure has the ability to extract watermark data. BEMD is employed to obtain the multiple range description as IMFs. Moreover, it's employed to enhance the visual impact of images. Also, SVD, DWT, as well as the Arnold transform are combined to increase the image's privacy, reliability, and imperceptibility against multiple attacks. The subjective metric is then employed to measure the watermarked image quality. A variety of geometrically and non-geometrically process attacks, like salt-and-pepper attacks, Gaussian noise attacks, JPEG compression, median filter, and shearing, are better handled by the suggested method, which also effectively improves robustness, security and visual quality.

5.1 Introduction

The open-chain usage of information technology for the distribution and sharing of digital documents has proven to be a significant and affordable method for doing so. Four categories of watermarking techniques can be made in accordance with the kind of facts to be watermarked: text watermarking, image watermarking, audio watermarking as well as video watermarking. Therefore, the topic of the current study uses images as the input data for watermarking because they have a better capacity for data embedding. Malicious attack challenges include preventing copyright violations, proprietary identification, and false identities [109]. Digital image watermarking can be used to overcome security and safety concerns, according to some researchers. Digital watermarking is a reliable method of content authentication and copyright protection for multimedia. Spatial domain and transform domain

approaches are the two primary categories of image watermarking methods. The spatial domain uses simple computation techniques. The primary spatial domain techniques include spread-spectrum, correlation-based, and LSB substitutions. The watermark information is used instantly in spatial domain watermarking and merged into the cover signal's pixel values, bit stream, or coding values. On the other hand, signal-processing attacks are more likely to succeed against spatial domain techniques [110]. By altering the coefficients of a transform, Singular value decomposition (SVD), discrete wavelet transform (DWT), discrete Fourier transform (DFT), and discrete cosine transform (DCT) algorithms are employed to embed the data. Though computationally challenging, transform domain watermarking approaches improve the robustness of watermark data.

Therefore, SVD technique is used to encode the watermark, and the offered process is used in many regular image processing utilizations, including image compression and watermarking [77]. Imperceptibility ("human eyes cannot distinguish between the watermarked and input image") and strength ("illegal persons or Teams are unable to delete the data's encoded watermark") are the next two characteristics of a successful watermarking technique. The strength of the watermarking technique is determined by its robustness to both intentional (malicious attacks) and unintentional changes during transmission and storage (compression, noise, filtering, rotation, etc.) [76].

To preserve digital content and intellectual property, many researchers employed a joint encryption-watermarking approach based on DWT, SVD as well as Arnold scrambled transform [76, 77, 78, 79, 80, 111, 33]. In [112], a DWT and SVD-based digital image watermarking procedure is introduced. This evolved to the use of a binary image as a watermark. The suggested technique additionally appears to be robust against various geometric and frequency domain attacks. For robustness and data security, an image watermarking method founded on the logistic and RSA algorithms was created in [110]. This experimental outcome demonstrates better imperceptibility and robustness.

In [81], the use of set partitioning in hierarchical tree (SPIHT) in the wavelet area for image watermarking is demonstrated. DCT and SVD support high-energy compaction properties, with the Arnold transform employed to enhance confidentiality, and the SPHIT technique utilized in Bit compression. This approach involves strings that enable precise rate control. In contradiction to multiple attacks, the result of offered technique is robust and imperceptible. various image watermarking is employed in [82] by combining RDWT, NSCT, SPHIT, and

SVD. As a result, the non-subsampled contourlet transform (NSCT) achieves shift variance and increased directionality assets. The SPHIT also achieves compression on the watermark image. The result demonstrates excellent strength and privacy against the various attacks. In this chapter, we offer an image watermarking method by SPIHT in the wavelet domain. The computation for embedding and recovery involves factors such as imperceptibility, security, and robustness. The work's primary roles are acknowledged as follows:

1. Considerable NC values can be achieved by employing the renowned transform domain and Arnold transforms, as well as a combination of SVD, BEMD, and DWT for a better trade-off between visual quality and resilience demands.
2. The watermark image is scrambled utilizing Arnold transform for increased privacy. Even after extraction, this makes it impossible for attackers to recover. The BEMD approach is utilized to disassemble the watermarking image to improve the quality of an image and obtain an enhanced frequency factor for the input image.
3. The proposed watermarking approach diminishes the cost of capacity, and the concealed watermark makes it possible to store and retrieve data quickly.
4. Tables 5.1, 5.2, 5.3, and 5.8 of our research certainly establish that the suggested approach recovers the concealed watermark, which is essentially similar to the original and embeds the watermarking transparently.
5. This method's performance is measured using a variety of experimental tests. Also, it is found that the values of NC and PSNR are better than those shown in other comparable methods [80, 81, 109].
6. According to Table 5.7, a subjective approach is employed to evaluate the watermarked image's imperceptibility.

5.2 Proposed Method

The DWT, Arnold transform, BEMD as well as SVD techniques of the suggested approach. The suggested approach is used to increase privacy and strength against various attacks without lowering the visual quality. In this experiment, we use a cover image that is 512 x 512 pixels in size and a watermark image that is only 256 x 256 pixels in size. In this research, the Peak Signal to Noise Ratio (PSNR), Normalized Correlation (NC), Number of Changing Pixel Rate (NPCR), Unified Averaged Changed Intensity (UACI), and Structural Similarity Index is used to quantify the significant distortion between the cover and watermarked image (SSIM). Here, a private key of 32 bits is employed to encode the watermark using the Arnold transform and

obtain the invisibility and privacy of the watermark image. A key is required during insertion to preserve the finest level of security, and an identical key ought to be delivered to the receiver to get the watermark or host image. On the contrary, using the same identical key throughout the decoding procedure, the watermark can be obtained. The techniques for embedding and extracting the watermark are depicted in Figure 5.1. The process is observed using the reverse of SVD, BEMD, Arnold transform and DWT on the extracted component to retrieve the watermark image.

5.2.1 Algorithm for watermarks embedding

The steps for embedding algorithm are as follows:

Start:

Step 1: Variables are declared as:

Camerman Image (I): Original Image
Baboon Image (I_w): watermark Image
 α : scale factor
SVD and DWT: techniques founded on transform domain
Haar: "Wavelet filter."
LL, LH, HL and HH: DWT sub-bands for the cover image
 U_y, S_y, V_y : SVD coefficients for the cover image
 U_y and V_y^T : Orthonormal matrices for D
 S_y : Diagonal matrix for D
I₁: watermarked image
 S_w^K : Modified value of S_y
S_{modi}: Modified DWT coefficient

Step 2: Input and watermark the image

$I \leftarrow \text{Camerman.jpg (512 x 512 original image size)}$
 $I_w \leftarrow \text{Baboon.jpg (256x256 watermark image size)}$

Step 3: Execute 2nd level DWT on the sub-image LL into LL1, LH1, HL1 and HH1.

$[LL1, LH1, HL1, HH1] \leftarrow \text{DWT}(I, \text{Haar});$

Step 4: Apply BEMD on the LL1 band of DWT to get the IMFs and residue (r).

$B \leftarrow \text{BEMD}(LL1);$

Step 5: Transform the watermark image I_w using Arnold use secret key to scramble an image's pixels.

$A \leftarrow \text{Arnold}(I_w);$

Step 6: To obtain the residue, use BEMD on the watermark image.

$B \leftarrow \text{BEMD}(A);$

Step 7: Compute the singular coefficient of the residue of BEMD

$U_y S_y V_y^T \leftarrow \text{SVD}(B)$
 $U_w S_w V_w^T \leftarrow \text{SVD}(I_w)$

Step 8: Compute the singular coefficient of the residue of BEMD on the scrambled watermark image

$U_y S_y V_y^T \leftarrow \text{SVD}(B1)$

Step 9: Image watermarking encoding

$\alpha \leftarrow 0.01 \text{ to } 0.5$
 $S_{\text{mark}} = S_y + \alpha \times S_w;$

Step 10: Obtain watermarked image

Inverse of SVD (SVD_{LL}) = $U_y(\text{new } S_w) V_y^T$;
 $LL_R = \text{IBEMD}(SVD_{LL}, \text{IMF}_1, \text{IMF}_2, \text{IMF}_3)$
 Apply inverse of DWT to LL_R , LH_1 , HL_1 and HH_1 with modified coefficient
 $X = \text{idwt2}(LL_R, LH_1, HL_1, HH_1, \text{"Haar"}, S_x)$

End;

5.2.2 Algorithm for watermarks recovery

The steps for robustly extracting the hidden watermarks algorithm are as follows:

Start:

Step 1: Variable affirmation

α : gain factor (efficiency factor)
 LL, HL, LH, HH : sub-bands for the watermarked image
 U_w, S_w, V_w : SVD coefficients for the watermarked image

Step 2: Apply DWT on watermarked image I_w

$[LL_2, HL_2, LH_2, HH_2] \leftarrow \text{DWT}(I_w, \text{"Haar"})$

Step 3: The I_w image decomposed with the BEMD method into IMF1, IMF2, IMF3 and residue R_w .

$P_w \leftarrow \text{BEMD}(LL_2);$

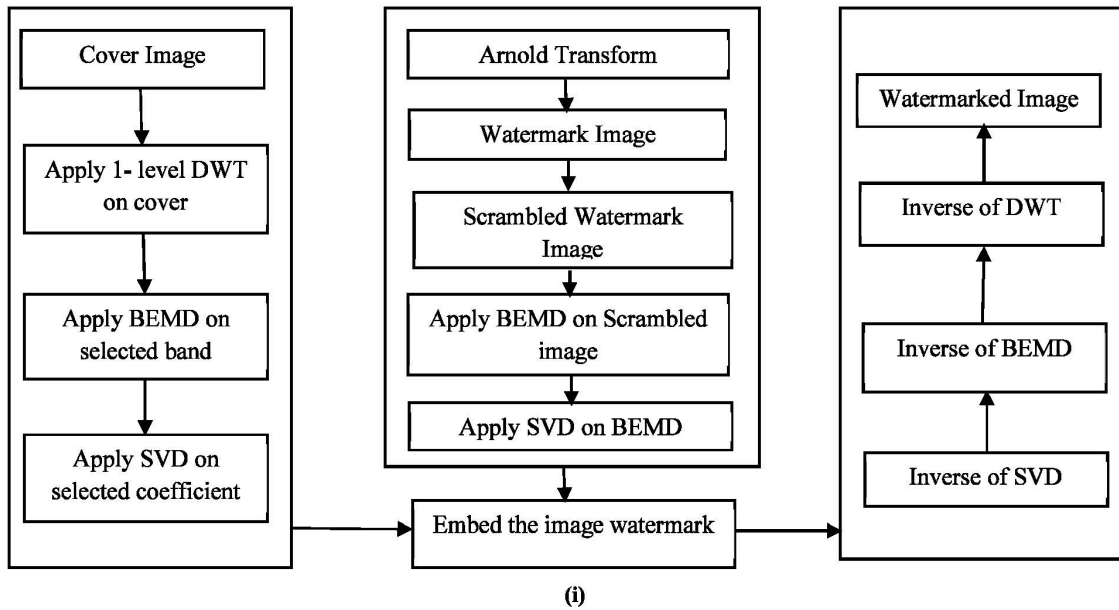
Step 4: Extract the watermark image from S_{wt} and Compute the singular value for P_w .

$S_{wt} = U_w \times S_w \times V_w;$
 $S_w \leftarrow \text{SVD}(P_w);$

Step 5: Retrieved the embedded watermark

$S_{wrec} = (S_w - s_y) / \alpha;$

End;



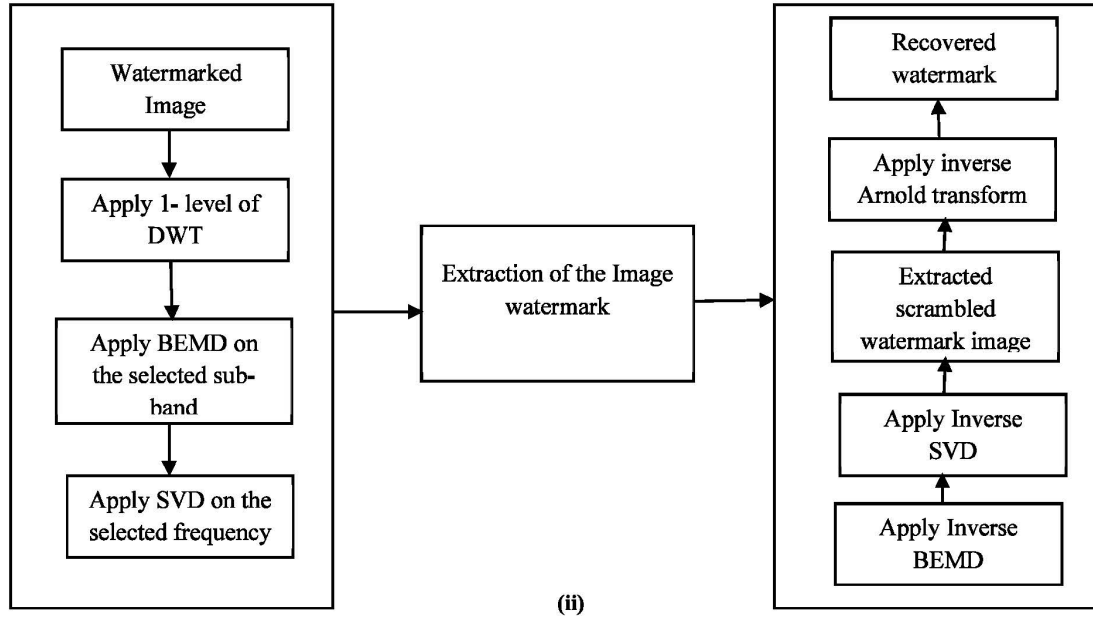


Figure 5.1: Arnold transformation-based watermark (i) Encoding and (ii) Recovery Process

5.3 Experimental Result and Analysis

All the experiments were conducted using MATLAB R2013a. For this testing objective, we are using the size of 512 x 512 cover images and 256 x 256 size of watermark images are employed. Five grey-level pictures, including Barbara, the baboon, cameraman, Lena, and boat are employed for testing. Peak-signal-to-noise ratio (PSNR), similarity index measure (SSIM), and normalized correlation (NC) are used in this method for testing. Also, this technique uses two crucial characteristics to determine how well it performs: the number of changing pixel rate (NPCR) and the unified averaged altered intensity (UACI). The mean-variance between actual and encoded images is calculated Using UACI. For higher resolution, the "Haar" wavelet is utilized in this case. The watermark image and original images used in the experiment are shown in Figure 5.2. Robustness and imperceptibility are just two of the many criteria used to evaluate the effectiveness of watermarking systems.

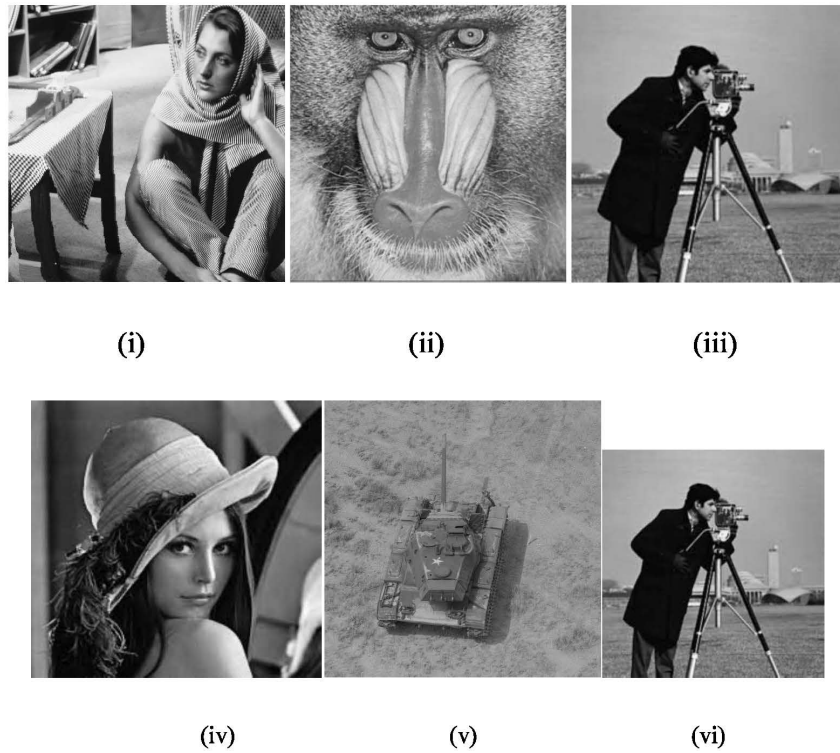


Figure 5.2 The input image of (i) Barbara (ii) Baboon (iii) Cameraman (iv) Lena (v) Boat (vi) the watermark image

The peak signal-to-noise ratio (PSNR) between two images is calculated in decibels. The ratio is employed to compare the quality of original and compressed images quality. The visual acuity will be better when the PSNR is greater. The PSNR, NC1, NC2 and SSIM performance is depicted in Table 5.1- Table 5.5.

Table 5.1: PSNR, SSIM, NC, NPCR and UACI values at distinct gain factor

Different Gain Factor	PSNR (in dB)	SSIM	NC	NPCR	UACI
0.010	42.47	1.0000	0.9522	0.9959	0.3465
0.080	42.15	0.9999	0.9964	0.9965	0.3470
0.090	41.07	0.9998	0.9961	0.9970	0.3461
0.10	40.81	0.9997	0.9972	0.9968	0.3446

0.30	38.69	0.9881	0.9981	0.9980	0.3453
0.50	38.35	0.9579	0.9999	0.9960	0.3469

Table 5.1 depicts the PSNR, SSIM, NC, NPCR and UACI assessments of our technique at a varying gain. We found that values of PSNR, SSIM, NC, NPCR, and UACI are above 38.35 dB, 0.9579, 0.9522, 0.9959 and 0.3446, respectively.

Table 5.2: PSNR, SSIM, NC, NPCR and UACI values at distinct Images

Distinct Images	PSNR (in dB)	SSIM	NC	NPCR	UACI
Barbara	41.13	0.9991	0.9962	0.9963	0.3767
Baboon	43.28	0.9988	0.9935	0.9906	0.4847
Lena	43.79	0.9965	0.9981	0.9951	0.3468
Camerman	44.06	0.9954	0.9992	0.9946	0.4598
Boat	42.36	0.9921	0.9931	0.9961	0.4789

Table 5.2 describes the value of PSNR, SSIM, NC, NPCR, and UACI for different images at a constant gain factor. It is observed that imperceptibility and robustness for cameramen are higher than other images. Table 5.3 demonstrates the PSNR value and NC value at different noise densities to observe the robustness and imperceptibility of different attacks.

Table 5.3: The PSNR and NC acquired against several attacks

Distinct Attacks	Noise Density	PSNR (in dB)	NC
Salt & Pepper	0.001	44.76	0.9979
	0.003	43.23	0.9921
	0.005	42.39	0.9880
	0.01	41.29	0.9998

	0.1	40.13	0.9877
Gaussian Attack	0.001	43.34	0.9956
	0.003	42.67	0.9875
	0.005	41.34	0.9596
	0.01	40.12	0.9519
JPEG Compression	10	42.45	0.9977
	30	40.11	0.9819
	60	40.18	0.9801
Median Filter	3×3	39.01	0.9978
	4×4	40.34	0.9832
Shearing	0.4×0.4	39.82	0.9701

Table 5.4 represents the robustness of the proposed method and former approaches [109, 81] by performing NC value. The result clearly states that our method achieved 0.9 scores for NC for most of the considered attacks. However, the minimum NC offered by our method is 0.8193 and 0.7989 against Scaling attack.

It has been further observed that the former technique [109] does not maintain the standard score for NC. The highest NC value offered by the former technique is 0.9961 against salt & pepper attack. Though, the minimal NC value is 0.6297 under Gaussian noise attack. Further, the best NC value for technique [81] is 0.9969 against Salt & Pepper and JPEG Compression attacks. However, the lowest NC value is reported as 0.5563 against scaling attack.

Table 5.4: NC values in comparison to previous methods

Different Attacks	Noise Density	NC [109]	NC [81]	Proposed Method
Salt & Pepper	0.001	0.9938	0.9979	0.9979
	0.01	0.9961	0.9424	0.9998

	0.1	N/A	0.7005	0.9877
Gaussian noise Attack	0.001	0.9591	0.9874	0.9956
	0.005	N/A	0.9219	0.9596
	0.01	0.6297	0.8569	0.9519
JPEG Compression	10	0.9913	0.9969	0.9977
Scaling Attack	($\times 0.5$)	N/A	0.5563	0.8193
	(1.1)	0.7251	N/A	0.7989

It is evident from this that the recommended strategy is more robust and offers less distortion than current approaches [109, 81].

Table 5.5: NC values compared to other techniques

Different Attacks	Noise Density	NC [81]	NC [80]	NC of proposed method
Median filter	3 \times 3	N/A	0.9949	0.9978
JPEG compression	10	0.9969	0.9965	0.9977

Table 5.5 represents the robustness of the proposed method and configured approaches [81, 80] by performing NC value. The results indicate that our technique received 0.9977 and 0.9978 for NC for the Median filter and JPEG Compression attacks taken into consideration.

Table 5.6: PSNR values in comparison to other methods

Different Images	PSNR[81]	PSNR[109]	PSNR of proposed method
Barbara	32.82	26.86	41.13
Boat	30.13	NA	42.36
Lena	30.00	31.06	43.79

Table 5.6 shows the imperceptibility of the proposed method and former methods [81, 109] by executing the PSNR value. The results show that the proposed technique obtained a maximum PSNR value of 43.79 dB for image Lena. According to the result, comparing the suggested method [81, 109] to existing ones, it offers improved imperceptibility.

Table 5.7: Visibility of watermarked images at different gain factor [18]

Gain Factor value	visibility of the watermarked image
0.001	Outstanding visibility
0.01	Very well visibility
0.05	Fine visibility
0.1	Satisfactory visibility
0.2	Unsatisfactory visibility
0.5	Extremely poor visibility

According to Table 5.7, the visibility of watermarked images is adequate at the gain factor of 0.5 from subjective evaluation.

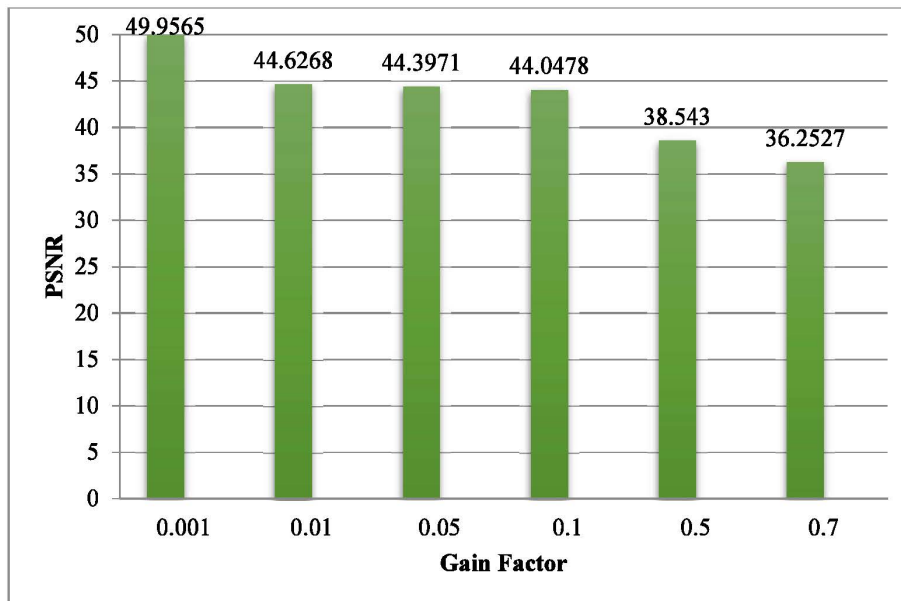


Figure 5.3 PSNR value against the unique gain value

The PSNR reading at various gain factors is depicted graphically in Figure 5.3. The PSNR values between the recommended procedure and the existing approach are shown in Figure 5.4.

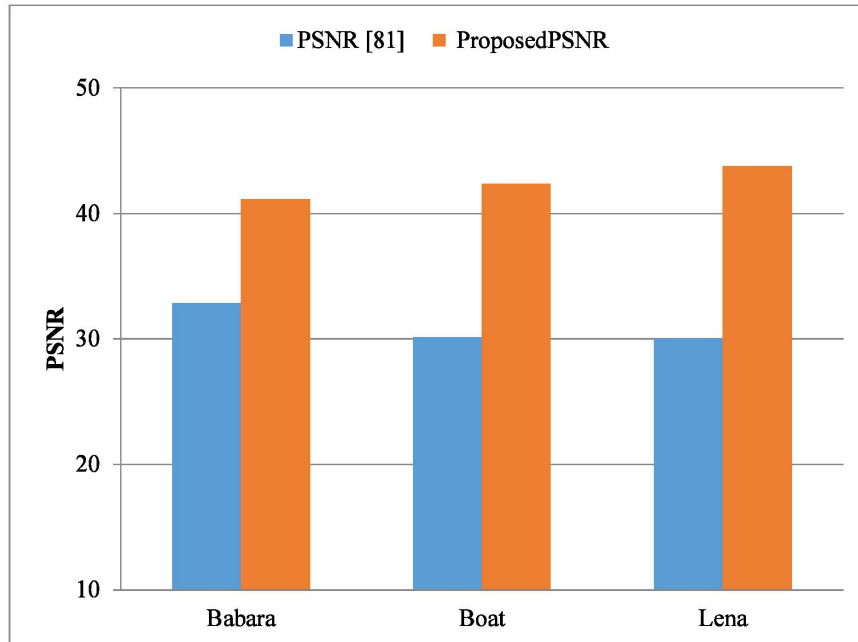
















Figure 5.4 Compared PSNR values

Table 5.8 represents the NC value for recovered watermark images for different images at different gain values. Therefore, the max NC value obtained 0.9991 for salt and pepper attack, and the minimal NC value is 0.9473 for the Gaussian noise attack.

Table 5.8: NC value for attacked and extracted images

Different Attacks	Attacked image	Achieved NC value	Extracted watermark image
Salt and pepper (0.001)		0.9987	

Salt and pepper (0.1)		0.9803	
Gaussian noise attack (0.001)		0.9914	
Gaussian noise attack (0.01)		0.9473	
Median Filter (3 × 3)		0.9978	
JPEG (60) compression		0.9991	
Shearing		0.9723	

A robust and secure watermarking using Arnold transformation in the wavelet domain is developed in this chapter. This method uses SVD, BEMD and DWT is used to enhance an image's resolution and decrease the size without affecting the image's quality. Therefore, the fusion of DWT and SVD can be employed to provide visual quality and robustness. The less fragile and strong frequency bands are decomposed using BEMD to identify the optimal frequency coefficients for the host image. By pixel-scrambling an image using the Arnold transform, the algorithm's security is improved. In this presented methodology, the outcomes

depict excellent strength, visible quality, and privacy against different attacks. This also develops outstanding implementation compared to other existing techniques. In addition, this described method has capability in the fields of texture segmentation, image enhancement, remote sensing, and medical image analysis. Future research will concentrate on increasing the security of the suggested method while keeping costs low.

L Singh, P. K. Singh and J. Sidhu, "Robust and secure watermarking method through BEMD, SVD and Arnold transform in wavelet domain", *International Journal of System Assurance Engineering and Management*, Springer, 1-13, 2022.

CHAPTER 6

ROBUST WATERMARKING APPROACH USING BEMD IN WAVELET DOMAIN

This chapter describes a watermarking methodology using BEMD established in the wavelet domain for ownership validation. This technique employs DWT as well as BEMD to invisibly embed a watermark into the innovative data. The researcher has shown that BEMD and watermarking together provide a significant visual appearance that is superior to other decomposition methods. The BEMD is employed to disintegrate the picture from the weak frequency to the highest strong frequency bands. The results of the experiment demonstrate that the PSNR value exceeds 40 dB in the absence of each and every attack and is robust for various attacks. Additionally, a performance evaluation of the proposed method with other equivalent methodologies indicates that the presented method is establishing better outcomes against different attacks.

6.1 Introduction

The digital watermarking approach is used to establish ownership verification and copyright protection. Many multimedia formats, including text, music, video, and images, can be employed in this process. To achieve the desired results, digital watermarks are embedded in multimedia content and extracted from it using a variety of techniques. Depending on the applications being employed, digital watermarking algorithms are classified. However, watermarking has some fundamental properties, including the strength of the watermark, visible quality, privacy, document payload, delicateness, computational rate, and encoding capacity [26]. In order to examine the not-linearly and inactive signal, the empirical mode decomposition method is first proposed. It generates the auxiliary to ordinary time-frequency techniques such as wavelet analysis and instantaneous Fourier transform. Intrinsic mode functions (IMF) are the primary purpose of empirical mode decomposition (EMD), which is formed via the destruction of signals. It is employed to display the signal's rapid to modest oscillations [113]. Further, Bi-EMD or BEMD is generated with the help of EMD. When BEMD is used in combination with watermarking, the visual quality is significantly increased than other decomposition methods. One of the well-known methods used in watermarking is called DWT. IMF and residual are the basis of BEMD. As a result, the band

with a great frequency is known as residue (r), while the sub-band with a small frequency is known as IMFs [88, 113, 89].



Figure 6.1 Lena's cover image divided into DWT's sub-bands

Figure 6.1 shows the decomposition of an image using DWT method into different sub-bands. Research has shown that several digital watermarking techniques combine with BEMD for the robustness as well as imperceptibility of the digital content. Here are a few significant methods that are described.

In [26, 113,], BEMD and DWT transform using different fusion algorithms are used in a reversible watermarking method for copyright protection and to improve capacity. In addition, BEMD employs to choose one from the most robust (IMFs) to the least robust (residue). The residual component is employed to insert a robust watermark that increases robustness with respect to geometric and non-geometric attacks. Several signals known as bi-dimensional intrinsic mode functions (BIMFs) are used to decompose BEMD. In this method, a group of local maxima or minima points are interpolated in two dimensions. The results of the experiment demonstrate that BIMFs have high visual quality and high speed. The BEMD approach is used to produce a blind and invisible watermarking technology [88]. This method includes BEMD on the encoding and extraction of the watermark with spread spectrum (SS) and code division multiple access (CDMA). However, the spread spectrum is used for the encoding in the wavelet domain, and the watermark image is separated into a 2-level BEMD. This method's output showed that it was robust against noise and attacks and had strong imperceptibility.

An efficient SVD method is suggested in [114] to improve the capacity and invisibility of the image during embedding process. In [89], it was recommended to use a watermarking method found on the LWT, DWT, as well as Arnold transform. This technique decomposes the original and watermark data using LWT and DWT, respectively. The high-frequency section of the DWT watermark is modified by the small frequency of LWT information of the input data. Arnold transforms further scrambled the encoded watermark before hiding it in the image's minimum important portions of the watermarked image.

In [115], DWT-DCT as well as SVD is used to invisibly combine the watermark image into the input data. For the purpose of authenticating health data, the watermarked image is further scrambled by chaotic encryption. This approach is imperceptible as well as robust against dissimilar attacks according to subjective and objective examination. In [29], in order to provide resistance against multiple attacks, unseen and visible watermarking techniques integrating DWT, SVD, as well as BEMD were introduced. This technique combines DWT, and SVD for increased robustness to attacks employing the encoding and recovery of watermarks. This outcome revealed that the PSNR is greater than 40 dB in the absence of the attacks. The author of [116] proposes a method for bi-directional empirical mode decomposition with dynamic watermarking. The source image gets split up into a number of IMFs and residues during this procedure. Therefore, the human visual system (HVS) is employed by IMFs and creates a logo image that is subsequently merged with the original picture. The findings demonstrated that this method has better robustness and imperceptibility than the DCT-based method. This technique has enhanced the fused image's visual quality and produces balanced local and tonal enhancement.

In [117], A non-blind watermarking technique found on DWT was recommended for patent defense and document certification purposes. 2D-DWT manages the embedding and extraction of watermarks to make the process easy. This method's PSNR measurement is higher than 50 dB, and it shows excellent robustness against geometric and comparison attacks. The use of bi-directional mode decomposition in digital image watermarking was suggested in [118] for copyright protection. In contrast to previous methodologies, BEMD provides a superior visual quality in this paper. The experiment findings indicate that the recommended strategy is the only feasible method. In [27], an invisible image watermarking utilizing clustering as well as BEMD algorithms were presented. This method uses clustering and BEMD to enhance the visible quality and strength with respect to attacks throughout the watermark encoding and

decoding process. The strong watermarking system found on DWT, as well as SVD in RGB color area for improved robust w.r.t attacks, was reported in [119]. This proposed method embeds and extracts data using the DWT-SVD algorithm. However, the host image is split into 3 bands, R, G, and B. Moreover, the R band is encoded using a privacy key and a hidden watermark. During the extraction phase, the watermarked image is separated into all of those colors, and then the R-plane can be used for subsequent processing. This approach is highly resistant to attacks from noise, Gaussian, average, and motion. In order to greatly enhance the results, [82] employs redundant discrete wavelet transform (RDWT) rather than DWT in the NSCT domain. Authors in [120] offered a DCT-based watermarking method employing colored images. By fusing LWT-DCT and BCH error-correcting code, the method also uses reliable, distortion-controlling watermarking at a low level of complexity.

This chapter develops a strong watermarking method found in BEMD and DWT domains. The following is the work's main contribution.

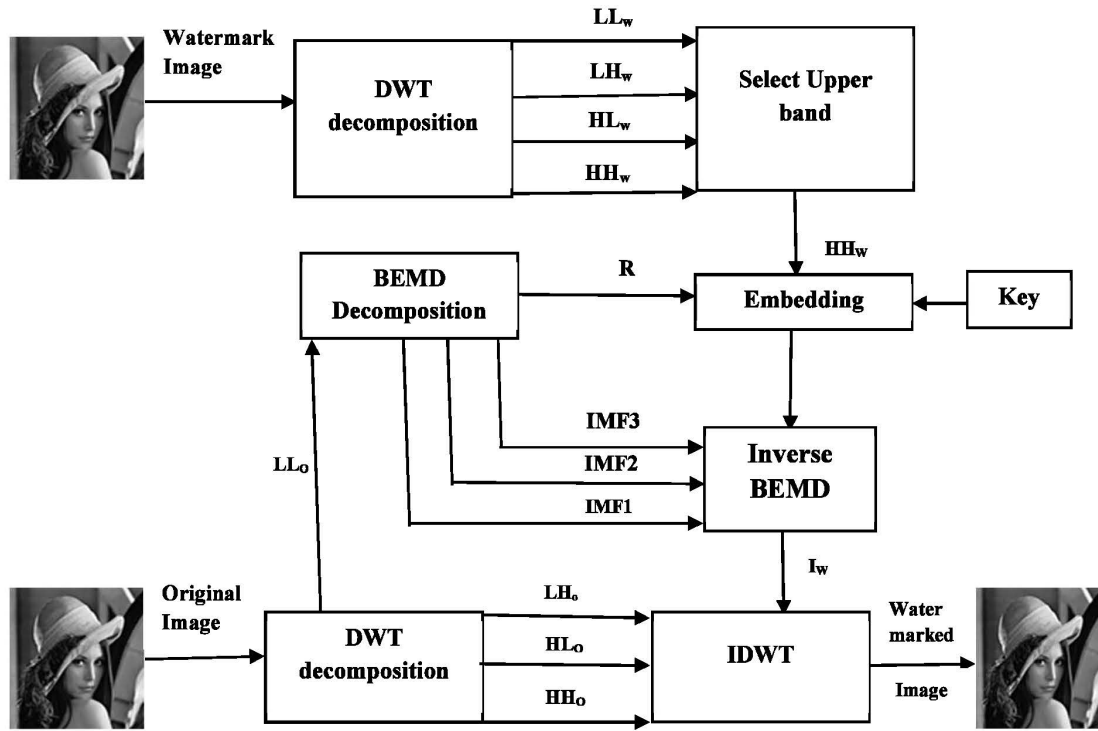
Increased Robustness: The proposed approach increases robustness by combining two techniques. Results indicate that the “NC value” is higher than [26].

Enhanced Imperceptibility: The imperceptibility of the procedure is determined by the PSNR. Moreover, Joshi et al.'s [121] PSNR values are lower than the proposed method.

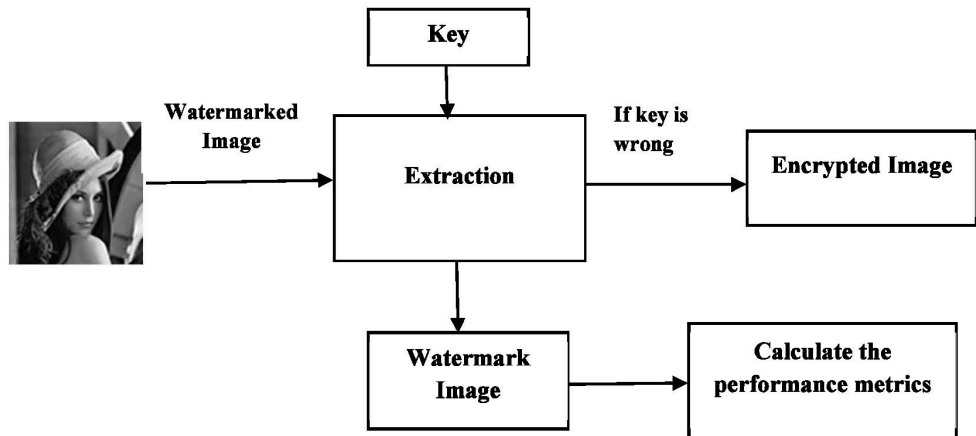
Include Key: Throughout the embedding and extraction procedures, the digital information is validated using a unique key.

6.2 The Proposed Method

In this work, initially, the cover and watermark data are first transformed into distinct frequency components using DWT. The LL sub-frequency of the DWT source data is transformed using the HH watermark components. The strength and visible quality evaluation of our technique are improved by choosing the LL sub-frequency of the input and HH sub-frequency of the watermark image, respectively. An average section of the cover image maintains the max information of the image in LL depiction [121, 122]. With the purpose of enhancing the privacy of the embedding and extraction processes, cypher keys are also produced using the DWT technique. The high-strength and less fragile frequency bands are also decomposed using BEMD. Figure 6.2 depicts the whole process used in our scheme.



(a)



(b)

Figure 6.2: BEMD-based watermark (a) Encoding and (b) Recovery Process

6.2.1 Algorithm for watermarking embedding

Start:

Variable declaration

2nd level DWT coefficient of original: $[LL_o, LH_o, HL_o, HH_o]$

DWT coefficient of watermark: $[LL_w, LH_w, HL_w, HH_w]$

Privacy Key: K

BEMD factor for decomposition: IMF1, IMF2, IMF3, residue

Watermarked image: WMimg

Source image after decomposition: DWTOimg

Step 1: Input and watermark the image

$I \rightarrow$ Host Image (512×512)

$I_w \rightarrow$ Watermark Image (512×512)

Step 2: Execute 2nd level DWT on host image

$DWT(I, Haar) \rightarrow [LL_o, LH_o, HL_o, HH_o]$

Step 3: Execute 2nd level DWT on the watermark image

$DWT(I_w, Haar) \rightarrow [LL_w, LH_w, HL_w, HH_w]$

Step 4: Choose the lowest sub-band and use BEMD decomposition during embedding

$BEMD \rightarrow BEMD(LL_o)$

Step 5: Compute the IMF and residue by BEMD.

$BEMD(LL_o) \rightarrow R$

Step 6: For watermark Image

$DWT(I_w) \rightarrow S1$

Step 7: Image watermarking encoding

$S = R + \alpha * S1$ where α = gain factor

Step 8: Achieve the watermark image

$Imw = IBEMD(S, IMF1, IMF2, IMF3)$

// After applying the embedding process, further (IDWT) is performed to the LH_o , HL_o , and HH_o with the IBEMD.

$WMimg = IDWT(Imw)$

Step 9: Create the privacy key by the X-OR cypher algorithm.

$Key \rightarrow K$

end;

6.2.2 Algorithm for watermarking recovery

The steps for extracting a watermark are as follows:

Start:

Step 1: Watermark image extraction procedure

$EWMImg \rightarrow ExtWMIImg$

Step 2: The extracted image is converted using DWT

$(ExtWMIImg, Haar) \rightarrow [LL_w, LH_w, HL_w, HH_w]$

Step 3: Apply DWT on LL_w

$DWT(LL_w) \rightarrow Sw$

Step 4: Recovered the embedded watermark

$$Sr = \frac{Sw - r}{\alpha}$$

Where α =gain factor

Step 5: Apply a secret key for the security

$Key \rightarrow K$

End;

6.3 Experimental Result and Evaluation

MATLAB version 2013 and the size of the cover Lena image and watermark Lena image of 512×512 pixels were utilized for testing purposes to assess the strength of the suggested work. Figure 6.3 (i) displays “Lena” as a host, and (ii) demonstrates the image as a watermarked picture. (iii) and (iv) denote the watermarked image against “salt & pepper attack and Gaussian attack”, respectively. Figure 6.3 (v) and (vi) display the watermarked image against “rotation attack and shearing attack”, respectively. Figure 6.4 demonstrate a representative image of various cover images that can be identified by their different names – “Lena”, “Barbara”, “Baboon”, “Tank”, and “Cameraman”.





Figure 6.3 (i) Host image “Lena” (ii) Watermarked image (iii) The watermark image against “salt and pepper attack” (iv) the watermark image against “Gaussian attack” (v) the watermark image against “2° rotation attack” (vi) the watermark image against “shearing attack”

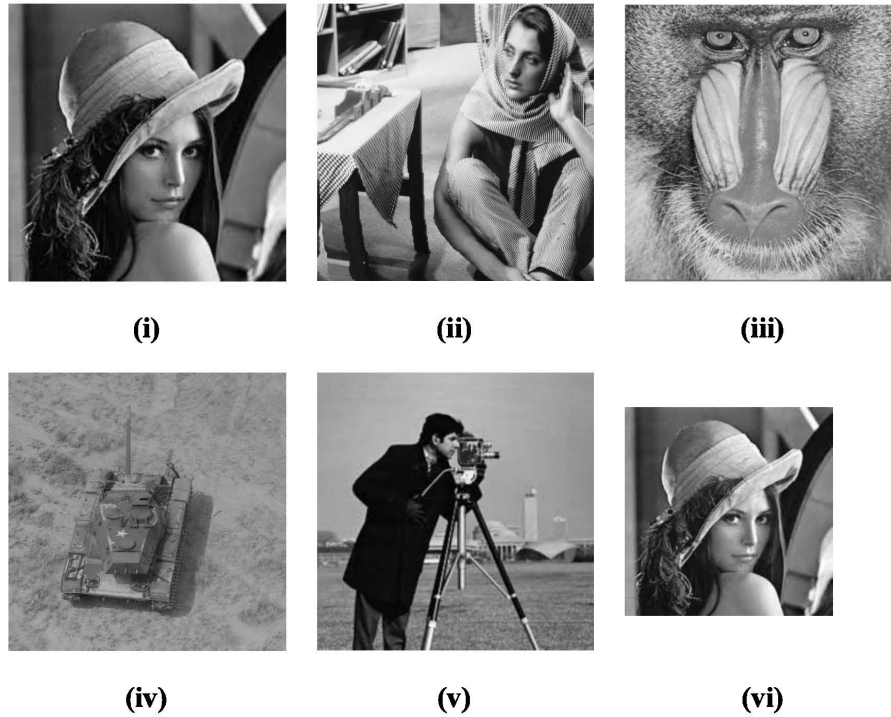


Figure 6.4 The host image of (i) “Lena” (ii) “Barbara” (iii) “Baboon” (iv) “Tank” (v) “cameraman” (vi) the “watermark image”

The performance of our method is evaluated using common measures like PSNR and NC. Chapter 1 provides details regarding the metric under examination.

Table 6.1: Values of PSNR and NC at various gain factors

Distinct Gain Factor	PSNR value (in dB)	NC value
0.001	41.7397	0.9244
0.005	41.6996	0.9248
0.01	41.6497	0.9253
0.05	41.2497	0.9293
0.1	40.7497	0.9343

The results in terms of the standard metric are provided in Table 6.1-Table 6.7. Table 6.1 depicts the PSNR and NC values (without any attacks) of our method at the varying gain and found that the proposed value of PSNR and NC is higher 40 dB and 0.9422, respectively.

Table 6.2 PSNR and NC values for distinct input images

Different Image	PSNR (in dB)	NC
Baboon	41.7397	0.9244
Cameraman	41.7396	0.9245
Tank	41.7397	0.9244
Lena	41.7395	0.9248
Barbara	41.7396	0.9245

NC as well as PSNR results for distinct images at gain=0.001 are listed in Table 6.2. It is clear that the highest NC and PSNR results are obtained as 0.9248 for Lena and 41.7397 dB for the baboon and tank, respectively.

Table 6.3 Values of PSNR and NC for various non-geometric attacks

Different Attacks	Noise Density	PSNR (in dB)	NC
	0.0001	39.2915	0.9508
	0.0005	39.2888	0.9508

Salt & Pepper	0.01	39.2060	0.9517
	0.05	38.8036	0.9557
	0.1	38.3139	0.9607
	0.5	35.0049	0.9942
JPEG compression	10	30.8473	0.9893
	50	31.2690	0.9843
	90	31.5627	0.9810
Gamma Correction		34.0019	0.9537
Median Filter		33.9094	0.9556
Gaussian attack	0.0001	39.2908	0.9508
	0.0005	39.2863	0.9509
	0.01	39.1709	0.9521
	0.05	38.8567	0.9554
	0.1	38.4890	0.9592

However, table 6.3 demonstrates PSNR and NC results for various geometrical and non-geometrical images. It can be detected that the highest “PSNR” and “NC” values are 39.2915 dB and 0.9942 for salt & pepper, respectively. However, PSNR values are poor for JPEG, Gamma correction and Median filter.

Table 6.4 PSNR and NC values acquired from various attacks

Distinct Attacks	Noise Density	PSNR (in dB)	NC
Rotation	1°	33.7598	0.9562
	3°	33.2282	0.9619
	5°	32.8739	0.9658

Scaling	(2, 0.5)	34.0516	0.9531
Shearing		34.0019	0.9537

Table 6.4 depicts the execution of the developed scheme under distinct attacks Rotation, Scaling and Shearing attacks at different noise densities. It is evident that the best value of PSNR and NC are higher at 32 dB and 0.9531, respectively, for distinct attacks.

Table 6.5 PSNR and NC values for various bands at various gain factors

Gain Factor value	“LL band”		“HL band”		“LH band”		“HH band”	
	PSNR (in dB)	NC	PSNR (in dB)	NC	PSNR (in dB)	NC	PSNR (in dB)	NC
0.001	41.7356	0.9244	41.7222	0.9246	41.7315	0.9244	41.7346	0.9244
0.005	41.6956	0.9248	41.6821	0.9250	41.6915	0.9248	41.6947	0.9249
0.01	41.6457	0.9253	41.6321	0.9255	41.6415	0.9253	41.6454	0.9254
0.05	41.2456	0.9293	41.2321	0.9295	41.2415	0.9293	41.2455	0.9293
0.1	40.7456	0.9343	40.7322	0.9345	40.7415	0.9343	40.7447	0.9345

Initially, we introduced HH constituents of the DWT watermark to the LL sub-bands of the DWT original data. However, the LL sub-bands of the DWT novel data have been further modified using the remaining DWT band of the watermark image. It is displayed in Table 6.5. Based on Table 6.5, the utmost PSNR and NC values for the LL band are 41.7356 dB (gain value = 0.001), and NC value for HH band is 0.9345 (gain value = 0.1), respectively. However, the HH band's lowest PSNR and NC are 40.7447 (gain value = 0.1), and the LL band's lowest values are 0.9244 (gain value = 0.001), respectively.

Table 6.6: NC values compared at various noise densities

Distinct Attack	Noise Density	NC [26]	NC of proposed work
Rotation	45°	0.979	0.982
Gamma Correction	0.6	0.995	0.962
Salt & Pepper	0.5	0.993	0.994

In Tables 6.6 and 6.7, we have contrasted the outcome of our technique with LWT-BEMD and DWT-CDMA [26, 88], respectively. Table 6.6 represents the robustness of the proposed method and former approaches [26] by performing NC value. The result clearly states that our method achieved an approximation 1 score for NC for most of the considered attacks. However, the minimum NC offered by our method is 0.962 against Gamma Correction.

Table 6.7: Comparative analysis of PSNR values

Different Images	NC	PSNR (in dB) value [88]	PSNR of the proposed value
Lena	0.9244	37.03	41.7357
Mandrill	0.9244	36.09	41.7356
Ships	0.9243	33.90	41.7357
Goldhill	0.9242	37.88	41.7356

Table 6.7 represents the imperceptibility of the proposed method and former approaches [88] by performing PSNR value. The result clearly states that our method achieved above 40 dB for PSNR for different images.

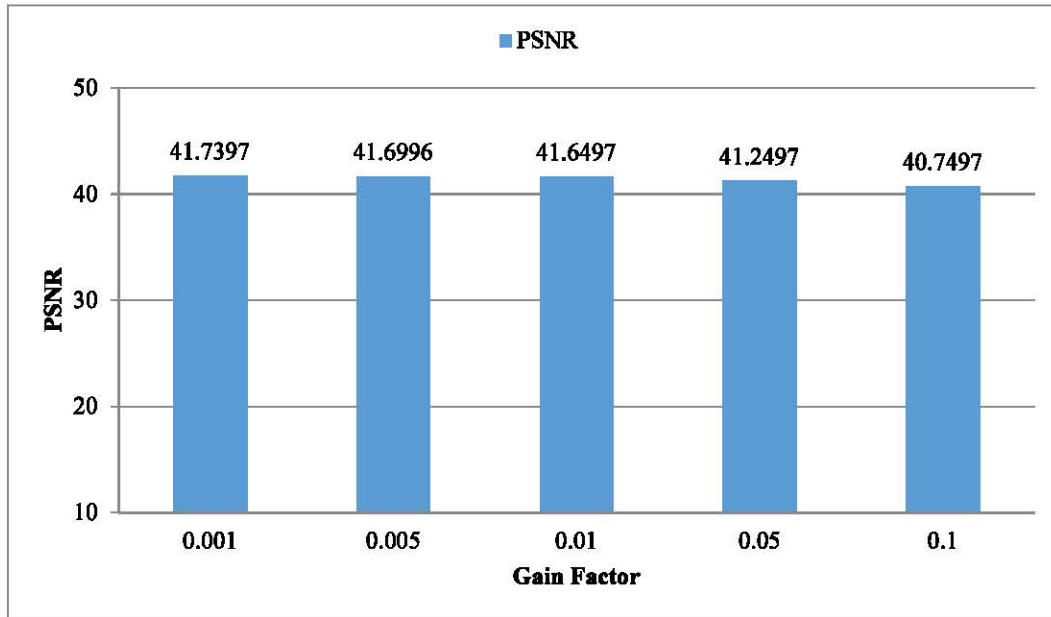


Figure 6.5 PSNR value at distinct gain factor

Figure 6.5 shows a visual depiction of the PSNR values obtained using the DCT-PSO and BEMD methods at various gain factors.

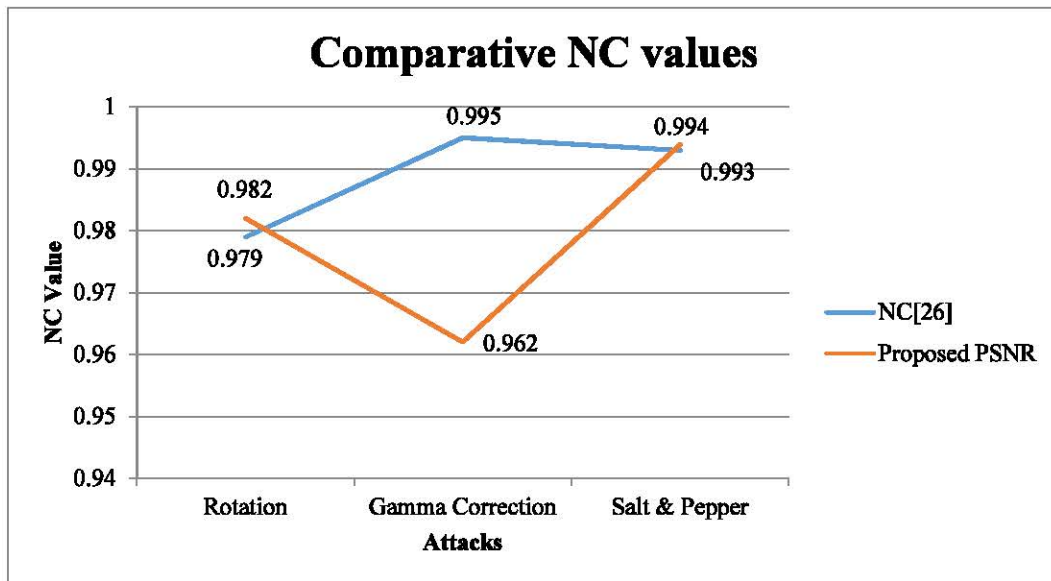


Figure 6.6 Comparative analysis of NC

Figure 6.6 and Figure 6.7 compares NC and PSNR values between the proposed strategy and the existing method [26, 88].

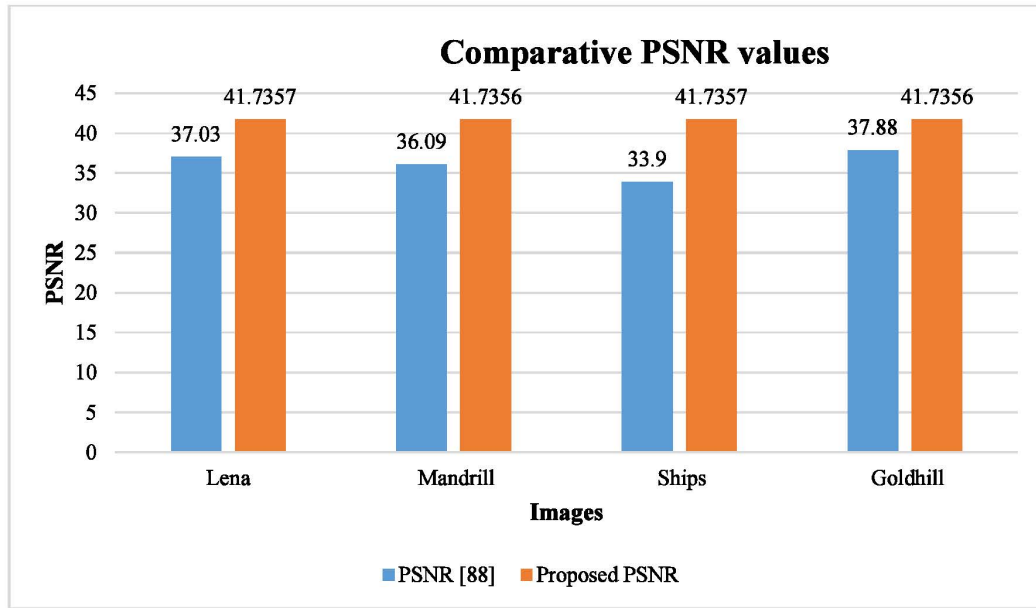


Figure 6.7 Comparative analysis of PSNR

Figure 6.8 displays the images for the execution of this technique previously and afterwards embedding the watermark, original and extracted watermark. The rising value of NC can be used to determine the robustness of the system [123].

Based on analysis of the proposed technique, it is determined that in comparison to other existing techniques, this scheme has the highest robustness against the most difficult attacks, such as rotation, gamma correction, salt and pepper of the image and other processing procedures that are most frequently used.

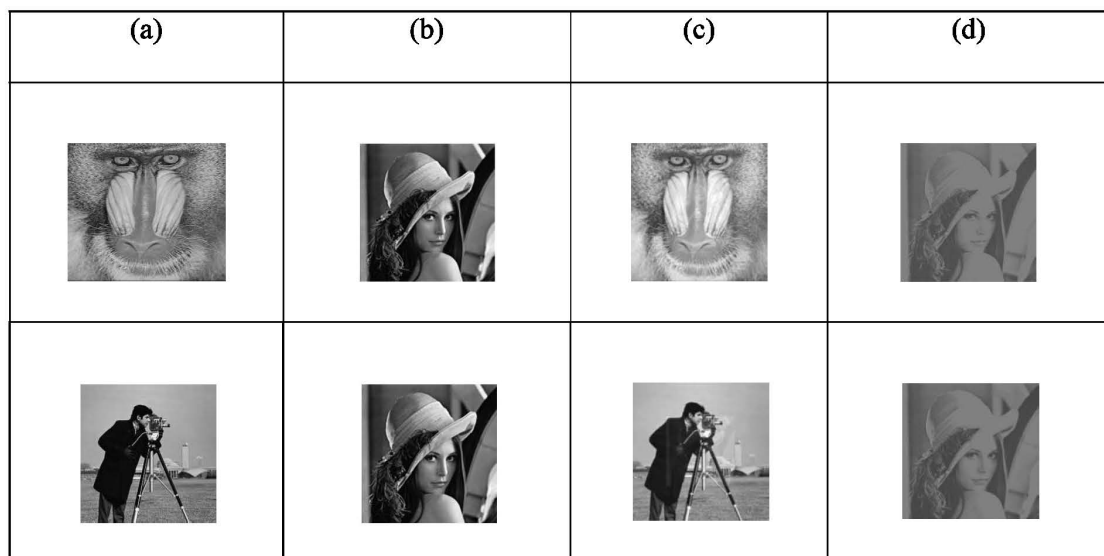




Figure 6.8 Pictures (a) Host (b) Watermark (c) Watermarked and (d) Recovered watermark

In this chapter, a strong digital watermarking procedure with DWT, as well as the BEMD approach is offered. This method makes use of various features of DWT and BEMD approaches. However, the properties of DWT are used to decompose the image into any dimension and reconstruct it without any data reduction. Moreover, the use of a cipher key increases the security of this technique. The PSNR and NC values obtained are definitely satisfactory when considering all factors. The results of the suggested algorithm demonstrate high robustness with respect to attacks. The research analysis demonstrates good visible quality in comparison to previous research as well as successful recovery of a hidden watermark. Without any attacks, we were able to acquire a PSNR value of 40 dB or more.

L Singh, A. Singh and P. K. Singh, "A robust image watermarking through bi-empirical mode decomposition and discrete wavelet domain" *Proceedings of ICETIT-2019*.

CHAPTER 7

CONCLUSION AND FUTURE DIRECTIONS

In this thesis, we have offered several improved wavelet-domain digital watermarking techniques. Therefore, it is difficult to create a watermarking scheme that produces an optimal balance among these factors, and the aim of this study was to provide some watermarking methods that produce the best trade-off among key performance parameters.

Chapter 1 begins with an introduction to digital watermarking and a study of a number of robust and secure methods used for prospective applications. Also, crucial uses and possible properties of digital watermarking as well as different techniques of spatial as well as transform schemes and key metrics, are discussed. And chapter 2 describes the review of the existing techniques.

Chapter 3 presented an improved PSO-based robust and imperceptible digital watermarking for concealing scrambled watermark images in the BEMD-DCT domain. The main focus of the technique was to improve robustness at acceptable imperceptibility. The security key is used to provide an extra level of security. By applying the PSO optimization technique on the input image and watermarked image, complex and multidimensional searches can be done and preserve the visibility of the image. Performance of the technique is measured for various gains, different cover images and attacks. In addition, the Robustness (NC value) of the proposed method is up to 0.999.

Chapter 4 discussed SVD, DCT, BEMD as well as PSO in the wavelet domain as a robust watermarking method. This chapter's objective was to enhance security, robustness, and imperceptibility with less distortion. Furthermore, Five alternative cover images, "Haar wavelet filters", and numerous attacks are used to critically examine the approach. The Robustness (NC value) of the proposed method is up to 0.9999.

Chapter 5 presented encryption based watermarking in the DWT domain. This chapter's primary goal was to use the Arnold transform to improve digital document security while keeping costs down. An overall observation of the approach revealed that it beats other comparable approaches in terms of safety, robustness, lack of distortion, and good

imperceptibility. The Robustness (NC value) and SSIM of the offered method are up to 0.9999 and 1, respectively.

In Chapter 6, we developed an improved DWT- BEMD-based watermarking technique. In our technique, The cover image's selected sub-bands contain watermark data. The image is divided using the BEMD from the least delicate to the highly robust frequency bands. The method's performance was superior to that of other competing approaches according to result demonstrations which also proved that it is robust against different attacks. The Robustness (NC value) and imperceptibility (PSNR) of the proposed approach are up to 0.9343 and 40 dB, respectively.

Based on the findings of experiments, it can be demonstrated that the PSNR, NC, and SSIM are highly dependent on the gain value, amount of embedded data and noise variations. NPCR and UACI evaluate the encryption algorithm's robustness, which is totally dependent on secure force encryption methods.

It's interesting to observe that the outcomes of our improved methods are appropriate for digital data security in a variety of applications, including medical applications and copyright protection. In addition, modern technologies like artificial intelligence, machine learning, deep learning, blockchain, and big data can be used to create watermarking algorithms that are more effective for real-world uses. We will also enhance the suggested method to include additional multimedia formats like text, audio and video.

REFERENCES

- [1] Singh A. K., Kumar B., Singh S. K., Ghrera S. P., & Mohan A., “Multiple watermarking technique for securing online social network contents using back propagation neural network”, *Future Generation Computer Systems*, volume: 86, pp: 926-939, 2018.
- [2] Dagadu JC, Li J., “Context-based watermarking cum chaotic encryption for medical images in telemedicine applications”, *Multimedia Tools and Applications*, pp: 1–24, 2018.
- [3] Kaur G., Kaur K., “Digital watermarking and other data hiding techniques”, *International Journal of Innovative Technology and Exploring Engineering*, No. 2, Volume: 5, pp:181–183, 2013.
- [4] Singh AK., “Some new techniques of improved wavelet domain watermarking for medical images”, PhD thesis, Department of Computer Engineering, NIT Kurukshetra, 2015.
- [5] Bhowmik D., Oakes M., Abhayaratne C. “Visual attention-based image watermarking”, *IEEE Access*, volume:4, pp:8002–8018, 2016
- [6] Singh AK., Kumar B., Dave M., Ghrera SP and Mohan A “Digital Image Watermarking: Techniques and Emerging Applications”, *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*, IGI Global, USA, pp: 246–272, 2016.
- [7] Mohanty SP, “Digital watermarking: A tutorial review”, 1999
- [8] Mohanty SP, Sengupta A, Guturu P, Kougiannos E, “Everything you want to know about watermarking”, *IEEE Consumer Electronics Magazine*, Vol. 6 No:3, pp:83–91, 2017.
- [9] Tanha M, Torshizi SD, Abdullah MT, Hashim F., “An overview of attacks against digital watermarking and their respective countermeasures”, In proc. of 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, IEEE, Kuala Lumpur, Malaysia, pp:265–270, 2012.
- [10] Singh AK, Dave M, Mohan A, “Hybrid technique for robust and imperceptible image watermarking in DWT–DCT–SVD domain”. *National Academy Science Letters*, Vol. 37, No. 4, pp: 351–358, 2014.
- [11] Singh AK, Kumar B, Singh G, and Mohan A “Medical image watermarking: techniques and applications”, pp.1-263, Springer, 2017.
- [12] Hore A., & Ziou D., “Image quality metrics: PSNR vs. SSIM”, In 2010 20th international conference on pattern recognition IEEE, pp: 2366-2369, Aug 2010.
- [13] Singh L., Singh A. K., & Singh P. K., “Secure data hiding techniques: A survey. *Multimedia Tools and Applications*”, Volume: 79, pp: 1–21, 2018.
- [14] Su Q, Chen B, “Robust color image watermarking technique in the spatial domain” *Soft Computing*, volume: 22, No: 1, pp: 91–106, 2018.

- [15] Das C, Panigrahi S, Sharma VK, Mahapatra KK ,” A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation”, *AEU-International Journal of Electronics and Communications* , vol.68, No:3, pp:244–253, 2014
- [16] Kalra GS, Talwar R, Sadawarti H ,”Adaptive digital image watermarking for color images in frequency domain”. *Multimedia Tools and Applications*, Vol. 74 no:17, pp:6849–6869, 2015.
- [17] Chen YY, Chi KY, “Cloud image watermarking: high quality data hiding and blind decoding scheme based on block truncation coding”, *Multimedia Systems*, 2017.
- [18] Chang IC, Hu YC, Chen WL, Lo CC, “ High capacity reversible data hiding scheme based on residual histogram shifting for block truncation coding”, *Signal Process*, vol.108, pp:376–388, 2015.
- [19] Chen J, Hong W, Chen TS, Shiu CW, “Steganography for BTC compressed images using no distortion technique”, *The Imaging Science Journal*, vol.58, no-4, pp:177–185, 2010
- [20] Hong W, Chen TS, Shiu CW., “Lossless steganography for AMBTC-compressed images”, In *Congress on Image and Signal Processing*, vol. 2,pp:13–17, 2008.
- [21] Ou D, Sun W, “High payload image steganography with minimum distortion based on absolute moment block truncation coding”, *Multimedia Tools and Applications*, vol. 74 no: 21, pp: 9117–9139, 2015.
- [22] Hossain MS, Muhammad G, “Cloud-assisted industrial internet of things (iiot)-enabled framework for health monitoring” *Computer Network*, vol.101, no-4, pp:192–202, 2016.
- [23] Gordy JD, Bruton LT.,“ Performance evaluation of digital audio watermarking algorithms”, In: *Proc. Of the 43rd IEEE Midwest Symposium on Circuits and Systems*, vol.1, pp: 456–459, 2000.
- [24] Yuan Z, Su Q, Liu D, Zhang X, “A blind image watermarking scheme combining spatial domain and frequency domain”, *The Visual Computer*, 2020.
- [25] Hu WC, Chen WH, Yang CY, “Robust image watermarking based on discrete wavelet transform discrete cosine transform-singular value decomposition” ,*Journal of Electronic Imaging*, vol.21, No.3, 2012.
- [26] Abbas NH, Ahmad SM, Parveen S, Wan WA, Ramli AR, “Design of high performance copyright protection watermarking based on lifting wavelet transform and bi empirical mode decomposition”, *Multimed Tools Appl*, vol. 77, no:19, pp:24593–24614, 2018.
- [27] Taghia J, Doostari MA, Taghia J, “An image watermarking method based on bi dimensional empirical mode decomposition”, *Congress on Image and Signal Processing, IEEE*, Vol. 5, pp.: 674–678, 2008
- [28] Sabri A, Karoud M, Tairi H, Aarab A, “Image Watermarking Using the Empirical Mode Decomposition”, *International Conference: Sciences of Electronic, Technologies of Information and Telecommunications*, pp.: 22–26, 2009.

- [29] Amira-Biad S, Bouden T, Nibouche M, Elbasi E , “A Bi-Dimensional Empirical Mode Decomposition Based Watermarking Scheme”, *International Arab Journal of Information Technology ,IAJIT*, vol.12, No.1, 2015.
- [30] Deng MH, Yang F, Wang RT , “Robust Watermarking Algorithm Based on Bi-Dimensional Empirical Mode Decomposition” *Materials Research*, Vol. 204, pp.: 627–631, 2011.
- [31] Khan A, Agrawal P, Sainthiya H , “Bidimensional empirical mode decomposition based image fusion”, *International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE)*, IEEE, pp.: 212–217, 2017.
- [32] Minghui D, Jingbo Z , “Robust image watermarking algorithm against geometric attack based on BEMD”, *International Conference on Computer and Communications Security*, IEEE, pp.: 36–39, 2009.
- [33] Wang X, Hu K, Hu J, Du L, Ho AT, Qin H , “Robust and blind image watermarking via circular embedding and bidimensional empirical mode decomposition”, *Visual Computation*, pp:2201–14, DOI: <https://doi.org/10.1007/s00371-020-01909-2>, 2020.
- [34] Guo J, Zheng P, Huang J, “ Secure watermarking scheme against watermark attacks in the encrypted domain”. *Journal of Visual Communication and Image Representation*, volume: 30, pp: 125–135, 2015.
- [35] Bianchi T, Piva A, Barni M , “Encrypted domain DCT based on homomorphic cryptosystems”, *EURASIP Journal on Information Security*, no. 1, pp:1-12, 2009
- [36] Haddad S, Coatrieux G, Cozic M, Bouslimi D, “Joint watermarking and lossless JPEG-LS compression for medical image security”, In *Proceedings of the International Conference on Watermarking and Image Processing* , vol. 38, no:4, pp:198–206, 2017.
- [37] Caldelli R, Filippini F, Barni M, “ Joint near-lossless compression and watermarking of still images for authentication and tamper localization”. *Signal Process Image Communication*, vol. 21, no:10, pp:890–903, 2006.
- [38] Fridrich J, Goljan M, Chen Q, Pathak V, “Lossless data embedding with file size preservation In *Security, Steganography, and Watermarking of Multimedia Contents VI*, vol. 5306, pp. 354-365. SPIE, 2004.
- [39] Seenivasagam V, Velumani R, “A QR code based zero-watermarking scheme for authentication of medical images in teleradiology cloud”, *Computational and mathematical methods in medicine*, pp:1–16, 2013.
- [40] Hsu CS, Hou YC, “Copyright protection scheme for digital images using visual cryptography and sampling methods”. *Optical Engineering* , vol.44, no. 7 , pp:077003-077003, 2005.
- [41] Kim J, Kim N, Lee D, Park S, Lee S, “Watermarking two dimensional data object identifier for authenticated distribution of digital multimedia contents”. *Signal Process Image Communication*, vol. 25, no-8, pp559–576, 2010.

- [42] Rawat S, Raman B , “A blind watermarking algorithm based on fractional Fourier transform and visual cryptography”, *Signal Process*, vol. 92, no-6, pp:1480–1491, 2012.
- [43] Wang MS, ChenWC, “A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography”, *Computer Standards & Interfaces*, vol.31, no-4, pp:757–762, 2009.
- [44] Dharwadkar NV, Amberker BB , “Watermarking scheme for color images using wavelet transform based texture properties and secret sharing”, *International Journal of Signal Processing*, vol. 6, no-2, pp:93–100, 2010
- [45] Hsieh SL, Tsai IJ, Huang BY, Jian JJ , “Protecting copyrights of color images using a watermarking scheme based on secret sharing and wavelet transform” *Journal of Multimedia* , vol.3, no-4, pp:42–49, 2008.
- [46] Chang CC, Chen KN, Lee CF, Liu LJ, “A secure fragile watermarking scheme based on chaos-andhamming code”, *Journal of Systems and Software*, vol. 84, no. 9, pp: 1462-1470, 2011.
- [47] Hsu CS, Tu SF, “Probability-based tampering detection scheme for digital images”, *Optics Communications*, no. 9pp: 1737-1743, 2010.
- [48] Lin PL, Hsieh CK, Huang PW, “A hierarchical digital watermarking method for image tampers detection and recovery”. *Pattern Recognition*, vol.38, no-12, pp:2519–2529, 2005.
- [49] Rawat S, Raman B , “A chaotic system based fragile watermarking scheme for image tamper detection”,*AEU-International Journal of Electronics and Communications*, vol. 65,no-10, pp:840–847, 2011.
- [50] Xia Z, Wang X, Zhang L, Qin Z, Sun X, Ren K, “A privacy-preserving and copy-deterrence contentbased image retrieval scheme in cloud computing”, *IEEE Transactions on Information Forensics and Security*, vol.11, pp:2594–2608, 2016
- [51] Zhang J, Xiang Y, Zhou W, Ye L, Mu Y ,(2011) “Secure image retrieval based on visual content and watermarking protocol” *The Computer Journal*, vol.54, no.10 , pp: 1661-1674, 2011.
- [52] Su Q, Chen B,“A novel blind color image watermarking using upper Hessenberg matrix” *AEU International Journal of Electronics and Communications*, vol.78, pp:64–71, 2017
- [53] Golea NE, Seghir R, Benzid R, “ A bind RGB color image watermarking based on singular value decomposition” ,*IEEE/ACS International Conference on Computer Systems and Applications*, Hammamet, Tunisia, pp:1–5, 2010
- [54] Naderahmadian Y, Hosseini-Khayat S, “Fast watermarking based on QR decomposition in wavelet domain” In *proc. of the 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Darmstadt, Germany, pp:127–130, 2010.

- [55] Song W, Hou JJ, Li ZH, Huang L (2011) Chaotic system and QR factorization based robust digital image watermarking algorithm. *J Cent S Univ Technol*, vol.18,no-1,pp:116–124, 2011.
- [56] Su Q, Niu Y, Zou H, Zhao Y, Yao T, “A blind double color image watermarking algorithm based on QR decomposition”, *Multimedia tools and applications*, vol.72, no-1, pp:987–1009, 2014.
- [60] Lei B, Zhao X, Lei H, Ni D, Chen S, Zhou F, Wang T, “Multipurpose watermarking scheme via intelligent method and chaotic map” ,*Multimedia Tools and Applications*, pp:1–23, 2017
- [61] Gupta R, Mishra A, Jain S, “A semi-blind HVS based image watermarking scheme using elliptic curve cryptography”, *Multimedia Tools and Applications*, pp: 1–26, 2017.
- [62] Gupta R, Jain S, Mishra A, “Watermarking system for encrypted images at cloud to check reliability of images”, 1st International Conference on Next Generation Computing Technologies, Dehradun, India, pp:46–49, 2015
- [63] Liu Y, Zhang L, Nie L, Yan Y, Rosenblum DS, “Fortune Teller: Predicting Your Career Path”, In *AAAI* pp:201–207, 2016.
- [64] Mohanty SP, Ramakrishnan KR, Kankanhalli M., “A dual watermarking technique for images”, In *Proceedings of the seventh ACM international conference on Multimedia (Part 2)*, pp:49–51, 1999.
- [65] Patra JC, Phua JE, Bornand C , “A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression” ,*Digital Signal Processing*, vol.20, no-6, pp:1597–1611, 2010.
- [66] Chang CC, Tsai P, Lin CC, “SVD-based digital image watermarking scheme”, *Pattern Recognition Letters* , vol.26, no. 10, pp: 1577-1586, 2005.
- [67] Patra JC, Karthik A, Bornand C, “A novel CRT-based watermarking technique for authentication of multimedia contents” *Digital Signal Processing*, vol. 20, no-2, pp: 442–453, 2010.
- [68] Chang BM, Tsai HH, Yen CY , “SVM-PSO based rotation-invariant image texture classification in SVD and DWT domains” *Engineering Applications of Artificial Intelligence*, vol. 52, pp96-107, 2016.
- [69] Saxena N,Mishra KK, Tripathi A, “DWT-SVD-based color image watermarking using dynamic-PSO”. In *Advances in Computer and Computational Sciences*, Springer, pp. 343–351, 2018.
- [70] Rao VS, Shekhawat RS, Srivastava VK ,”A DWT-DCT-SVD based digital image watermarking scheme using particle swarm optimization”, *Conference on Electrical, Electronics and Computer Science*, pp.1–4, 2012.
- [71] Kaur A, Singh J, “An efficient image watermarking technique using aging leader based particle swarm optimization”, *International Journal of Information Systems & Management Science*, 2018.
- [72] Zhang L, Wei D, “Dual DCT-DWT-SVD digital watermarking algorithm based on particle swarm optimization”, *Multimedia Tools and Applications*, vol.78, No.19, pp.:28003–23, 2019

- [73] Ravi P , “A Novel PSO Algorithm Based on Lossless Image Compression with Optimized DWT”, vol.8, issue.7, pp.: 33–39, 2019.
- [74] Yadav N, Rajpoot D, Dhakad SK, “Optimization of Watermarking in Image by Using Particle Swarm Optimization Algorithm”, 6th International Conference on Signal Processing and Communication (ICSC), IEEE, pp. 85–90, 2020.
- [75] Kang X, Chen Y, Zhao F, Lin G, “Multi-dimensional particle swarm optimization for robust blind image watermarking using intertwining logistic map and hybrid domain”, *Soft Computation*, pp:10561–84, 2020.
- [76] Wang B, Ding J, Wen Q, Liao X, Liu C, “An image watermarking algorithm based on DWT DCT and SVD”, In: *IEEE international conference on network infrastructure and digital content*, pp:1034–1038, 2009.
- [77] Kamble S, Maheshkar V, Agarwal S, Srivastava VK, “DWT-SVD based robust image watermarking using Arnold map”, *International Journal of Information Technology and Knowledge Management*, vol. 5, no. 1, pp: 101-105, 2012
- [78] Ye G, Wong KW, “An efficient chaotic image encryption algorithm based on a generalized Arnold map”, *Nonlinear dynamics*, vol.69, no-4, pp:2079–87, 2012.
- [79] Chen L, Zhao D, Ge F , “Image encryption based on singular value decomposition and Arnold transform in fractional domain” *Opt Communication*, vol. 291, pp:98–103, 2013.
- [80] Zhang Z, Wang C, Zhou X, “Image watermarking scheme based on Arnold transform and DWT-DCT-SVD”, In: *IEEE 13th international conference on signal processing (ICSP)*, pp 805–810, 2016.
- [81] Kumar C, Singh AK, Kumar P , “Improved wavelet-based image watermarking through SPIHT”. *Multimedia Tools and applications*, vol. 79, no-15, pp: 11069–11082, 2020.
- [82] Kumar C, Singh AK, Kumar P, Singh R, Singh S, “SPIHT-based multiple image watermarking in NSCT domain”, *Concurrency and Computation: Practice and Experience*, vol.32, no. 1 , 2020.
- [83] Wang X, Hu K, Hu J, Du L, Ho AT, Qin H , “Robust and blind image watermarking via circular embedding and bidimensional empirical mode decomposition”. *Visual Computing* vol.36, no-10, pp: 2201–2214, 2020.
- [84] Ding W, Ming Y, Cao Z, Lin CT, “A generalized deep neural network approach for digital watermarking analysis”, *IEEE Transactions on Emerging Topics in Computational Intelligence*. Vol. 6, no.3, pp: 613-27, 2021.
- [85] Kavitha RS, Eranna U, Giriprasad MN, “DCT-DWT based digital watermarking and extraction using neural networks”, In *2020 International Conference on Artificial Intelligence and Signal Processing (AISP)*, pp. 1-5, IEEE, 2020.

- [86] Hernandez-Joaquín A, Melendez-Melendez G, Cumplido R, “A secure DWT-based dual watermarking scheme for image authentication and copyright protection”, *Multimedia Tools and Applications*, pp: 1-23, 2023.
- [87] Radha Kumari R, Vijaya Kumar V, Rama Naidu K, “Deep learning-based image watermarking technique with hybrid DWT-SVD”, *The Imaging Science Journal*, pp:1-17, 2023.
- [88] Fkirin A, Attiya G, El-Sayed A, Shouman MA, “Copyright protection of deep neural network models using digital watermarking: a comparative study”, *Multimedia Tools and Applications*, Vol. 81, no.11, pp:15961-75, 2022.
- [89] Nematollahi MA, “A machine learning approach for digital watermarking. *Australian Journal of Multi-Disciplinary Engineering*”, pp:1-1, 2023.
- [90] Ansari, I. A., Pant, M., & Ahn, C. W., “PSO optimized and secured watermarking scheme based on DWT and SVD”. In *International conference on soft computing for problem solving*, pp. 411–424, Springer, 2016.
- [91] Singh AK, Dave M, Mohan A, “Hybrid technique for robust and imperceptible multiple watermarking using medical images”, *Multimedia Tools and Applications*, vol.75 no-14, pp: 8381–401, 2016.
- [92] Ansari IA, Pant M, “Multipurpose image watermarking in the domain of DWT based on SVD and ABC” *Pattern Recognition Letters*, vol. 94 pp: 228-236, 2017.
- [93] Agrwal SL, Yadav A, Kumar U, Gupta SK (2016) Improved invisible watermarking technique using IWT-DCT, 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)IEEE, pp:283–285, 2016.
- [94] Lee Y, Nah J, Kim J, “Digital image watermarking using bi dimensional empirical mode decomposition in wavelet domain”, 11th IEEE International Symposium on Multimedia, pp.: 583–588, 2009.
- [95] Abbas, N.H., Ahmad, S.M.S., Ramli, A.R.B. and Parveen, S, “A multi-purpose watermarking scheme based on hybrid of lifting wavelet transform and Arnold transform”, *Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, IEEE, pp. 1–6, 2016.
- [96] Zear A, Singh AK, Kumar P, “A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine” *Multimedia Tools and Applications*, vol.77, No.4, pp.:4863–82, 2018.
- [97] He Y, Hu Y, “A proposed digital image watermarking based on DWT-DCT-SVD” 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), pp: 1214–1218, 2018.

- [98] Kang XB, Zhao F, Lin GF, Chen YJ , “A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength” *Multimedia Tools and Applications*, vol.77, No.11,pp.:13197–224, 2018.
- [99] Naik K, Trivedy S, Pal AK , “An IWT based blind and robust image watermarking scheme using secret key matrix”. *Multimedia Tools and Application*, vol.77, no-11, pp: 13721–13752, 2018.
- [100] Li D, Deng L, Gupta BB, Wang H, Choi C, “A novel CNN based security guaranteed image watermarking generation scenario for smart city applications”, *Inform Science*, vol. 479, pp:432–447, 2019.
- [101] Savakar DG, Ghuli A, “Robust Invisible Digital Image Watermarking Using Hybrid Scheme”. *Arabian Journal for Science and Engineering*, vol-44, no. 4, pp:3995–4008, 2019.
- [102] Khedr WM, Elsoud MW, “A Novel Blind and Robust Watermarking Technique of Multiple Images”, *International Conference on Computational Science and Computational Intelligence (CSCI)*, IEEE, pp: 595–599, 2019.
- [103] Liu J, Huang J, Luo Y, Cao L, Yang S, Wei D, Zhou R, “An optimized image watermarking method based on HD and SVD in DWT domain”, *IEEE Access*, vol.7,pp:80849–80860, 2019.
- [104] Sinhal R, Ansari IA (2019) A multipurpose image watermarking scheme for digital image protection, *International Journal of System Assurance Engineering and Management*.
- [105] Khare P, Srivastava VK, “A reliable and secure image watermarking algorithm using homomorphic transform in DWT domain”, 2020.
- [106] Jha CK, Kolekar MH ,”Empirical Mode Decomposition and Wavelet Transform based ECG Data Compression Scheme”, *IRBM*, 2020.
- [107] Zhong X, Huang PC, Mastorakis S, Shih FY, “An Automated and Robust Image Watermarking Scheme Based on Deep Neural Networks”, *IEEE Transactions on Multimedia*, pp:1951-1961, 2020.
- [108] Srivastava A, “Performance Comparison of Various Particle Swarm Optimizers in DWT-SVD watermarking for RGB Images”, *Sixth International Conference on Computer and Communication Technology*, pp. 244–250, 2015.
- [109] Singh AK, “Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images”, *Multimedia Tools and Applications*, vol. 76, no-6, pp:8881–900, 2017.
- [110] Liu Y, Tang S, Liu R, Zhang L, Ma Z , “Secure and robust digital image watermarking scheme using logistic and RSA encryption”, *Expert System Application*, vol- 97, pp:95–105, 2018.
- [111] Vaish A, Kumar M, “Color image encryption using MSVD, DWT, and Arnold transform in fractional Fourier domain” *Optik*, vol.145, pp:273–283, 2017.

- [112] Li Y, Gou W, Li B, "A new digital watermark algorithm based on the DWT and SVD", In: International symposium on distributed computing and applications to business, engineering and science, pp 207–210, 2011.
- [113] Yeh MH, "The complex bi-dimensional empirical mode decomposition", Signal Processing, vol.92, no.2, pp: 523-541, 2011.
- [114] Chung KL, Yang WN, Huang YH, Wu ST, Hsu YC, "On SVD-based watermarking algorithm. Applied Mathematics and Computation", Vol.188, No.1, pp:54-57, 2007.
- [115] Thakur S, Singh AK, Ghrera SP, Elhoseny M, "Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications", Multimedia Tools and Applications, pp:1-14, 2019.
- [116] Huang W, Sun Y, "A New Image Watermarking Algorithm Using BEMD Method", International Conference on Communications, Circuits and Systems, Kokura, Japan, pp: 588-592, 2007.
- [117] Ambadekar SP, Jain J, Khanapuri J, "Digital Image Watermarking Through Encryption and DWT for Copyright Protection", In Recent Trends in Signal and Image Processing, pp:187-195, 2018.
- [118] Sinsha PP, Ranjith Ram A, "Review on image watermarking using bidimensional empirical mode decomposition", International Journal of Engineering and Innovative Tech-nology, vol. 4, no-11, pp:209-213, 2015.
- [119] Rahman MA, Rabbi MF, "DWT-SVD based New Watermarking Idea in RGB Color Space" International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 8, no.6, pp:193-198, 2015
- [120] Singh AK, "Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image", Multimedia Tools and Applications, pp: 1-11, 2019.
- [121] Joshi K, Yadav R, "A LL subband based digital watermarking in DWT", International Journal of Engineering and Manufacturing (IJEM), vol.7, no-2, pp: 50-63, 2017.
- [122] Khairnar PP, Manjare CA, "Image Resolution and Contrast Enhancement of Satellite Geographical Images with Removal of Noise using Wavelet Transform", arXiv preprint, vol. 10, no.12, pp: 1-5, 2014.
- [123] Verma VS, Jha RK, Ojha A, "Significant region based robust watermarking scheme in lifting wavelet transform domain", Expert Systems with Applications, vol. 42, no.21, pp: 8184-8197, 2015.

LIST OF PUBLICATIONS

Journal(s)

1. Singh, L., Singh A. K., & Singh, P. K. (2020). Secure data hiding techniques: a survey. *Multimedia Tools and Applications*, 79(23), 15901-15921. [SCI Indexed, IF=2.757].
2. Singh L, Singh P. K. (2021) "A robust image watermarking through SVD-DCT and BEMD in Wavelet domain based on PSO" *Multimedia Tools and application*, 81(16), 22001-26. [SCI Indexed, IF=2.757].
3. Singh L, Singh P. K. & Sidhu J. (2021) "A proposed secure watermarking technique based on BEMD, SVD and Arnold transform in wavelet domain", *International Journal of Systems Assurance Engineering and Management (IJSAM)*, Springer [Scopus] DOI: <https://doi.org/10.1007/s13198-022-01732-z>.
4. Singh L, Singh P. K. & Sidhu J. (2022) "Comparison based on the basis of applications of various transform techniques based on watermarking" *Journal of Computing Science and Engineering, JCSE*. [Communicated]

Book chapter published –

1. Published chapter “An efficient image watermarking through BEMD and discrete cosine domain based on PSO” In Innovations in Information and Communication Technologies (IICT-2021) (Springer)

Link: https://link.springer.com/chapter/10.1007/978-3-030-66218-9_56

DOI: https://doi.org/10.1007/978-3-030-66218-9_56

2. Published chapter “A Robust Image Watermarking Through Bi-empirical Mode Decomposition and Discrete Wavelet Domain” In Lecture Notes in Electrical Engineering book series (LNEE, Volume 605) (ICETIT 2019) (Springer)

Link: https://link.springer.com/chapter/10.1007/978-3-030-30577-2_92

DOI: https://doi.org/10.1007/978-3-030-30577-2_92

International Conferences Presented:

1. Singh L, Singh A. K., & Singh P. K. (2020). A Robust Image Watermarking Through Bi-empirical Mode Decomposition and Discrete Wavelet Domain. In Proceedings of ICETIT 2019. Springer, pp. 1041-1054 DOI: https://doi.org/10.1007/978-3-030-30577-2_92.
2. Singh L & Singh P. K. (2021) “An efficient image watermarking through BEMD and discrete cosine domain based on PSO”, In Proceedings of IICT 2020, Springer, pp: 469-474 DOI: https://doi.org/10.1007/978-3-030-66218-9_56
3. Singh L, Singh A. K & Singh P. K. (2018). Image Processing Techniques for Forestry applications. *3rd Himachal Pradesh science congress (HIMCOSTE) at IIT Mandi.* (Abstract presentation)