

IMPROVED TECHNIQUES OF ROBUST AND SECURE WATERMARKING FOR DIGITAL DOCUMENTS

Thesis submitted in fulfilment of the requirement of the Degree of

Doctor of Philosophy

By

CHANDAN KUMAR



Department of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology

Waknaghat, Solan-173234, Himachal Pradesh, INDIA

December 2019

TABLE OF CONTENTS

INNER FIRST PAGE	I
ACKNOWLEDGEMENT	IV
DECLARATION BY THE SCHOLAR	V
SUPERVISOR'S CERTIFICATE	VI
PREFACE	VII
LIST OF ABBREVIATIONS	VIII-IX
LIST OF FIGURES	X-XI
LIST OF TABLES	XII-XIII
CHAPTER 1: INTRODUCTION AND REVIEW OF LITERATURE	1-21
1.1 GENERAL EMBEDDING / RECOVERY PROCESS FOR WATERMARK(S)	2
1.2 IMPORTANCE AND NECESSITY OF WATERMARKING TECHNIQUES	3
1.3 IMPORTANT CHARACTERISTICS OF DIGITAL WATERMARKING	4
1.4 CLASSIFICATION OF DIGITAL WATERMARKS	5
1.5 BASIC CONCEPTS OF SPATIAL AND TRANSFORM DOMAIN TECHNIQUES FOR WATERMARKING	7
1.5.1 SPATIAL DOMAIN TECHNIQUE	7
1.5.2 TRANSFORM DOMAIN TECHNIQUE	8
1.6 PERFORMANCE METRICS	11
1.7 REVIEW OF EXISTING WATERMARKING METHODS	13
1.8 LIMITATIONS OF PREVIOUS WATERMARKING SCHEMES AND PROPOSED OBJECTIVES	19
1.9 MAJOR CONTRIBUTION OF THE PROPOSED WORK	19
1.10 THESIS ORGANIZATION	21
CHAPTER 2: SPIHT BASED ROBUST AND DISTORTION CONTROL DIGITAL WATERMARKING IN DWT-SVD-DCT DOMAIN	22-36
2.1 INTRODUCTION	22
2.2 PROPOSED SPIHT BASED WATERMARKING TECHNIQUE	23
2.3 EXPERIMENTAL OUTCOMES .	26
CHAPTER 3: RDWT BASED DUAL WATERMARKING IN NSCT DOMAIN	37-58
3.1 INTRODUCTION	37
3.2 PROPOSED METHOD	38
3.2.1 ALGORITHM FOR WATERMARK EMBEDDING	41
3.3.2 WATERMARK RECOVERY ALGORITHM	43
3.3 EXPERIMENTAL RESULTS	43
3.3.1 PERFORMANCE MEASUREMENT FOR DIFFERENT FORM OF SECRET DATA	50
CHAPTER 4: DUAL WATERMARKING APPROACH THROUGH SECURE FORCE (SF) ENCRYPTION	59-68
4.1 INTRODUCTION	59
4.2 PROPOSED TECHNIQUE	60
4.3 EXPERIMENTAL RESULTS	60

CHAPTER 5: IMPROVED DWT- SVD BASED DIGITAL IMAGE WATERMARKING THROUGH HAMMING ERROR CORRECTION AND ARNOLD TECHNIQUE	69-83
5.1 INTRODUCTION	69
5.2. THE PROPOSED METHOD	70
5.2.1 ALGORITHM FOR WATERMARKS EMBEDDING	71
5.2.2 WATERMARK RECOVERY PROCESS	75
5.3 EXPERIMENTAL RESULTS AND ANALYSIS	76
CHAPTER 6: CONCLUSION AND FUTURE DIRECTIONS	84-85
REFERENCES	86-96
LIST OF PUBLICATIONS	97

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 many challenges 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. Pardeep Kumar**, Associate Professor (JUIT, Wagnaghat) and **Dr Amit Kumar Singh**, Assistant Professor (NIT, Patna) for their incessant guidance, eternal encouragements, painstaking efforts and keen interest during the investigation and finally scanning the manuscript in meticulous way.

I am also grateful to **Prof. (Dr.) Satya Prakash Ghrrera**, Head, Department of Computer Science and Engineering & IT, for his insightful comments and administrative help at various occasions. I extend my sincere thanks to my DPMC members **Dr. Suman Saha**, **Dr. Ruchi Verma** and **Dr. Rajiv Kumar** 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. Hukam Chand Sharma and Smt. Urmila Sharma 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 can never forget to mention my adorable daughter ‘Shanaya’ (Shiva) for her love and affection, which give me constant strength to go on throughout the span of my studies. I am grateful to my wife Dr. Seema Sharma for having patience and giving priority to my research work.

This note of acknowledgement will be always be incomplete without the mention of my Sisters and Brother-in-laws Mr Pawan Sharma, Mrs Pankaj Sharma, Mr Anil Sharma and Mrs Kanchan Sharma for their encouragement and never ending help during the entire course of study.

A special thanks to all adorable kids of our family Shargun, Gunjan, Chunnu, Agatha, Arushi, Aariv, Navya, Aradhya, Utkarsh, Seryu and Naman 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 almighty to facilitate me at every stage of my dream to accomplish this task.

Needless to say, errors and omissions are solely mine.

Date: 20th, December, 2019

(Chandan Kumar)

DECLARATION BY THE SCHOLAR

I hereby declare that the work reported in the PhD thesis entitled **“Improved Techniques of Robust and Secure Watermarking for Digital Documents”** submitted at **Jaypee University of Information Technology, Wagnaghat, India** is an authentic record of my work carried out under the supervision of **Dr. Pardeep Kumar** and **Dr. Amit 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.

(Signature of the Scholar)

(Chandan Kumar)

Department of Computer Science and Engineering & IT

Jaypee University of Information Technology, Wagnaghat, Solan

Date 20/12/2019



JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY

(Established by H.P. State Legislature vide Act No. 14 of 2002)
P.O. Wagnaghat, Teh. Kandaghat, Distt. Solan - 173234 (H.P.) INDIA
Website : www.juit.ac.in
Phone No. +91-01792-257999 (30 Lines)
Fax : +91-01792-245362

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the PhD thesis entitled "**Improved Techniques of Robust and Secure Watermarking for Digital Documents**", submitted by **Chandan Kumar** at **Jaypee University of Information Technology, Wagnaghat, India** is a bonafide record of his original work carried out under our supervision. This work has not been submitted elsewhere for any other degree or diploma.

(Signature of Supervisor-1)
(Dr. Pardeep Kumar)
Associate Professor
Deptt.of CSE & IT
JUIT, Wagnaghat, Solan, India

(Signature of Supervisor-2)
(Dr. Amit Kumar Singh)
Assistant Professor
Deptt. of CSE
NIT Patna, Bihar, India

Date: **Dec 20, 2019**

PREFACE

With the remarkable progress of information and communication technology (ICT), a lot of digital information is quickly and easily being created, distributed and transmitted over the public networks. However, security and privacy of digital data has been potential issue due to attempts of different attacks, when they are transmitted over the network. The attacks include illegal use of information and claim ownership, data tempering and leakage. Further, survey established that the copyright violation and stolen personal information are the growing and dangerous offense. Digital watermarking is the most popular technique used to provide protection of digital data from unauthorized users. In this technique, some kind of secret digital information is embedded into multimedia document for copyright protection and content authentication.

Present work focuses on security of digital documents to prove authenticity of transmitted documents. Starting with examination of all existing methods related with digital documents, thesis offers superior robustness, imperceptibility and security of watermark.

The entire research study has been organized in six chapters.

Initial contribution of chapter 1 start with overview of digital watermarking and review of various robust and secure state-of-the-arts approaches implemented for potential applications. In addition, potential characteristics of digital watermarking, important applications, spatial and transform domain techniques and major performance parameters are discussed. An improved wavelet-based image watermarking using SPIHT is presented in Chapter 2. Main focus of this chapter is to improve robustness and acceptable imperceptibility. Chapter 3 discusses multiple images watermarking using SPIHT in NSCT domain. Aim of this chapter is to achieve high capacity, improve robustness and imperceptibility at same time. Encryption based multiple watermarking in NSCT domain for securing digital documents in wavelet domain is developed in Chapter 4. Main focus of this chapter is to enhance security of digital documents. In Chapter 5, we presents the hybrid transforms and error correcting code based improved robust watermarking approach at low distortion. Finally, summary of the entire work along with findings and scope of further work is given in Chapter 6.

LIST OF ABBREVIATIONS

NC	Normalized Correlation
PSNR	Peak signal-to-noise ratio
SSIM	Structural similarity index measure
CC	Correlation coefficient
DWT	Discrete wavelet transform
HMM	Hidden markov model
DCT	Discrete cosine transform
NCST	Non subsampled contour let transform
RDWT	Redundant discrete wavelet transforms
SVD	Singular value decomposition
IDWT	Integer discrete wavelet transforms
ABC	Artificial bee colony
SWT	Stationary wavelet transform
NIG	Normal inverse Gaussian
DFT	Discrete Fourier transforms
RIDWT	Redistributed invariant discrete wavelet transform
DFFT	Discrete fractional Fourier transform
BDMRS	Basic dynamic multi-keyword ranked search
EDMRS	Enhanced dynamic multi-keyword ranked search
PWLCM	Piecewise Linear Chaotic Map
DFS	Depth first search
PCA	Principal Component analysis
MEO	Multi objective evolutionary optimizer
GA	Genetic algorithm

PSO	Particle swarm optimization
RANSAC	Random Sample Consensus
MRSE	Multi-keyword ranked search over encrypted cloud
KNN	K nearest neighbour
ACR	Affine Covariant Regions
BER	Bit error rate
LWT	Lifting Wavelet Transform
ATT	Arnold Transform technique
ECC	Error correcting code
LSB	Least significant bits
DFrFT	Discrete fractional Fourier transform
CS	Compressive sensing
SPIHT	Set partitioning in hierarchical tree
RRnET	Reversible random extension transforms
OFDM	Orthogonal frequency division multiplexing
FCT	Features Classification Tree

LIST OF FIGURES

1.1	Comparison of (a) identity theft complaint by different age group and (b) cybercrime /identity theft across various countries.	1
1.2	Basic components of security	2
1.3	Diagrammatical representation of general watermarking systems	3
1.4	Major characteristics of the watermark	5
1.5	Important types of watermarking techniques	6
1.6	(i) Spatial and (ii) transform domain techniques	7
1.7	Diagrammatical representation of image decomposition using 2D-DWT	9
2.1	SPIHT based watermark (a) embedding and (b) extraction process	26
2.2	(i) Cover image, (ii) Logo watermark (iii) Watermarked image.	27
3.1	Embedding (i) and extraction (ii) process	41
3.2	(1) Cover-image, (2) Logo-image, (3) Signature-image and (4) watermarked-image.	45
3.3	Extracted watermarks(logo(1)& signature(2))	45
3.4	Performance under various attacks	46
3.5	Proposed Embedding and extraction process	51
3.6	(a) Host image, (b) Text watermark, (c) Logo watermark, (d) Generated dual watermark, and (e) Watermarked image	52
3.7	Recovered watermarks (a) logo and (b) text	52
3.8	Watermarked (attacked) and watermarks (extracted) images	53
4.1	Diagram representing (a)Embedding (b)Extraction procedure.	61-62
4.2	(a) Cover image, (b) Logo & (c) Signature watermark, and (d) watermarked image	62
4.3	Recovered (a) Logo & (b) Signature, watermark	62
4.4	Watermarked(attacked) and watermarks(extracted) images	63
5.1	Process of embedding and extraction for watermarks	74

5.2	(I) Host image, (II) Logo (III) Signature, and (IV) Watermarked image	78
5.3	Recovered watermarks, (I) Logo and (II) Signature	78
5.4	Watermarked (attacked) and watermarks (extracted)	79

LIST OF TABLES

1.1	Comparison between steganography, watermarking and cryptography	3
1.2	Basic property of U,S and V	11
2.1	Experimental observation against different gain value	28
2.2	Performance against various attacks	29
2.3	Performance of proposed method under considered cover images	30
2.4	Experimental results against varying bit rate	31
2.5	PSNR,SSIM and NC performance comparison between proposed technique and other reported techniques	33
2.6	NC performance comparison between proposed technique and Shivani et al. method[118]	34
2.7	Robustness comparison with techniques[109]	34
2.8	NC performance comparison between proposed technique and other schemes [109-111].	35
2.9	Quality evaluation of marked image by subjective measure	35
3.1	Performance under bit rate=1, 2, 3 and varying gain	47
3.2	Performance under fixed gain (0.5) and various bit rates	47
3.3	Performance results of considered cover images	48
3.4	Performance of proposed technique against various attacks.	48
3.5	Reported PSNR, NC's and SSIM values for different filters	49
3.6	Robustness comparison of our technique with[34, 141]	49
3.7	Performance measurements under different gain and bit rates	55
3.8	Experimental results for different covers images	55
3.9	Performance under different attacks for cover Image 'Lena'	56
3.10	Results for image 'Bird'	56
3.11	Comparison of proposed technique under various attacks	57
4.1	PSNR, NC1, NC2 values for proposed method	65

4.2	Performance of various images against gain=0.5 and bit rate =3.	66
4.3	Implementation of various attacks on cover image 'Lena' at constant gain=0.5 and bit rate=3.	66
4.4	Performance of considered host image 'Bird' at gain=0.5 and changing bit rate.	67
4.5	Performance of proposed method against technique[141]	67
5.1	Performance under various gain factors	80
5.2	Performance against fixed gain value(0.05)	80
5.3	Performance evaluation for various cover images	80
5.4	Performance for image 'Lena' against various attacks.	81
5.5	Performance evaluation for different sized characters under different gain and fixed bit rate=3.	81
5.6	Comparison of experimental results against author[75]	82
5.7	Performance of proposed scheme against technique[118]	83

CHAPTER 1

INTRODUCTION AND REVIEW OF LITERATURE

In recent time, information and communication (ICT) is found to be necessary and cost efficient method for transmission of digital documents over open channel [1]. However, securing multimedia information/digital documents related with potential applications is found to be a big issue over open channel [1]. Any attackers/unauthorized person can alter, modify or theft the useful information. In addition various surveys reported that identity theft is the main contributors to fraud in India as well as other countries [1-3]. Identity theft complaints by different age group as recently reported by Security Solutions India are depicted in Fig. 1.1(a) [3]. However, cybercrime comparison of top ten countries as reported by American cyber security company Symantec in 2016 is shown in Fig 1.1(b) [4].

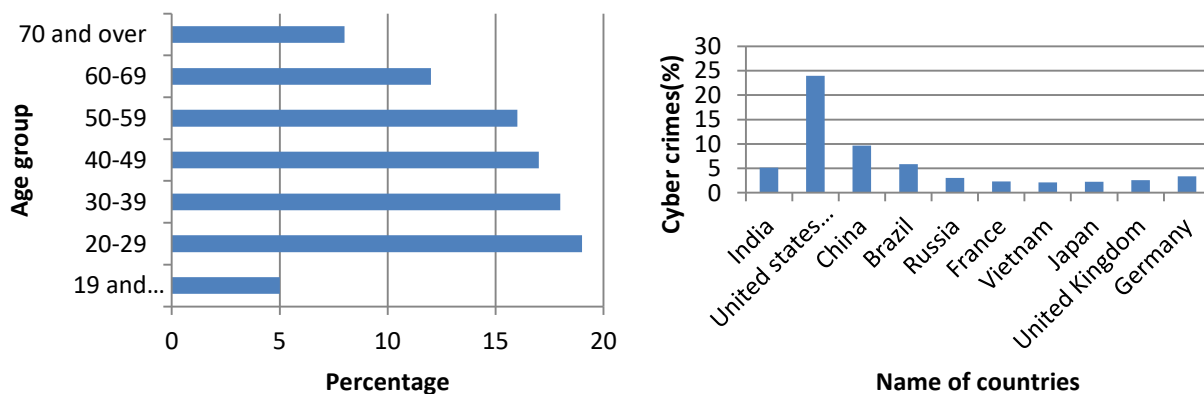


Fig.1.1: Comparison of (a) identity theft complaint by different age group and (b) cybercrime /identity theft across various countries.

Digital watermarking is one of popular method to provide security of digital content for various potential applications [5-6]. This technique imperceptibly embeds secret information into cover media for copyright protection, content authentication and annotation [7]. Further, watermarking should survive for various processes of decryption, re-encryption and geometrical manipulation [8, 9].

It has been seen that robustness, imperceptibility, embedding capacity, security and computational complexity are some of major characteristics/requirements of any digital

watermarking systems [10]. However, maintaining all requirements simultaneously is very difficult for any researchers.

To secure the transmission of digital data, most of the applications must provide basic security components [11]: confidentiality, authenticity, integrity and non-repudiation. These components are depicted in Fig. 1.2. The confidentiality refers that only authorized users can access to the transmitted data. The authenticity property ensures that the data comes from true source and belongs to the correct person. The integrity means data has not been altered by illegal person. Non-repudiation refers that proof of the origin and integrity of the data.

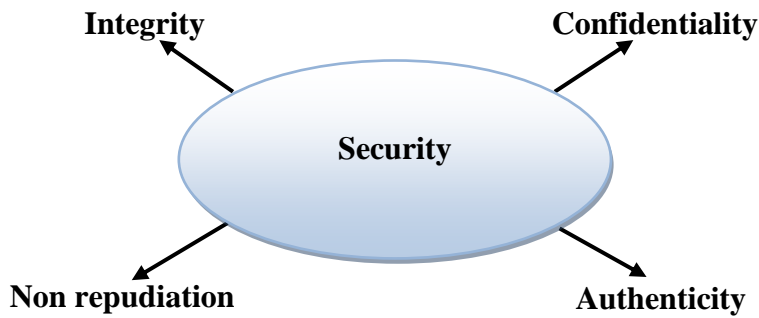


Fig.1.2: Basic components of security [1]

1.1 General embedding /recovery process for watermark(s)

General framework of watermarking is defined in terms of embedding and extraction procedure of hidden information. These procedures are depicted in Fig.1.3 [12]. Here initially, payload is encoded into cover image (D) to produce watermarked image. Finally, payload is detected by decoder. The payload (P_L) is secret information or message that is to be embedded into cover. Initially payload is embedded inside cover and then whole information/watermarked image (D_L) is transferred to decoder where payload detection process takes place. After detection it decodes the output message. The watermarked image (D_L) is represented as:

$$D_L = E(D, P_L) \tag{1.1}$$

At receiver end, decoder takes test/watermarked image (D_L) and original image (D) as input and generate as extracted watermark (P_R).Extracted watermark is represented as:

$$P_R = I(D_L, D) \tag{1.2}$$

Finally comparator(Y) compares extracted watermark (P_R) with original watermark(P_L) for checking difference (Z) between them.

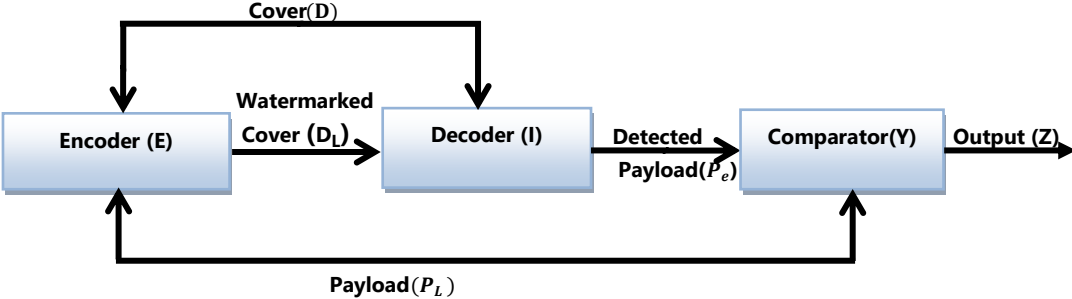


Fig.1.3: Diagrammatical representation of general watermarking systems

1.2 Importance and necessity of watermarking techniques

Steganography, watermarking and cryptography, are the popular scheme used to provide security to digital documents [12].Main differences between these schemes are illustrated in Table 1.1 [13]

Table1.1 Comparison between steganography, watermarking and cryptography [13]

Property	Steganography	Watermarking	Cryptography
Uses of carrier, secret information, output key	Stego-file is generated by embedding payload into digital data using key which is optional	Watermarked image is generated by embedding watermark into digital media.	Cipher-text is generated by encrypting data in image or text file
Cover option	There is no restriction in cover selection	Cover selection is restricted	N A
Purpose/ requirement	Capacity is main requirement for secret communication provided by steganography	Main requirement to preserve copyright information is robustness	Robustness is main requirement to protect the data
Process of detection and retrieval	Data can be fully regenerated without requirement of cover	Cross-correlation is needed for data regeneration process. Original cover is needed for same.	Data is fully retrieved without requirement of cover
cover media and visibility relation	Information is commonly not associated with cover and is imperceptible to human vision system	Watermarks are sometimes perceptible to human visual system and becomes one of feature of cover image.	Hidden data can be easily recognized due to encryption. However deciphering of data is not easy

As compare to cryptography, watermarking technique is useful in protection of digital data even after decryption. Thus watermarking helps to avoid illegal use of personal information and protect it from unauthorized users. However, cryptography focuses on protection of the

contents during transit and not after decryption. Digital image watermarking provides a way of embedding digital data into cover digital data for the purpose of annotation, authentications and copyright protection [14]. Watermarking should survive under various procedures (decryption, re-encryption and geometrical manipulation) [15].

1.3 Important characteristics of digital watermarking

The major characteristics of digital watermark as illustrated in Fig. 1.4[16] are as follow:

- (i) **Robustness:** It refers the capability of the hidden data to withstand any kind of attacks and thus can be used for copyright protection.
- (ii) **Imperceptibility:** It refers the watermark should be done in such a manner it does not degrade the quality of marked data.
- (iii) **Capacity:** It refers the amount of data that can be placed inside the cover image. Information may be in form of image, text number etc.
- (iv) **Security:** The security is measured in term of difficulty to eliminate or change the hidden watermark without damaging the cover image.
- (v) **Data payload:** Amount of information hold by watermark is data payload. A good watermark should contain all necessary data within it. For watermark of size= n bits, there are 2^n possible watermark.
- (vi) **Fragility:** Fragility is reverse of robustness as the main focus is authentication of contents.
- (vii) **Computational cost:** It refers the cost of embedding and extracting data in/from cover image. For efficient watermarking, embedding should be faster than extraction process [23].
- (viii) **Tamper resistance:** It is used to check the authenticity of digital images. Due to sensitivity of watermark against alteration, integrity of watermark can be checked whether it has been ever altered or changed.

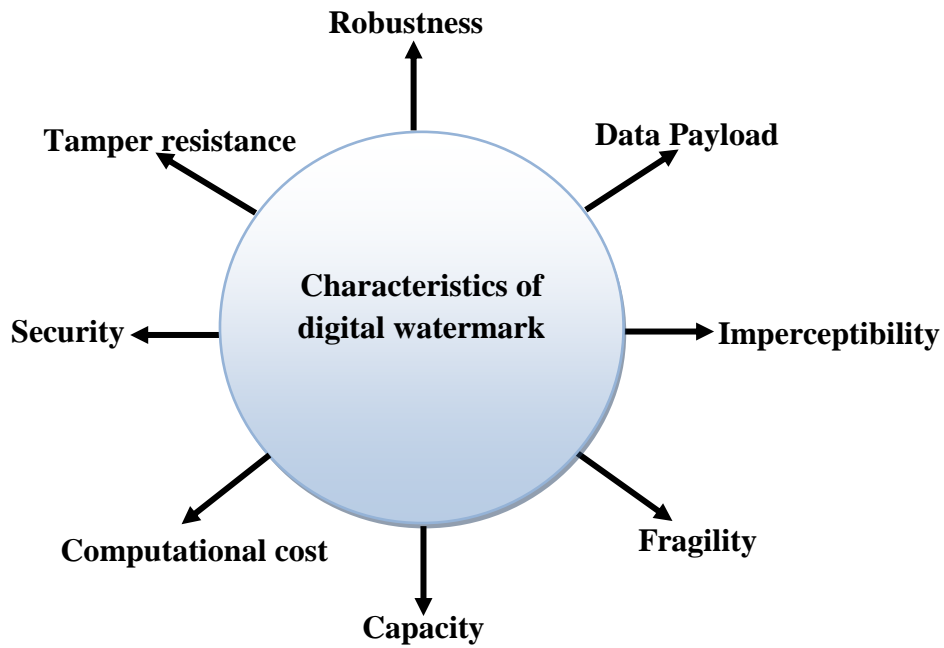


Fig. 1.4: Major characteristics of the watermark

1.4 Classification of digital watermarks

In [17], Mohanty introduced various kinds of watermark and its techniques in different ways. Fig.1.5 shows various types of watermarking schemes. Digital watermarking is mainly divided based on, working domain, document, human and application. Working domain is further divided into spatial domain and transform domain. Complexity of former technique is low as compared to transform domain technique [1]. However, transform domain schemes are more robust [18]. On the basis of document, it is divided into text, image, audio and video. Based on human perceptual, watermark can be divided into visible and invisible.

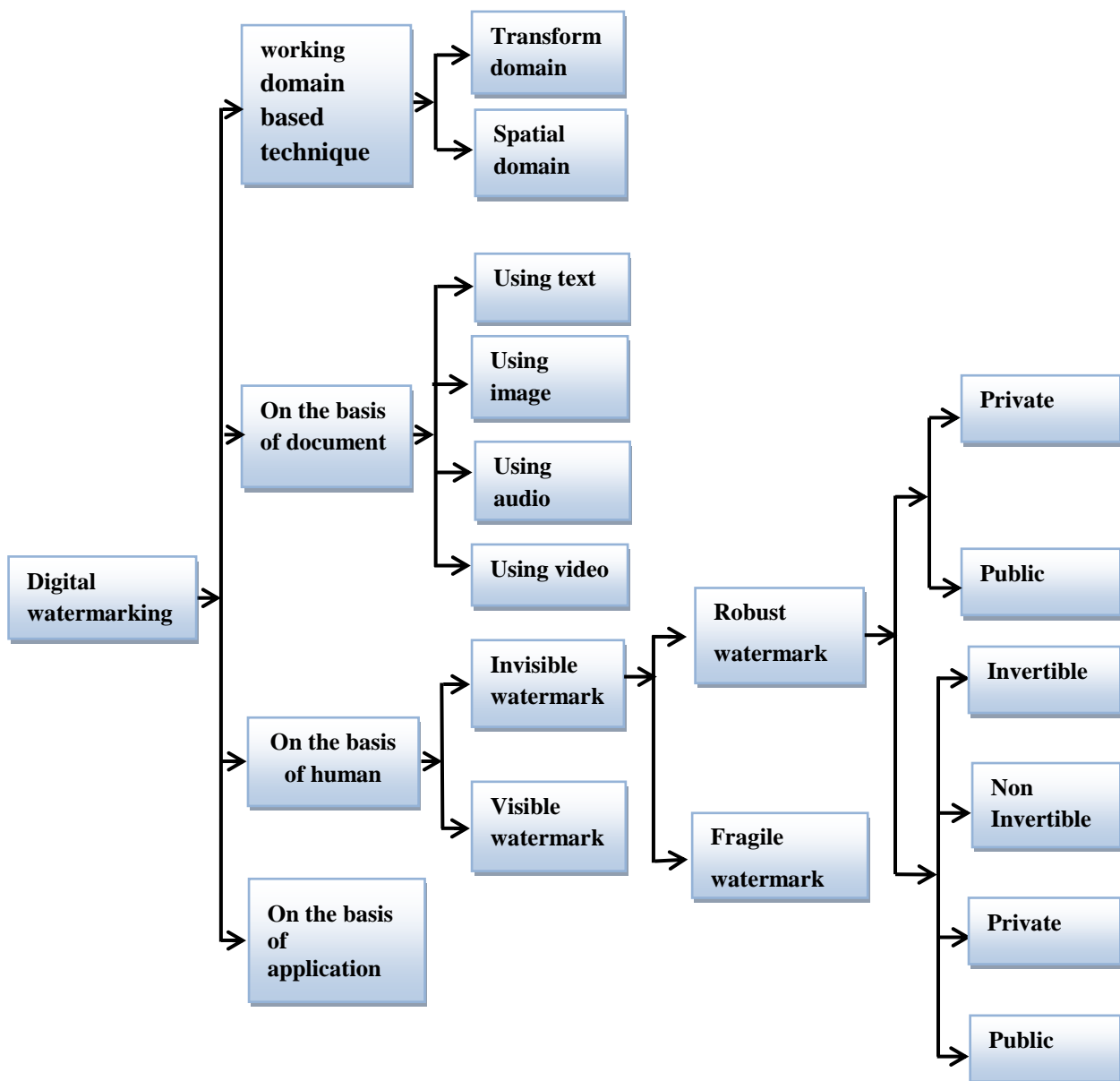
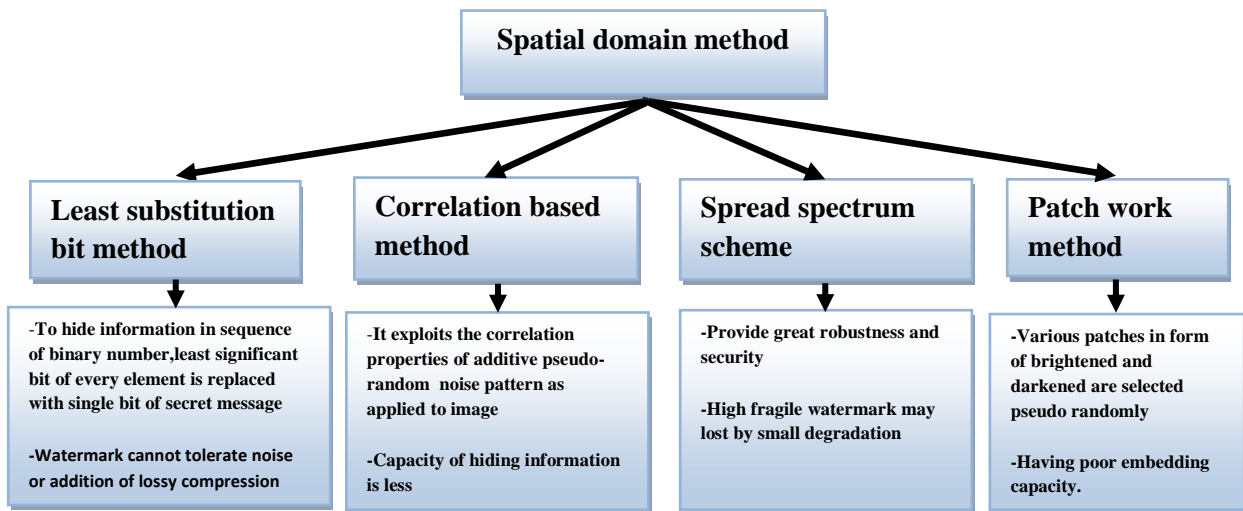
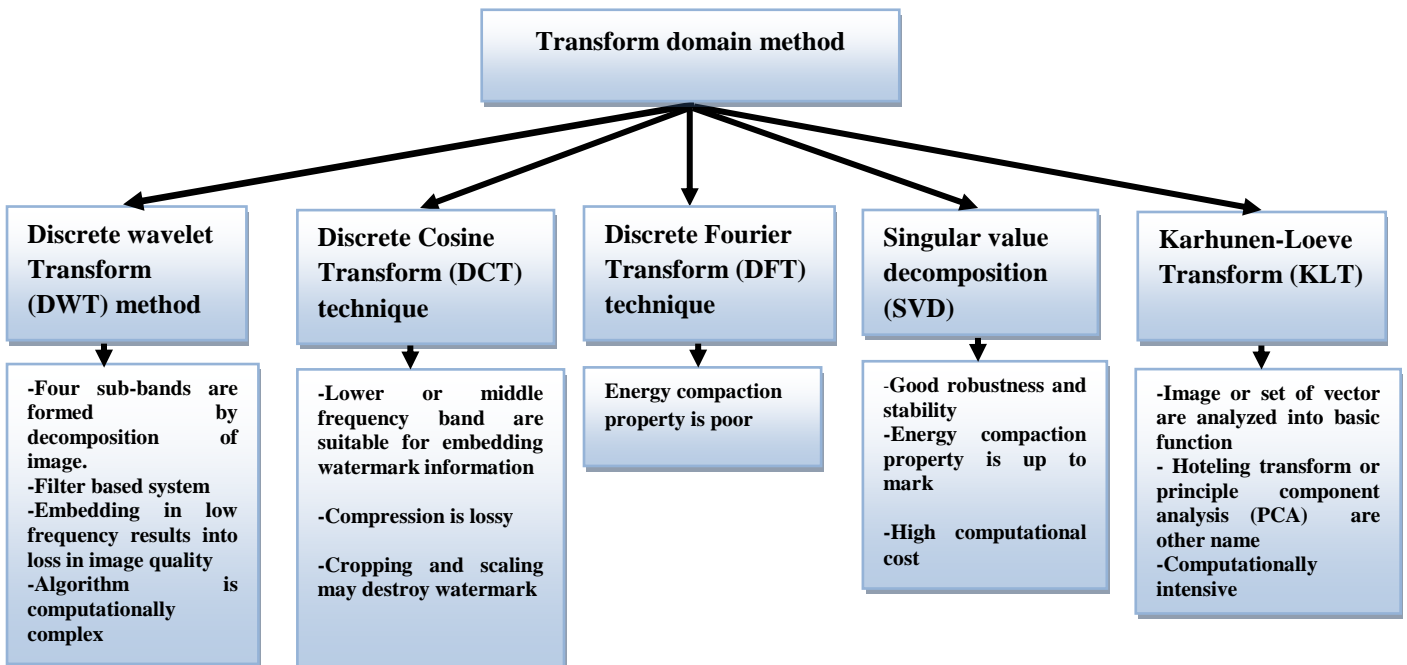


Fig.1.5: Important types of watermarking techniques

Further invisible watermark is further divided into robust and fragile watermark. Finally robust watermarking is distinguished into invertible, non-invertible, private and public. Some of the popular spatial and transform domain shames are shown in Fig. 1.6.



(i)



(ii)

Fig.1.6: (i) Spatial and (ii) transform domain techniques

1.5 Basic concepts of Spatial and transform domain techniques

Refer Fig. 1.6, it is interesting to see that least substitution bit (LSB), Correlation based technique and Spread Spectrum is some of the basic spatial domain techniques. However, DWT, DCT, DFT and SVD are the most popular approaches of transform domain techniques.

1.5.1 Spatial domain technique:

The popular spatial domain techniques are given below [143].

- (i) Least substitution bit (LSB): In this scheme information in form of sequence number is hidden by replacing one bit of secret message. However watermark can survive for some attacks such as cropping and is unable to survive under noise or lossy compression attack. Least significant bit of mantissa is used for floating point arithmetic. Size of message is small as compared to the information to be hidden in term of bits.
- (ii) Correlation based technique: A pseudo-random noise (PN) pattern, WT (e, f) is added to cover image C (e, f), according to equation given below:

$$C_w(e, f) = C(e, f) + \alpha \times WT(e, f) \quad (1.3)$$

Here α and C_w denotes gain factor and watermarked image respectively. Value of α should be selected for improved robustness and imperceptibility simultaneously. Watermark is recovered using pseudo-random noise generator algorithm. During watermark detection, single bit is set if correlation lies beyond certain threshold T. This process is repeated independently for each block of image.

(iii) Spread Spectrum:

It is noted that embedding of watermark into insignificant region leads to easy destruction of watermark by common signal and geometrical processes. In spread spectrum system larger bandwidth is selected to transmit narrow band signal. Similarly watermark's energy is spread over various frequency components so that in each component have small and undetectable energy. Therefore, using this technique watermark is embedded into perceptually significant regions of data and hence is robust to common watermarking attacks. Further, in this technique there is less requirement of human visual system (HVS), however recovery procedure requires original image. Moreover, due to fragility, minor degradation can destroy watermark.

1.5.2 Transform domain technique:

The popular transform domain techniques are given below [143].

(i) **Discrete wavelet transform (DWT):**

DWT is a filter-based system that decomposes an object into a collection of four multi-resolution sub-bands that are non-overlapping. They can be represented as LL (Approximation sub band), LH (Horizontal sub-band), HL (Vertical sub-band) and HH (Diagonal sub-band). Due to more sensitivity of human visual system towards low frequency portion (LL sub-band), it is preferred to embed watermark inside remaining three parts to sustain better quality of image. Further, multiple scale wavelet decomposition can be obtained by repeating the process. Normally, the majority of the image energy is concentrated in the lower frequency coefficient sets LL, so embedding watermarks in these coefficient sets significantly degrade the image. However, robustness significantly increases, if embedding is done in low frequency coefficient sets. In contrast to this, edges and textures of the image are included in the high frequency coefficient sets (HH) and the human eye is generally not sensitive to changes in such coefficients[7,20,23]. Fig.2[19] depicts the diagrammatical representation of 2-dimensional DWT. Here, $J(m)$ and $K(m)$ represents coefficients of low and high pass filters respectively.

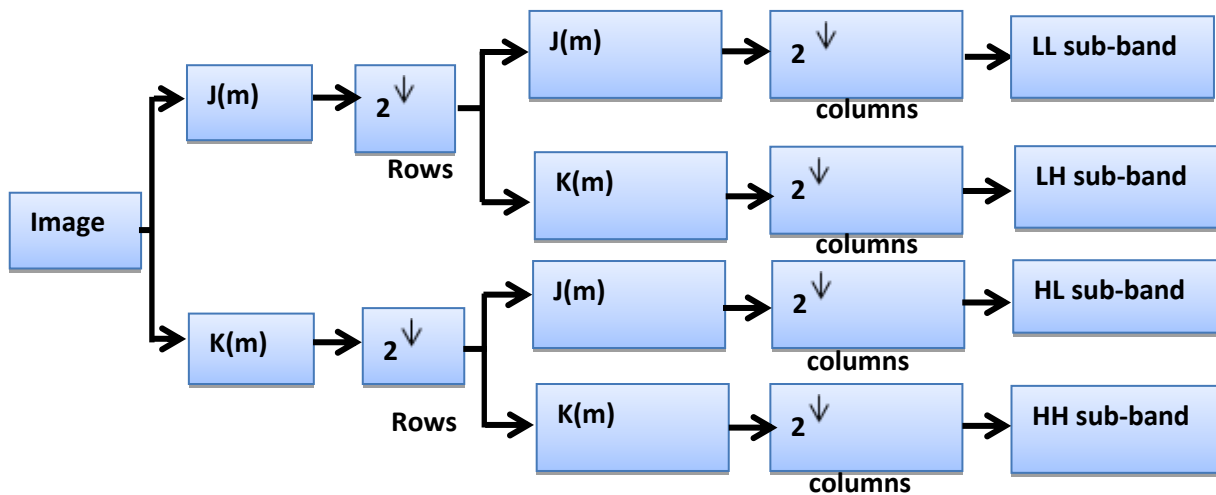


Fig.1.7. Diagrammatical representation of image decomposition using 2D- DWT

(ii) **Discrete cosine transforms (DCT):**

DCT image is divided into different frequency parts. Embedding into middle frequency component leads to increase in resistance against lossy compression without significantly altering the cover image. Further, DCT has high energy compaction property due to which it is capable of packaging most energy information in few coefficients. It also

reduces block like appearance (known as blocking artifact) that appears when edges between sub-images becomes noticeable. DCT for input image (size: $N \times N$) can be represented as:

$$B(i,j) = \frac{1}{\sqrt{2N}} E(i) E(j) \sum_{z=0}^{N-1} \sum_{y=0}^{N-1} I(x,y) \cos \frac{(2x+1)i\pi}{2N} \cos \frac{(2y+1)j\pi}{2N} \quad (1.4)$$

$$E(i), E(j) = \frac{1}{\sqrt{N}} \text{ for } i, j = 0 \text{ and } E(i), E(j) = \sqrt{\frac{2}{N}} \text{ for } i, j = 1, 2, \dots, N-1 \quad (1.5)$$

Here $B(i,j)$ represents DCT coefficients with row i and column j for DCT matrix. However intensity of image (for pixel with row x and column y) is represented by $I(x,y)$ [7, 20].

(iii) Discrete Fourier transforms (DFT):

DFT is used for digital watermarking process due to possibility of controlling frequency of cover images. Watermark can be easily embedded by selecting suitable parts of cover image to make efficient for watermarking. Significance of discrete Fourier transforms over spatial domain techniques are [143]:

- Resistant against geometrical attacks such as rotation and translation.
- Stronger watermark can be embedded because watermark information is spread over entire image.

For a square image of size $N \times N$, the two-dimensional DFT is given by [21]:

$$F(k,l) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f(i,j) e^{-\beta 2\pi i \left(\frac{ki}{N} + \frac{lj}{N} \right)} \quad (1.6)$$

The value of each point $F(k,l)$ is obtained by multiplying the spatial image with the corresponding base function and summing the result. Where $f(i,j)$ is the image in the spatial domain and exponential term $(e^{-\beta 2\pi i \left(\frac{ki}{N} + \frac{lj}{N} \right)})$ is the basis function corresponding to each point $F(k,l)$ in fourier space.

(iv) Singular value decomposition (SVD):

SVD provides robustness against geometrical attacks and it has been found that singular value of image provides rotation, scale and translation invariance. Thus use of SVD in digital watermarking improves performance. Basic properties of U , S and V are depicted in table 1.2.

SVD for rectangular matrix is denoted as:

$$A = USV^T \quad (1.7)$$

Where A: M×N matrix

U: Orthogonal matrices

S: Diagonal matrix

Table 1.2: Basic properties of U,S and V

U	S	V
Orthonormal matrix	Diagonal matrix	Orthonormal matrix
Matrix not unique	Contain singular values of matrix which are unique	Matrix not unique
Always real if matrix is of real value	Always real if matrix is of real value	Real if matrix is of real value
NA	Singular values are stable against attacks	NA

1.6 Performance Metrics

In Section 1.6, it is interesting to see that Peak signal to noise ratio (PSNR), (ii) Normalized correlation(NC), (iii) Bit error rate(BER),(iv) Structural similarity index measure(SSIM), (v) Number of changing pixel rate(NPCR) and Unified averaged changed intensity(UACI) are used as important metric to evaluate the performance of most of the watermarking system.

(i) PSNR:

It determines the quality of cover after embedding of some secret watermark [22].

$$PSNR(R, S) = 10 \log \frac{(255)^2}{MSE(R, S)} \quad (1.8)$$

Where MSE (mean square error) is represented as:

$$MSE(R, S) = \frac{1}{L \times M} \sum_{a=1}^L \sum_{b=1}^M (R_{ab} - S_{ab})^2 \quad (1.9)$$

Where(R, S) are images of size (L × M), R_{ab} , S_{ab} are pixel of original and watermarked image size, respectively.

(ii) NC:

It measures the similarity between original secret data (watermark) and extracted data. The NC value may lies between 0 to 1. However, the value more than 0.7 is more suitable for most of the applications [22].

$$NC = \frac{\sum_{a=1}^L \sum_{b=1}^M (WT_{\text{originalab}} \times WT_{\text{recoveredab}})}{\sum_{a=1}^L \sum_{b=1}^M \cdot WT_{\text{originalab}}^2} \quad (1.10)$$

Where $WT_{\text{originalab}}$ and $WT_{\text{recoveredab}}$ are pixels of original and recovered watermark respectively.

(iii) **BER:**

BER is measured as ratio among wrongly decoded bits and total number of bits. BER is suitable for watermark with random binary sequence [22]. Normally, author should keep its value near or equal to zero.

$$BER = \frac{\text{Number of incorrectly decoded bits}}{\text{Total number of bits}} \quad (1.11)$$

(iv) **SSIM:**

Visual resemblance among original and watermarked image is known as SSIM. Acceptable SSIM value ranges between -1 and 1, Considered images should be similar if $SSIM=1$ [22].

$$SSIM(d, e) = g(d, e) h(d, e) i(d, e) \quad (1.12)$$

Where

$$g(d, e) = \frac{2\mu_d\mu_e + C_1}{\mu_d^2 + \mu_e^2 + C_1} \quad (1.13)$$

$$h(d, e) = \frac{2\sigma_d\sigma_e + C_2}{\sigma_d^2 + \sigma_e^2 + C_2} \quad (1.14)$$

$$i(d, e) = \frac{\sigma_{de} + C_3}{\sigma_d\sigma_e + C_3} \quad (1.15)$$

Here C_1 , C_2 and C_3 : Constants with positive values

$g(d, e)$, $h(d, e)$ and $i(d, e)$: Luminance, contrast and structure comparison functions respectively.

$\mu_d\mu_e$: Mean luminance of image d and e respectively

$\sigma_d\sigma_e$: Standard deviation of image d and e respectively

σ_{de} : Covariance between image d and e respectively

(v) **NPCR and UACI :**

NPCR is a rate of changing pixel rate between plain and ciphered image. UACI is defined as average intensity differences among plain and ciphered image. As the value of UACI increases, crypto system becomes more resistance to attacks [23]. For grid (n,p) pixel value in 'C₁' and 'C₂' are shown as C₁(n,p) and C₂(n,p), respectively.

NPCR is calculated as:

$$NPCR = \sum_{n,p} \frac{T(n,p)}{Z} \times 100\% \quad (1.16)$$

Where 'Z' is total number of pixels in cipher text and V(n,p) is defined as:

$$V(n,p) = \begin{cases} 0, & \text{if } C_1(n,p) = C_2(n,p) \\ 1, & \text{if } C_1(n,p) \neq C_2(n,p) \end{cases} \quad (1.17)$$

$$UACI = \sum_{n,p} \frac{|C_1(n,p) - C_2(n,p)|}{V \times Z} \times 100\% \quad (1.18)$$

Here 'V' represents largest supported pixel value compatible with cipher text image format. NPCR and UACI have critical values as 0.99 and 0.33 respectively [23].

1.7 Review of existing Watermarking methods

In method [24] genetic algorithm (GA) is implemented along with DCT-SVD to embed watermark information into host image. Results clearly show superiority of scheme than other mentioned techniques. A blind watermarking scheme based on hidden Markov model (HMM) in DWT domain is proposed by Amini et al. [25]. Experimental outcomes confirm the robustness of method under common attacks and bit error rate is comparably low compared to method [26, 27]. Author [28] introduced a robust method using generic algorithm along with DWT and DCT. Watermark inside the selected sub-bands of cover image is encoded by random sequence pattern. Performance measurement in term of PSNR and NC shows superior performance than other referred techniques [29-31]. Further it has been observed that the scheme is expensive than other individual DWT and DCT methods. In method [32] a robust scheme is developed using SVD in NSCT domain. Combination of NSCT and SVD leads to better reconstruction of image. Further for better robustness and security, SVD and Arnold transform is applied respectively. Test clearly revealed that the technique is superior to other existing methods [33-35]. Though; computational cost of RDWT based scheme is more than that of DWT based techniques. Integer discrete wavelet transform (IDWT) and SVD based robust watermarking is proposed by Lei et al.[36]. Two watermarks are embedded inside selected sub band of IDWT and SVD for better protection.

Next, an artificial bee colony (ABC) is introduced to make good trade-off among major performances metrics. Test results clearly show improved robustness of proposed algorithm as compared to other mentioned technique [37]. It has been further observed that proposed work perform well against brute-force attack. A logistic map-based chaotic encryption algorithm in cloud computing environment is presented by Cao et al.[38]. It is clear from experiment that the technique provides excellent embedding capacity and robust against common watermarking attacks. A robust watermarking technique is introduced by Pan-Pan et al. [39]. In this work, watermark is embedded into RGB component of cover. Test outcomes clearly show robustness of technique against signal processing attack along with de-synchronization attacks. Further, watermark detection rate is found to be better than [40-43]. Furthermore the scheme is found to be computationally expensive and has less embedding capacity. Abbas et al.[44] introduces a method based on LWT along with Arnold transform. Low frequency sub-band of LWT decomposed cover image is selected to embed watermark into cover. Technique is found to be survived against various attacks. In technique [45], SVD technique is used to embed tamper localization and self-recovery bits into host image. Experimental outcomes show improved robustness and image quality than technique [46]. A robust watermarking technique by using spatial transform along with transform domain is developed by Ansari and Pant [47]. Further principal components of watermark are used to modify the cover image after decomposing with SVD. It is evident from results that scheme perform well as compared to other mentioned technique under consideration. Author [48] has introduced a method for digital watermarking using color images. Initially DWT decomposes ‘Y’ component. Finally, watermark (logo) is embedded into ‘Y’(high frequency component). Performance measurement in terms of PSNR, SSIM clearly shows better performance than that of [49,50]. Authors [51] introduced a robust watermarking method using contourlet domain. Watermark information is embedded in contourlet domain using multiplicative secure spread spectrum. Performance of method in term of BER is better than other reported techniques[52-54]. A semi fragile watermarking scheme based on Fourier transform (DFT) using substitution box is introduced by [55]. Further, watermark bits generated by chaotic map are embedded into cover image. Analysis of results clearly shows improvement in robustness and security. Further it has been observed that the scheme is computationally complex. A robust and lossless algorithm using combination of visual cryptography and SVD using wavelet is introduced by Ali et al.[56]. In this scheme, translation invariant domain is calculated by combination of wavelet and fractional Fourier transforms. Next, watermark information is embedded into pre calculated random position of Fourier transformed

matrix. Various simulation results clearly show the superiority of scheme on basis of robustness and computational time in comparison with other mentioned schemes [57,120-121]. Author [58] introduced a watermarking scheme using DFT along with compressive sensing. Initially, cover image is partitioned into most significant (used for encryption) and less significant information (used for embedding) using DFT. Method is reported as best in term of PSNR and BER than technique [59]. A hybrid multiple watermarking scheme using wavelet transform is described by Singh et al.[60]. Further, the robustness and security of watermarks is improved by using suitable ECC and common encryption algorithm respectively. Various test results shows resistance against attacks along with checkmark attacks. Authors [61] developed watermarking scheme using DCT and PCA for e-governance documents. Results outcomes clearly prove the robustness of scheme against common watermarking attacks. A DWT based watermarking scheme using hybrid multi-watermarking decoder is introduced by Wang et al.[62].Further, watermark information in multiple forms is inserted into selected cover image. Results clearly prove the robustness of scheme (calculated in term of BER) against common watermarking attacks. A chaotic mixture based blind watermarking method is introduced by Author [63]. The encrypted version of watermark is embedded into host image. NC and BER performance is better than methods suggested in [64-66]. A multiple-watermarking scheme using compressive sensing (CS) based dual watermarking is proposed by [67]. In this work; multiple watermarks are embedded inside cover using DWT and histogram alteration. Test results clearly prove that the algorithm is imperceptible and secure. A watermarking method using three different transform schemes is proposed by author [68]. Performance of technique is measured in term of PSNR and NC value. Further highest reported PSNR is 42.30dB. However NC value is up to 0.9993. In [69], non-blind watermarking scheme is introduced to achieve robustness, imperceptibility, excellent embedding capacity and strong security. Experimental results clearly show superiority of algorithm in term of robustness and computation time than other mentioned techniques [84,115-117] under considered attacks. A GA-particle swarm optimization domain based reversible watermarking technique is presented by Naheed et al.[70]. Experimental results clearly show improved performance in term of embedding capacity and imperceptibility as developed by the Luo et al. method [71]. Author [72] has developed a reversible and separable watermarking method. Host image is encrypted with multi-granularity encryption. Further, Pixel shifting technique is applied to embed watermark into targeted image. Results in term of PSNR and embedding capacity are found to be better than technique [73].However image becomes less imperceptible with increase in block size. A DWT and SPIHT based watermarking algorithm is described by author [74].

Test result under various attacks clearly shows robustness of scheme against common watermarking attacks. A robust and imperceptible technique based on DWT and SVD for telemedicine applications is proposed by [75]. Watermark is decomposed into two parts which are embedded into cover image. Further, various error correcting code are applied on cover image. Performance under various attacks shows the robustness of scheme as compared to other mentioned algorithm. Bhatnagar et al. [76] introduced a dual watermark embedding scheme using SVD along with random extension transforms (RRnET). Initially, cover image is transform by RRnET followed by embedding of logo watermark. Next, binary watermark is embedded using threshold technique. Technique is found to be suitable for various applications due to robustness, security and sensitivity. A multi-scale Gaussian filtering model based robust watermarking scheme for de-synchronization attacks is proposed by Ji et al. [77]. Further, this model is used to take out feature point from host image which are geometrically invariants. In this work, dither quantization modulation is used to embed watermarking information. Number of experiments performed, confirms the robustness of technique against different watermarking attacks than other state-of-art methods [78, 79].

In [80], PSO is used to improve the robustness of the watermark. The outcome demonstrated on different images showed the usefulness of the method.

Author [81] has presented a secure watermarking scheme in encrypted domain. A watermark is placed inside the encrypted version of the cover image. The result demonstration showed that the method is secure. In ref. [41], all affine covariant regions of image are selected to embed watermark information. Further, comparison of scheme with techniques [79, 82, 83] clearly confirms robustness of scheme against attacks. Results clearly show better performance of scheme against various mentioned attacks. In [84], author introduced a transform domain based watermarking scheme for directly embedding watermark into singular vector of transformed DWT cover image. It is clear from experimental results that the scheme is not only robust against attacks, but also computationally low. In method [85] authors has used combination of DWT, DCT and SVD along with compressive sensing (CS) and Orthogonal Matching Pursuit (OMP). In proposed scheme, firstly SVD is applied on watermark to obtain principal component. Next, vector is generated by Gaussian random matrix of DCT coefficients, followed by SVD application. Finally watermark is embedded into cover image. Test results clearly prove that scheme has better performance against various kinds of attacks. A fragile watermarking scheme using chaotic maps is introduced by Nazari et al. [86]. First of all, different blocks of cover image

are generated and for security purpose chaotic maps encryption is applied on it. Further, according to block mapping procedure, watermark information is embedded into block. Number of test has been conducted that clearly prove that the performance of method is outstanding against attacks. Further it has been observed that algorithm is best than other mentioned scheme [87-89]. Author [90] has introduced a watermarking scheme using CMYK color image. DCT and DFT are used to transform the selected components (Y and K). Further, these components are selected for data embedding. Experimental results clearly show that technique is robust and imperceptible. In [91], a watermarking method using ECC and spiral scanning is developed. Experimental results clearly show superiority of scheme against various attacks. Medical images based compression and lossless method is developed by author [92]. In this scheme, compressed version of watermark is placed inside the RONI portion of host image. Results clearly show that the scheme offered higher compression ratio as compared to other mentioned techniques. In ref.[93], author has introduced a real time compression for cover image. Initially watermark is secured by encryption technique before embedding into BTC compressed image. The outcome proved that the scheme is efficient at low computational cost. Further it has been observed that scheme is better in term of PSNR as compared to other mentioned scheme [94, 95]. Author [96] presented a semi-blind scheme using SVD and chaotic permutation. Initially cover and watermark images are divided into fixed size block by using chaotic permutation. Further, SVD of watermark is used to modify singular value of cover using code book scheme. Test clearly proves that the method is robust as compared to other mentioned techniques [97,98,99,100]. Author [101] has developed a watermarking approach in data mining background. The binary form of association rule is embedded into singular value of cover image. Number of experiments performed on proposed scheme clearly show the superiority against other mentioned techniques [50,102,103,104,105]. Author[106] has proposed robust Weibull distribution based watermarking scheme using DCT domain. Further, outcome of different distribution techniques are examined and found that mid-frequency DCT coefficients are best characterizes by weibull distribution (long-tailed). Improved PSNR and BER values clearly prove superiority against JPEG compression attacks. In method[107], author introduced a spread spectrum based watermarking method in DCT domain. DCT is applied on host image and middle coefficient is selected followed by PN-sequence embedding into it. Test clearly proves robustness and imperceptibility for common watermarking attacks. Kumar et al.[108] introduced a medical hiding technique for securing clinical record on wireless channel.

The entire test evaluated in terms of PSNR and BER clearly shows superiority of technique than other mentioned scheme. Authors[109] introduced a watermarking scheme using combination of transform techniques. The outcomes reveal that the method offered high NC values as compared to former approaches[110-111] against common watermarking attacks. In [112], security is achieved by embedding multiple watermarks into cover image. In addition, text watermark is encrypted via simple encryption prior to embedding into cover. This encryption scheme reduces the cost as demanded in selected applications. The outcome shows better robustness of scheme against different kinds of attacks. Author [118] has presented a robust and secure watermarking scheme. Further, SPIHT and Chinese remainder theorem (CRT) is applied to achieve better robustness and security. NC value of method is high as compared to techniques suggested in [58, 113,114, 119-121]. In [122], author described a robust watermarking using SVD and NSCT. The outcome showed that scheme is robust.

An imperceptible method using NSCT along with scale invariant feature transform (SIFT) is explored by Hua et al. [123]. Proposed method offered good capacity and robust results. SPIHT based robust watermarking using DWT is introduced by Meenpal [124]. Security of watermark is improved by using Arnold scrambling method. Experimental demonstration showed that the method is robust against common attacks and found greater NC value than former technique [125].

A multiple watermarking method for healthcare images using DCT, SVD along with NSCT is presented by Singh et al.[126]. Performance results measured in term of PSNR and NC clearly prove robustness of method under various attacks. Author [127] has presented a compression and back propagation neural network based multiple watermarking methods. Next, watermark information in encoded form is embedded inside cover. Proposed technique performs better in terms of robustness and imperceptibility.

With the help of turbo code, encoded version of watermark is embedded inside the wavelet-LSB of the cover[128]. The outcome showed that the method offer better trade-off between key parameters. A dual watermarking method has been described by Shi et al.[129]. Further image is decomposed into fragile, robust and no watermark part before embedding into cover image. Various test results proved robustness against different attacks. In ref.[130], author described the embedding of two watermarks in the cover. The scheme offer high PSNR as compared to [131-132] without compromising robustness.

1.8 Limitations of previous watermarking schemes and proposed objectives

The previous section introduced a detail review of wavelet domain watermarking approaches using various techniques such as GA, compression, HMM, encryption, ECCs and several other transform domain techniques. It is important to notice that robustness, imperceptibility, security and capacity are some of the most significant factor of the watermarking system. However, there is a trade-off between these factors. Most of the researchers are enhancing any one or two factors but they compromise with rest of the other factors. Hence, there is strong need of efficient digital watermarking technique that can offer good trade-off between all these factors. In this thesis, some techniques are introduced that offer optimal trade-off between these factors.

Therefore, the potential objectives of the present work are as follows:

- (i) To examine the performance of different state-of-the-art digital documents watermarking schemes to identify most prospective one.
- (ii) To develop watermarking technique(s) for digital data security that offers better performance in terms of significant factors against attacks.
- (iii) To address the issue of robustness, imperceptibility and security of the techniques at same time.
- (iv) To determine the performance of developed technique(s) by standard metric against well-known signal processing attacks.

1.9 Major contribution of the proposed work

The initial contribution of the thesis begins with developing a robust and distortion less watermarking using transform domain techniques. The method uses DWT to decompose the cover image into four non overlapping sub-components. Then, due to excellent energy compaction property of DCT, it is applied to lower frequency sub-band of the DWT image. Further, SVD is applied on DCT image to produce singular vector of the cover image. The scrambled version of the watermark is used to improve the confidentiality. The scrambled watermark is further transformed by DCT-SVD. The method uses singular vector of the scrambled watermark to modify (embed) the singular vector of the cover image. The imperceptibility and robustness of the suggested technique is tuned at various gain factors and bit rates. Finally, compressed watermarked image as obtained via SPIHT is efficiently transmitted on open (unsecure) channel. At the receiver end, user decompresses the

information first and then extracts the secret data via appropriate extraction algorithm. Performance of technique is evaluated for various gain, bit rate, different cover images and potential attacks. In addition, subjective evaluation is also performed for the method. It is proved from results, the suggested technique is robust and secure than of other schemes.

Due to potential importance of dual watermarking in various applications, we have developed a dual watermarking scheme in our second contribution. It is established that RDWT and NSCT are shift invariant in nature and rich directionality. The method uses redundant discrete wavelet transform (RDWT), SVD, Arnold transform and SPIHT to makes it more robust than former schemes. Firstly, the method uses the sub-image having maximum entropy and NSCT is applied on it. Next, we apply RDWT to NSCT image to obtain the RDWT image. RDWT image is further transform via SVD to obtain the singular vector of the image (cover). The method obtained singular vector for both watermarks with similar procedure. Here, the signature watermark first scrambled via Arnold transform before SVD applied on it. Furthermore, the method uses singular vectors of both watermark to modify (embed) the vector of cover image. Finally, compressed version of the marked image is obtained via SPIHT is efficiently transmitted on open (unsecure) channel. At the receiver end, user decompresses the information first and, then extracts the secret data via appropriate extraction algorithm. The method is extensively estimated for various gain, three different bit rate, ten different cover images, seven potential wavelet filters and well known attacks. In addition, subjective evaluation is also performed for the method. Furthermore, the proposed scheme is also tested for two different forms of the secret data (image and text watermark) instead of the same form of the data.

Another contribution is to increase security of watermark at low complexity. A dual watermarking approach in NSCT domain is developed. The idea is same as our previous technique (RDWT based dual watermarking in NSCT domain as discussed in the second contribution), however, this approach uses secure force (SF) encryption (after compress the watermarked image via SPIHT) to provide better security at low cost. It is established that secure force algorithm not only provides security, but it has low complexity than other encryption techniques. Extensive assessment of the approach confirmed that the method is secure, robust, distortion-less and has low computational complexity which outperforms the other existing approaches.

In our fourth contribution, an error correction code based robust and imperceptible watermarking technique is developed to reduce the channel noise distortion. The method jointly uses hamming error correction code and Arnold technique to provide robustness and security, respectively. In the embedding process of image and text watermarks, the method uses DWT to decompose the cover image. Second, the selected component of DWT is transform by SVD. The image watermark data is first scrambled by Arnold transform and the scrambled data is divided into equal parts. Each part is imperceptibly embedded into the two different first level DWT components of the SVD cover image. However, hamming code uses to encode the other watermark (in the text form) before embedding into the second level of the DWT cover image. Finally, SPIHT used to compress the marked image prior to transmission on open network. The extraction procedure is implemented in reverse order. All test results clearly confirms that the robustness of our scheme is better than other schemes.

1.10 Thesis Organization

The entire research study has been organized in six chapters.

Initial contribution of chapter 1 start with overview of digital watermarking and review of various robust and secure state-of-the-arts approaches implemented for potential applications. In addition, potential characteristics of digital watermarking, important applications, various transform domain techniques and key performance factors are discussed. SPIHT based robust and distortion control digital watermarking in DWT-SVD-DCT domain is presented in Chapter 2. Main focus of this chapter is to improve robustness and acceptable imperceptibility. Chapter 3 discusses RDWT based dual watermarking in NSCT domain. Aim of this chapter is to achieve high capacity, improve robustness and imperceptibility at same time. Dual watermarking approach through secure force (SF) encryption is developed in Chapter 4. This chapter is related with security enhancement related to digital documents. In Chapter 5, Improved DWT- SVD based digital image watermarking through Hamming error correction and Arnold technique is proposed. Finally, Chapter 6 discusses about conclusion and future directions

The comprehensive survey presented in this chapter has been published in Multimedia Tools and Applications, Vol. 77, Issue 3, pp.3597-3622. Springer, mentioned under list of publications at the end of the Chapter 6.

CHAPTER 2

SPIHT BASED ROBUST AND DISTORTION CONTROL DIGITAL WATERMARKING IN DWT-SVD-DCT DOMAIN

This chapter presents an improved SPIHT based robust and distortion control digital watermarking in DWT-SVD-DCT domain. Firstly, the method uses DWT to decompose the cover image into four non overlapping sub-components. Then, DCT is applied to lower frequency sub-band of the DWT image. Further, SVD is applied on DCT image to produce singular vector of the cover image. The scramble version of watermark image is obtained prior to embedding. The scrambled watermark is further transformed by DCT and SVD. The method uses singular value of the scrambled watermark to modify (embed) the singular value of the cover image. The imperceptibility and robustness of the method is tuned at various gain factors and bit rates. Finally, compressed watermarked image as obtained via SPIHT is efficiently transmitted on open channel. At the receiver end, user decompresses the information first and, then extracts the secret data via appropriate extraction algorithm. Performance of technique is evaluated for various gain, bit rate, different cover images and potential attacks. In addition, subjective evaluation is also performed for the method. The outcomes show that the suggested technique has a significantly higher robustness and security than former schemes.

2.1. Introduction

Nowadays users can transmit and download multimedia data like images and video over internet [143]. However one of issue related with internet is that, data is not secure against copying, storing, deletion or tampering. Some procedure is needed to avoid the unauthorized user/uses of data. So watermarking is found to be one of capable technique to protect integrity of digital data. However an efficient watermarking scheme is required to maintain confidentiality of media contents. In this method, for authentication purpose some data is embedded inside cover image.

Some robust and imperceptible watermarking schemes using multiple transform schemes are developed in [109-111]. In [109], author imperceptibly embedded thorax image watermark in the transform domain of the cover. The scheme modified the singular value of the cover with the singular value of watermark. The results demonstration on selected images showed that the technique is robust for dissimilar attacks. Harish et al. [111] described hybrid

watermarking method using DWT, DCT and SVD. The principal components of watermark are embedded in DCT domain of DWT decomposed host image. Shivani et al.[118] has proposed a watermarking technique using DCT and listless SPIHT. Further, security of technique is enhanced by using Chinese remainder theorem. Next, SPIHT provides better robustness along with good image quality. It has been reported that the technique outperforms against common watermarking attacks. A digital watermarking approach using hierarchical listless (HL) and discrete Tchebichef transform (DTT) is introduced by Senapati et al.[120]. Experimental results in term of PSNR and SSIM clearly prove better performance of scheme against attacks. Further, embedding and recovery time of the watermark is less than the DCT based watermarking scheme.

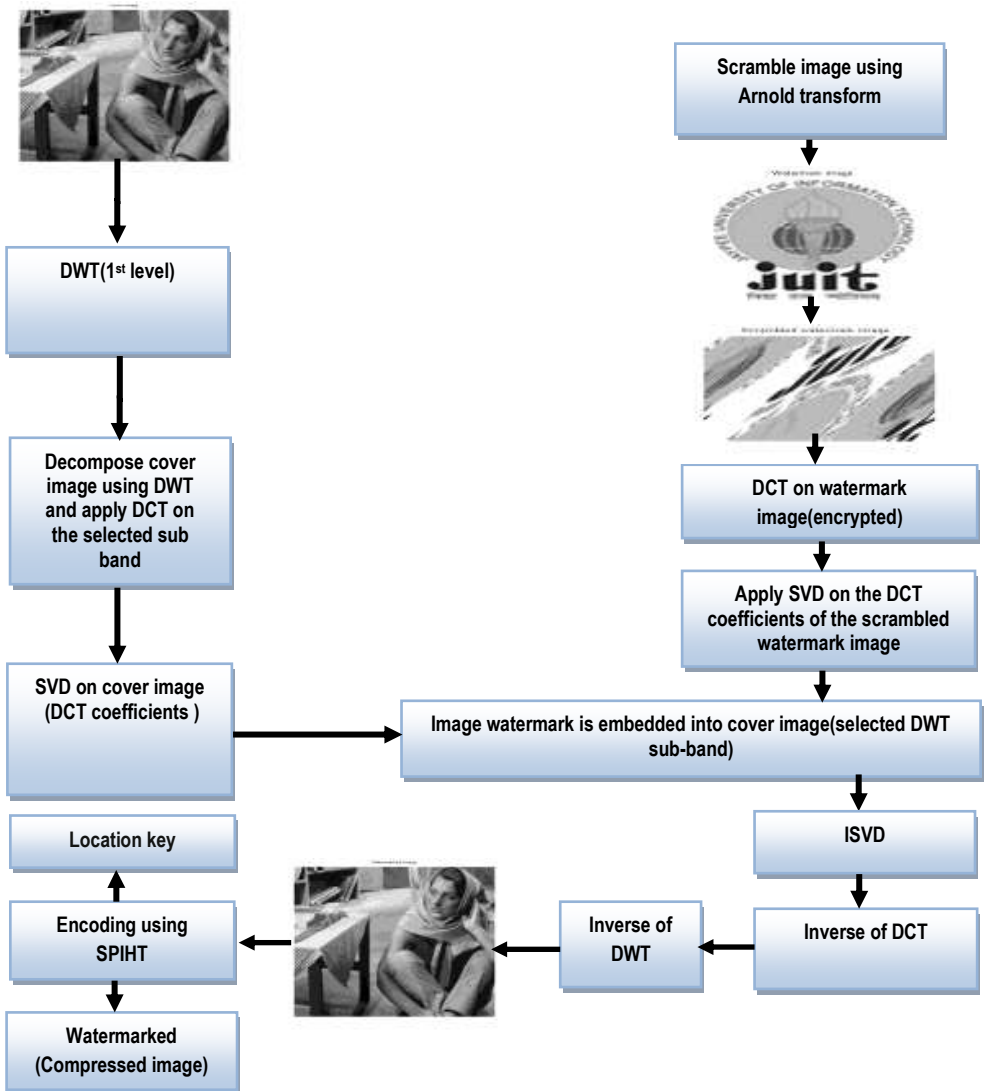
In this chapter, an improved SPIHT based robust and distortion control digital watermarking in DWT-DCT and SVD domain is proposed. The main contribution of our work is identified as follows :

- It is evident that combination of DWT-DCT and SVD based watermarking technique performed superior to the technique based on DWT, DCT, or SVD individually or the fusion of any two of them [18].
- The scrambled version of watermark image is determined by Arnold transform [134] prior to insertion into the cover image. Hence, confidentiality of the secret watermark image is improved.
- To reduce the storage cost, enhance transmission efficiency and better visual quality, watermarked data is compressed by SPIHT prior to transmission on the open channel.
- As results indicated in Table 2.1-Table 2.8, our technique offer excellent performance for various attacks and found superior robustness to other DWT based techniques [108,118,119,120].
- Refer Table 2.9, Subjective method is used to calculate the visual quality of the marked image.
- Watermarking is used to reduce the extra bandwidth demand of digital data and hidden data act as keywords for fast retrieval [112].

Rest of the chapter is structured as follows. The proposed technique is introduced in Section 2.2. The outcome and result study is presented in Section 2.3.

2.2 Proposed SPIHT based watermarking technique

Fig. 2.1 shows the complete process of our proposed technique. The combination of DWT-DCT-SVD and SPIHT is used to provide robust and distortion control watermarking technique using digital image. Initially in embedding process cover image 'Barbara' is decomposed by DWT. Further DCT is applied on selected sub-band of DWT and singular value is obtained for DCT cover image. Next, scrambled version of the logo watermark is obtained prior to embedding. Further, SVD is used to determine the singular value of the DCT scrambled logo image. Finally, the scrambled watermark image is embedded into the cover image. Further, compressed watermarked image is obtained after applying SPIHT encoding on watermarked image. The recovery of watermark is obtained via reverse of embedding process. The reverse process of embedding is used to obtain the extracted watermark.



(a)

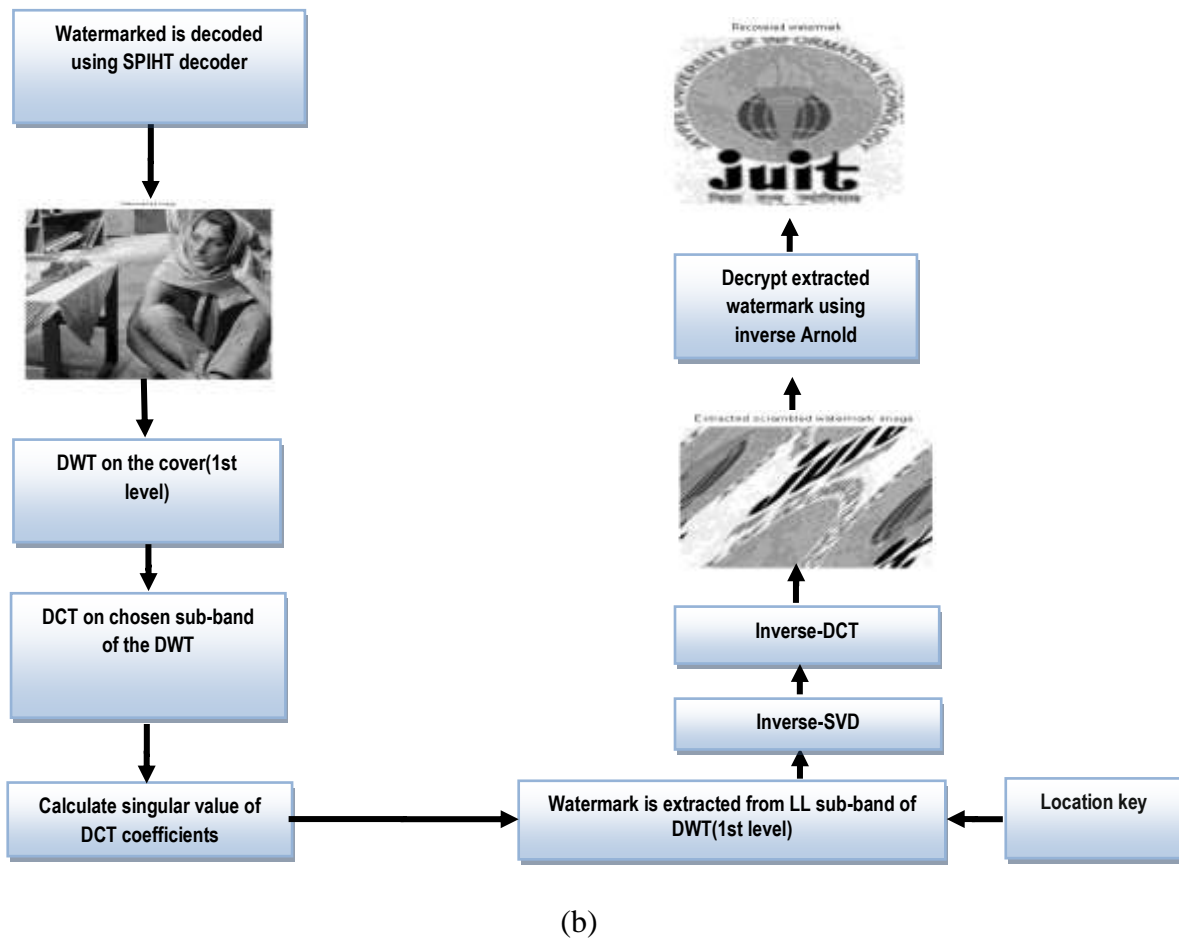


Fig 2.1: SPIHT based watermark (a) embedding and (b) extraction process

2.3. Experimental outcomes

All the experiments were conducted using MATLAB (ver. 13). In this scheme, cover (size: 512×512) and watermark (Size: 256×256) are used for experiments [Internet source: https://www.bing.com/images/search?sp=-1&pq=bottlecapswithhinges&sc=1-24&sk=&cvid=E05E08632494486CB86D9B4FA66D5806&q=Bottle+caps+with+hinges+&qft=filterui:license-L2_L3_L4&FORM=IRFLTR; <http://www.juit.ac.in/>]. Fig.2.2 represents some samples of our cover and watermark images.



Fig. 2.2: (i) cover image, (ii) logo watermark (iii) watermarked image.

Standard metrics such as PSNR, SSIM and NC are considered to determine the performance of our approach. The detail of the considered metric is presented in Chapter 1.

The results in terms of standard metric is provided in Table 2.1-Table 2.8. Table 2.1 depicts the PSNR, NC and SSIM value (without any attacks) of our method at varying gain and found that the value of PSNR, NC and SSIM is above 25.31 dB, 0.9422, and 0.971311, respectively. NC and SSIM result under various attacks at gain=0.17 are listed in Table 2.2. It can be seen that, highest NC and SSIM results are obtained as 0.9992 and 0.989342, respectively under compression attacks. However, SSIM values are poor under rotation attack. Table 2.3 demonstrates about PSNR, SSIM and NC results for various cover and watermark images. It can be observed that highest PSNR, SSIM values are above 28.55 dB, 0.992088, respectively. However NC values are poor for Barbara/baboon and Boat/Finger. Table 2.4 depicts the performance of proposed scheme against considered cover/watermark at fixed gain (0.07). It can be seen that best value of PSNR, SSIM values are above 26.65 dB, 0.976750, respectively for different images. However, NC value is poor against Barbara-Baboon images.

As clearly mentioned in section 2.1, our technique uses fusion of DWT-DCT-SVD along with wavelet based compression (SPIHT) to provide better performance than former techniques [109, 118, 119, 120].

Table 2.5 shows the PSNR, SSIM and NC results for the considered image in comparison with similar techniques[118-120], using different bit rate ranges. When the bit rate value high, the proposed method achieve high imperceptibility and robustness.

Table 2.1: Experimental observation against different gain value

Gain	PSNR(dB)	NC value	SSIM value
0.01	38.47	0.9422	0.999954
0.08	35.35	0.9935	0.997615
0.09	34.68	0.9950	0.997003
0.1	34.025	0.9962	0.996330
0.17	30.07	0.9984	0.989905
0.3	25.31	0.9990	0.971311

Table 2.2: Performance against various attacks

Applied attacks	Variation in Noise	Measured NC value	Obtained SSIM (after attacks)
Salt & Pepper with varying noise	0.001	0.9969	0.985077
	0.003	0.9853	0.97658
	0.005	0.9713	0.968246
	0.01	0.9424	0.949458
	0.02	0.8959	0.912951
	0.1	0.7005	0.677389
	0.5	0.5810	0.190452
Gaussian Noise with changing variance	0.001	0.9874	0.978836
	0.003	0.9502	0.95878
	0.005	0.9219	0.939639
	0.01	0.8569	0.895718
	0.02	0.7906	0.81776
JPEG- compression process	10	0.9969	0.979408
	30	0.9987	0.986209
	60	0.9988	0.987701
	80	0.9990	0.989342
	100	0.9992	0.989325
Cropping	(20 20 400 480)	0.8970	0.789895
	(250 300 550 700)	0.8952	0.789895
Rotation	300	0.9984	0.295227
	500	0.9984	0.260456
	700	0.9984	0.353285
	1000	0.9984	0.393222
Scaling	(0.5)	0.5563	0.707554
	(1.5)	0.5227	0.812598
Sharpening Mask	0.1	0.9297	0.946208
	0.3	0.9306	0.94849
	0.5	0.9313	0.950011
	0.7	0.9318	0.951043
Median Filter-Attack	(4 4)	0.9528	0.976881
	(10 10)	0.9578	0.960935
	(20 20)	0.7936	0.923243
	(50 50)	0.7936	0.923243
Histogram attack		0.6736	0.719232

Table 2.3: Performance of proposed method under considered cover images

Cover/ Watermark	Peak signal to noise ratio(dB)	SSIM	NC
Barbara/ Baboon	32.82	0.994922	0.9846
Lena/ Cameraman	30.00	0.993811	0.9965
Boat/ Finger	30.13	0.992587	0.9846
Barbara/ Juit logo	28.55	0.992088	0.9973
MRI/ Thorax	34.68	0.995857	0.9950

Table 2.4: Experimental results against varying bit rate

(Cover-Watermark)	Bit rate	PSNR (measured in dB)	Structure similarity index	Robustness(NC)
(Lena-Baboon)	0.25	32.73	0.992862	0.9705
	0.5	35.03	0.995941	0.9911
	1	36.21	0.996982	0.9892
	1.5	36.55	0.997233	0.9885
	2	36.59	0.997262	0.9896
	2.5	36.70	0.997341	0.9896
	3	36.72	0.997355	0.9902
(Barbara-Baboon)	0.25	26.65	0.976750	0.8812
	0.5	29.91	0.989215	0.9827
	1	33.22	0.995107	0.9815
	1.5	34.38	0.996312	0.9878
	2	34.69	0.996582	0.9933
	2.5	34.95	0.996793	0.9933
	3	35.02	0.996845	0.9937
(Boat-Baboon)	0.25	29.10	0.982170	0.9491
	0.5	31.76	0.990536	0.9875
	1	33.75	0.994158	0.9860
	1.5	34.46	0.995089	0.9895
	2	34.76	0.995445	0.9902
	2.5	34.82	0.995515	0.9918
	3	34.93	0.995629	0.9918

It has been noted from table that our method obtained PSNR, SSIM and NC value greater than 32.73 dB, 0.9929 and 0.9705, respectively. However, former technique [118] has PSNR, SSIM and NC value greater than 30.93 dB, 0.8982 and 0.3201, respectively. Further, PSNR, SSIM and NC values offered by [119] is greater than 31.24dB, 0.9075, and 0.1317, respectively. It can also be seen that the PSNR value is greater than 30.93 dB, SSIM value is greater than 0.8974 and NC value is greater than 0.3032, as reported by the method in [120].

Therefore, one can noticed that proposed method achieves high imperceptibility and robustness as compared to other existing approaches [118-120].

Highest NC values as reported by technique [118] are 0.7158, 0.7208, 0.5034, 0.9771, 0.515 against cropping, noise, sharpening, inverting and histogram equalization attack, respectively. However, we have obtained maximum NC as 0.9416, 0.7255, 0.7397, 0.9873 and 0.8165, respectively for the same attacks.

Therefore, it can be seen that the proposed method offer better robustness as compared to former technique [118].

Further, NC value of the proposed method and other similar approach [109] for well known attacks are listed in Table 2.7. The best NC value obtained by the proposed method against Poisson attack is 0.9922. However, the minimum NC value is 0.9126 under pepper and noise attack. The NC values indicate that the method successfully recover the hidden watermark.

It is further seen that the highest reported NC value by existing approach [109] is 0.9973 against Poisson attack. However, lowest reported NC value is 0.8430 against pepper and noise attack.

Table 2.5: PSNR, SSIM and NC performance comparison between proposed technique and other reported techniques

Considered cover images	Applied bit Rate (bpp)	Considered Techniques	Obtained PSNR value (in dB)	Measured SSIM value	Calculated NC value
Cover image(Lena)	0.25	[118]	30.93	0.8982	0.3201
		[119]	31.24	0.9075	0.1317
		[120]	30.93	0.8974	0.3032
		Our method	32.73	0.9929	0.9705
	0.5	[118]	31.36	0.9292	0.9804
		[119]	31.10	0.9167	0.9848
		[120]	31.31	0.9301	0.9828
		Our method	35.03	0.9959	0.9911
	1	[118]	31.13	0.9617	0.9804
		[119]	33.87	0.9600	0.9801
		[120]	34.02	0.9621	0.9797
		Our method	36.20	0.9970	0.9892
	1.5	[118]	34.40	0.9676	0.9149
		[119]	34.35	0.9658	0.9227
		[120]	34.76	0.9677	0.9180
		Our method	36.54	0.9972	0.9885
	2	[118]	34.90	0.9693	0.9257
		[119]	34.83	0.9686	0.9298
		[120]	34.76	0.9677	0.9180
		Our method	36.58	0.9973	0.9896
	2.5	[118]	35.44	0.9740	0.9598
		[119]	35.41	0.9738	0.9510
		[120]	35.33	0.9733	0.9517
		Our method	36.70	0.9973	0.9896
	3	[118]	35.65	0.9739	0.9558
		[119]	35.65	0.9724	0.9490
		[120]	35.52	0.9744	0.9480
		Our method	36.72	0.9974	0.9902
	Lossless at 3.5	[118]	36.00	0.9750	0.9831
		[119]	35.83	0.9762	0.9841
		[120]	35.68	0.9754	0.9747
		Our method	36.77	0.9975	0.9903

Table 2.6: NC Performance comparison between proposed technique and Shivani et al. method[118]

Attacks	Cropping	Noise attack	Sharpening mask	Inverting	Histogram equalization
NC[118]	0.7158	0.7208	0.5034	0.9771	0.5415
NC(Our scheme)	0.9416	0.7255	0.7397	0.9873	0.8165

Table 2.7: Robustness comparison with technique [109]

Mentioned attacks	Considered Gain(K)	Noise-density	NC[109]	NC(Our scheme)
Pepper &Noise attack	0.9	0.01	0.9962	0.9984
		0.02	0.9917	0.9960
		0.03	0.9869	0.9914
		0.06	0.9641	0.9726
		0.08	0.9468	0.9568
	0.7	0.01	0.9961	0.9984
		0.02	0.9910	0.9943
		0.03	0.9823	0.9890
		0.06	0.9508	0.9637
		0.08	0.9277	0.9424
	0.5	0.01	0.9948	0.9981
		0.02	0.9855	0.9913
		0.03	0.9719	0.9220
		0.06	0.8430	0.9430
		0.08	0.8892	0.9126
Speckle-attack	0.9	0.01	0.9981	0.9983
		0.02	0.9906	0.9961
		0.03	0.9849	0.9927
		0.06	0.9631	0.9778
		0.08	0.9458	0.9640
	0.7	0.01	0.9948	0.9980
		0.02	0.9896	0.9952
		0.03	0.9818	0.9901
		0.06	0.9409	0.9679
		0.08	0.9275	0.9500
	0.5	0.01	0.9944	0.9978
		0.02	0.9848	0.9921
		0.03	0.9724	0.9830
		0.06	0.9262	0.9498
		0.08	0.8918	0.9245
Gaussian-attack	0.9	0.01	0.9872	0.9925
	0.7	0.01	0.9841	0.9896
	0.5	0.01	0.9752	0.9831
Poisson-attack	0.9		0.9981	0.9988
	0.7		0.9974	0.9991
	0.5		0.9973	0.9992

Table 2.8 represent the robustness of the proposed method and former approaches [109-111] by performing NC value under popular attacks. Result indicate that our method obtained superior NC value than schemes proposed in [109-111]

Table 2.8: NC Performance comparison between proposed technique and other schemes [109-111]

No. of attacks	NC[109] value	NC [110] value	NC[111] value	NC(Proposed method)
Gaussian	0.9872	0.9762	0.9690	0.9925
Salt & pepper	0.9962	0.9894	0.8940	0.9984
Poisson	0.9981	0.9981	0.9390	0.9992
Speckle	0.9981	0.9981	0.9890	0.9983

We have further determined the quality of marked image by subjective scheme [135] in Table 2.9. In this scheme, different people are involved to confirm the quality of marked image. From this table, quality of the marked image is satisfactory at all considered gain value except the value = 0.3.

Table 2.9: Quality evaluation of marked image by subjective measure

Gain	Imperceptibility(Quality measurement)
0.01	Outstanding
0.08	Very good
0.1	Good
0.17	Acceptable
0.3	poor

In this chapter, an improved SPIHT based robust and distortion control digital watermarking is developed for concealing scrambled watermark image in DWT-SVD-DCT domain. The scrambled watermark offer extra level of security. The developed watermark technique is mainly needed for digital document security for various applications. By applying the SPIHT compression scheme on the watermarked image, the storage and bandwidth demand is

reduced preserving the PSNR performance of the proposed technique. Further, our technique has shown better performance as compared to other similar approaches. In our future work, DWT and SVD may replace with some more appropriate transform domain techniques for dual watermarks to withstand benchmark attacks.

The work presented in this chapter has been published in *Multimedia Tools and Applications*, pp.1-14. doi: 10.1007/s11042-018-6177-0 (Springer). This is declared under the list of publications at the end of the Chapter 6.

CHAPTER 3

RDWT BASED DUAL WATERMARKING IN NSCT DOMAIN

This chapter presents a dual watermarking technique using SPIHT in NSCT domain. In this technique, two images data (logo and signature) is placed inside the cover. The method uses redundant discrete wavelet transform (RDWT), SVD, Arnold transform and SPIHT to makes it more robust than other state-of-the-art approaches. The method is extensively estimated for various gain, five different bit rate, ten different cover images, seven potential wavelet filters and well known attacks. Furthermore, the proposed scheme is also tested for two different forms of the secret data (image and text watermark) instead of the same form of the data. Furthermore, the result of the suggested scheme is obtained superior to other existing techniques under consideration.

3.1. Introduction

Due to continuous and remarkable development of internet people are allowed to easy storage, copy and distribution of digital data for various applications [133, 136-138]. However, copyright protection and digital content authentication are the major issue in the recent time [137-138]. Many researchers used digital image watermarking to address these issues [137-139]. It is important to see that the transform domain techniques are more popular to achieve better robustness than spatial techniques [18].

Out of the transform domain techniques, DWT is widely used for image watermarking [140]. However, shift sensitivity and poor directionality are some of issue related with DWT that are avoided by redundant wavelet transforms (RDWT) [141]. Due to excellent property of RDWT [1, 34, 143], most of the information is preserved during forward and backward transformation. In addition, NSCT have also shift invariant and rich directional information. A blind watermarking approach using RDWT-SVD based on 4×4 image block is introduced by Ernawan et al.[144]. Further, human visual system (HVS) entropy is calculated for cover image block. Furthermore, watermark is scrambled by Arnold encryption to produce chaotic image prior to embedding into selected blocks of lower HVS entropy. Experimental results show that proposed method can survive against most of common watermarking attacks. However computational cost of method is high due to presence of RDWT and Arnold encryption.

In [145], Khare et al. suggested a watermarking technique, which placed a watermark inside the RDWT-DCT-SVD domain of the host image. The scheme achieves good robustness for various kinds of attacks. An approach based on RDWT and block SVD is proposed by Gaur et al. [146]. Two watermarks are embedded inside cover image for additional security. Further, second watermark (MNNIT logo) is scrambled by Arnold scheme prior to embedding process. The technique found high capacity result. However there is small degradation in image quality. A novel watermarking approach based on scale-invariant feature transform (SIFT) and non- subsampled transform (NSCT) is introduced by Hua et al.[123]. Initially SIFT is used to extract high invariance feature points of image. Finally, extracted feature points are placed with secrete data using NSCT. The technique is found to be robust against noise and having better capability, good capture quality and tampering resistance.

Due to rich property of NSCT, RDWT and SVD in image processing applications, a NSCT, RDWT and SVD based dual watermarking technique is proposed in this chapter. The technique uses combination of NSCT, RDWT and SVD along with SPIHT compression scheme to provide robust and imperceptible system for digital document security. The key role of the suggested scheme is summarized below.

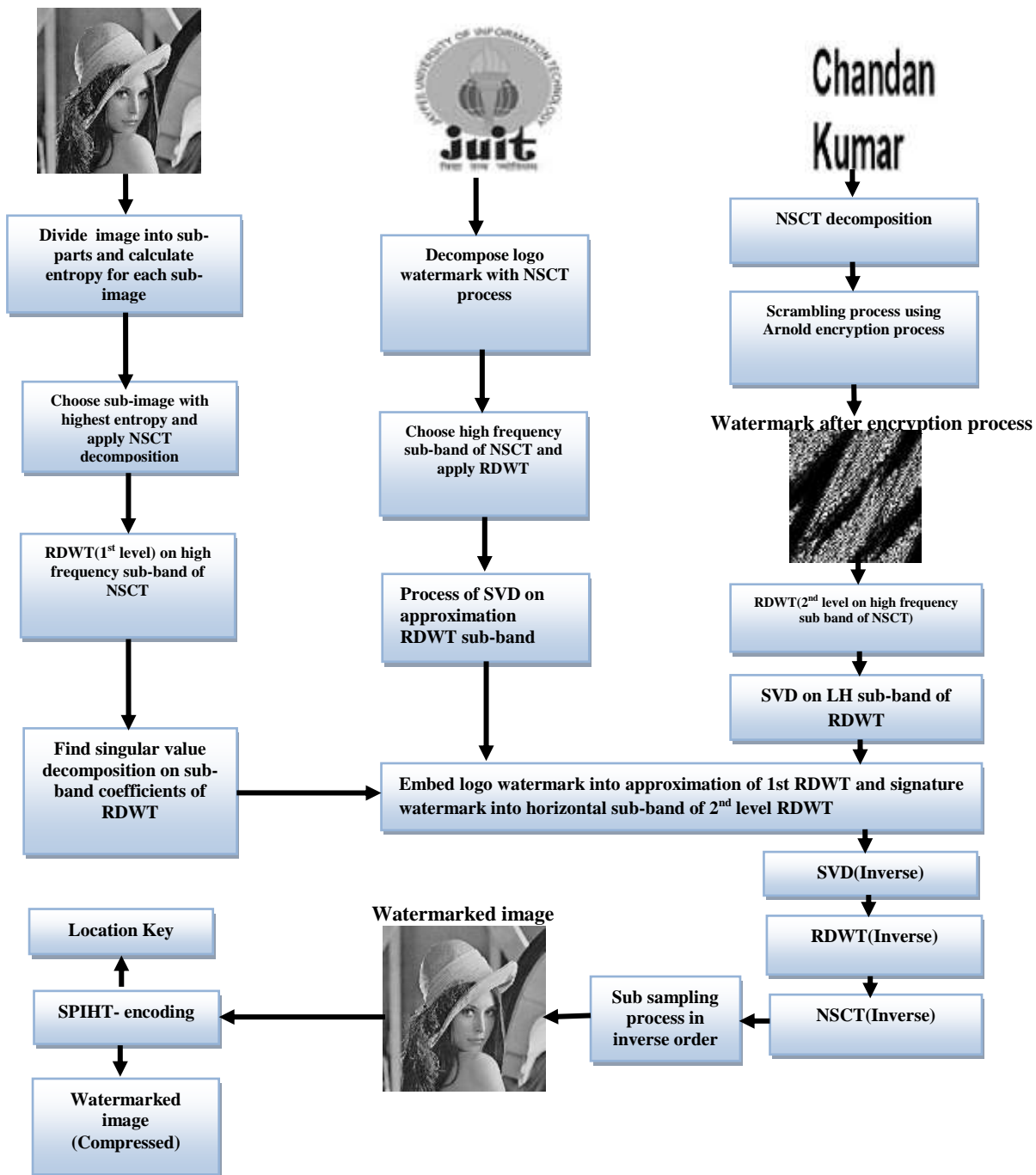
- Shift sensitivity and poor directionality are some of issue related with DWT. Use of RDWT and NSCT enhance the robustness [141]. Further, SVD provide very stable singular value against geometrical attacks which is required for efficient watermarking techniques.
- Uses SPIHT [118] to compress the marked image prior to transmission on open channel. This compressed form of the image reduce the storage and bandwidth cost. In addition, compression ratio can also be controlled due to presence of exact rate control which leads to better reconstruction of image.
- Dual watermarks are used to improve the security of the scheme.
- Refer the results indicated in Table 3.6 and 3.11; the NC value of our scheme is superior to other similar approaches under consideration [34,141].
- Finally, confidentiality of watermark is further maintained by Arnold transform [134]. Unauthorized recovery of watermark is not possible even after extraction.

3.2. Proposed method

In this work, firstly, the method uses the sub-image having highest entropy and NSCT is applied on it. Next, we apply RDWT to NSCT image to obtain the RDWT image. RDWT

image is further transform via SVD to obtain the singular vector of the image (cover). The method obtained singular vector for both watermarks with similar procedure. Here, the signature watermark first scrambled via Arnold transform before SVD applied on it. Furthermore, the method uses singular vectors of both watermark to modify (embed) the vector of cover image. The inverse of the above process generates a watermarked image. Finally, compressed version of the marked image as obtained via SPIHT is efficiently transmitted on open (unsecure) channel. At the receiver end, user decompresses the information first and, then robustly extracts the secret data via appropriate extraction algorithm. The complete process involved in our scheme is presented in Fig. 3.1.

Host image (Dimension:512×512) Logo-watermark (Dimension:256×256) Signature-watermark (Dimension:128×128)



(i)

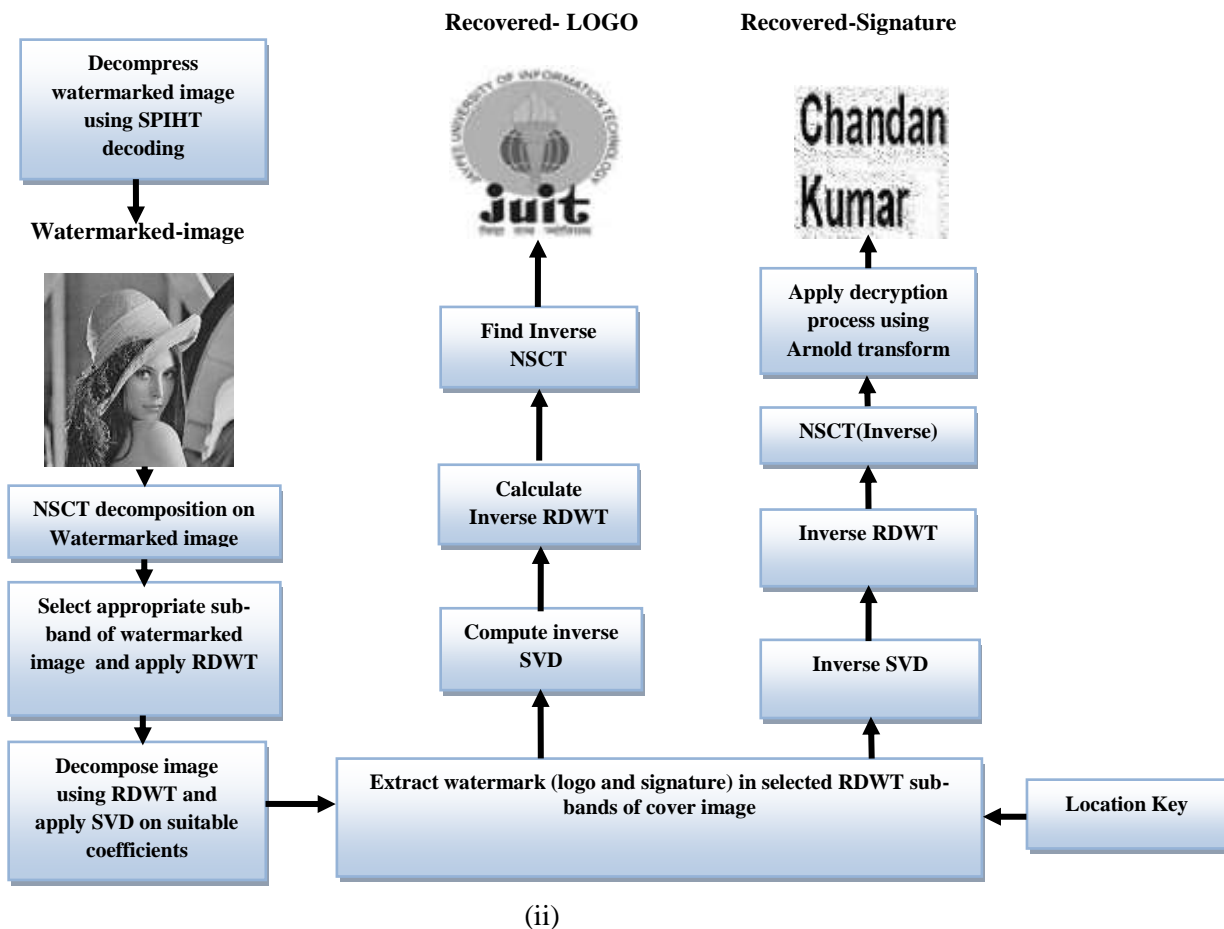


Fig. 3.1: Embedding (i) and extraction (ii) process

3.2.1 Algorithm for watermarking embedding

Embedding of the watermarks involve following steps:

1. Sub-sampling of cover image 'CI'(size:512×512)

$$CI_1 = CI(2\mu - 1, 2\beta - 1)$$

$$CI_2 = CI(2\mu - 1, 2\beta - 1)$$

$$CI_3 = CI(2\mu - 1, 2\beta - 1)$$

$$CI_4 = CI(2\mu - 1, 2\beta - 1)$$

$$\text{where } \mu = 1, 2, \dots, M/2 \text{ and } \beta = 1, 2, \dots, M/2. \quad (3.1)$$

2. Consider highest entropy as EN and applying 1st level NSCT on 'EN' which produce two low frequency and four high frequency sub-bands as given below:

$$[EN_{Y1}, EN_{Y2}, EN_{Z111}, EN_{Z112}, EN_{Z121}, EN_{Z122}] \leftarrow \text{NSCT}[EN] \quad (3.2)$$

EN_{Y1}, EN_{Y2} denotes low frequency sub bands and $EN_{Z111}, EN_{Z112}, EN_{Z121}, EN_{Z122}$ represents sub-bands having high frequency.

3. RDWT (first level) on EN_{Z121} (having sub-band with high frequency).

$$[EN_{A11}, EN_{H11}, EN_{V11}, EN_{D11}] \leftarrow \text{RDWT}[EN_{Z121}] \quad (3.3)$$

Here $EN_{A11}, EN_{H11}, EN_{V11}$ and EN_{D11} are the approximations, horizontal, vertical and diagonal sub-band respectively

4. Calculate SVD for ' EN_{A11} ' and ' EN_{H11} ' sub-bands.

$$[U_{ENA11}, S_{ENA11}, V_{ENA11}] \leftarrow \text{SVD}[EN_{A11}] \quad (3.4)$$

$$[U_{ENH11}, S_{ENH11}, V_{ENH11}] \leftarrow \text{SVD}[EN_{H11}]$$

5. Apply NSCT decomposition (1st level) on both watermarks. Further, apply scrambling on watermark 2 using Arnold transform

$$[W11_{T11}, W11_{T22}, W11_{B1111}, W11_{B1112}, W11_{B1121}, W11_{B1122}] \leftarrow \text{NSCT}[W1]$$

$$[ARW22_{T11}, ARW22_{T22}, ARW22_{B1111}, ARW22_{B1112}, ARW22_{B1121}, 2ARW2_{B1122}] \leftarrow \text{AR1}\{\text{NSCT}[W2]\} \quad (3.5)$$

Where $W11_{T11}$ and $W11_{T22}$, are sub-bands with low frequency and

$W11_{B1111}, W11_{B1112}, W11_{B1121}$ and $W11_{B1122}$ are sub-band with high frequency.

6. RDWT (1st level) on $W11_{B1121}$, and $ARW22_{B1121}$.

$$[W11_{A11}, W11_{H11}, W11_{V11}, W11_{D11}] \leftarrow \text{RDWT}[W11_{B1121}] \quad (3.6)$$

$$[ARW22_{A11}, ARW22_{H11}, ARW22_{V11}, ARW22_{D11}] \leftarrow \text{RDWT}[ARW22_{B1121}]$$

Here

$W11_{A11}, W11_{H11}, W11_{V11}, W11_{D11}$ and $ARW22_{A11}, ARW22_{H11}, ARW22_{V11}, ARW22_{D11}$ denotes approximation, horizontal, vertical and diagonal sub bands formed after forward RDWT transformation of $W11_{B1121}$ and $ARW2_{B1121}$ respectively.

7. Singular value of $W11_{A11}$ and $ARW22_{H11}$ sub-bands for both watermarks

$$[U_{W11A11}, S_{W11A11}, V_{W11A11}] \leftarrow \text{SVD}[W11_{A11}] \quad (3.7)$$

$$[U_{ARW22H11}, S_{ARW22H11}, V_{ARW22H11}] \leftarrow \text{SVD}[ARW22_{H11}]$$

8. Singular value of both watermarks modified the Singular value of cover image ('logo' and encrypted 'signature').

$$\begin{aligned} S_{111} &= S_{ENA11} + \alpha \times S_{W11A11} \\ S_{222} &= S_{EH11} + \alpha \times S_{ARW22H11} \end{aligned} \quad (3.8)$$

Here ' α ' is considered gain factor value.

9. Calculate inverse of the process(see Fig. 3.1) to obtain Watermarked image (I_w)
10. Implement SPIHT compression technique on watermarked image(I_w)

3.2.2 Watermark recovery algorithm

Steps are as follow:

1. Decoding of watermarked image by SPIHT.
2. Apply sub-sampling on watermarked image ' I_w ' followed by selection of sub-image with higher entropy (E_w) using Eq. 1.
3. Apply 1st level NSCT on ' E_w '. Perform RDWT on E_{WB1121} as used in Eq. 2.

$$[E_{Wp1}, E_{WQ1}, E_{WR1}, E_{WS1}] \leftarrow \text{RDWT}[E_{WB1121}] \quad (3.9)$$

4. Calculate SVD of E_{Wp1} and E_{WQ1}

$$[U_{E_{Wp1}}, S_{E_{Wp1}}, V_{E_{Wp1}}] \leftarrow \text{SVD}[E_{Wp1}] \quad (3.10)$$

$$[U_{E_{WQ1}}, S_{E_{WQ1}}, V_{E_{WQ1}}] \leftarrow \text{SVD}[E_{WQ1}]$$

5. Image and text watermark

$$S_{C1} = (S_{E_{WA1}} - S_{EA1}) / \alpha \quad (3.11)$$

$$S_{C2} = (S_{E_{WH1}} - S_{EH1}) / \alpha \quad \text{Where } \alpha \text{ is gain.}$$

6. Inverse SVD on S_{C1} and S_{C2} .
7. Inverse of RDWT and NSCT to recover both watermarks.
8. Inverse Arnold on encrypted signature watermark.

3.3. Experimental results

To determine the performance of the proposed work, we used MATLAB version 2013b and the size of cover Lena image (512×512 pixel) and two watermarks logo (256×256 pixel) and signature (128×128 pixel) utilized for testing purpose [Internet source: <https://www.bing.com/images/search?sp=-1&pq=bottlecapswithhinges&sc=1->

24&sk=&cvid=E05E08632494486CB86D9B4FA66D5806&q=Bottle caps with hinges &qft= filterui:license-L2_L3_L4&FORM=IRFLTR; <http://www.juit.ac.in/>].

PSNR[137,147,148], NC and SSIM [9] are used as standard metric to evaluate the performance of our proposed technique. NC_1 and NC_2 is the notation used to determine robustness of logo and signature watermarks, respectively. Figure 3.2 demonstrates cover image, watermarks and watermarked images. However, Figure 3.3 represents recovered watermarks. Figure 3.4 demonstrates attacked watermarked and recovered watermarks. The PSNR, NC_1 , NC_2 and SSIM performance is depicted in Table 3.1- Table 3.5.

Table 3.1 depict the PSNR, NC_1 , NC_2 and SSIM values of our technique at varying gain and bit rate. We found that value of PSNR, NC_1 , NC_2 and SSIM are above 34.21 dB, 0.9874, 0.9204, and 0.966211, respectively. PSNR, NC, SSIM results against various cover images is shown in table 3.3. Highest value of PSNR, NC_1 , NC_2 , and SSIM are 40.97 dB, 1, 0.9495 and 0.999391, respectively for various considered images.

NC and SSIM results under various attacks at gain=0.5 are presented in table 3.4. It can be observed from table that highest NC's are obtained as 1, 0.9497, respectively against different attacks. However SSIM value is poor against Gaussian noise.

NC and SSIM performance for various filters is depicted in table 3.5. It has been observed from table that highest PSNR, NC_1 , NC_2 , values are 36.37 dB, 1, 0.9576 respectively under various wavelet filters. However SSIM value is poor under 'db4' filter.

As clearly mentioned in section 3.1, our method uses combinations of RDWT, SVD, Arnold transform and SPIHT to make it more robust and secure than other state-of-the-art approaches [34, 141].

Table 3.6 represent the robustness of proposed method and former approaches [34,141] by performing NC value. Result clearly state that our method achieved 1 score for NC for most of the considered attacks. However, minimum NC offered by our method is 0.9378 against Histogram-equalization.

It has been further observed that former technique[34] do not maintain the standard score for NC. The highest NC value offered by former technique is 0.9951 against average filtering attack. However, lowest NC value is 0.8481 against Gaussian noise attack. Further, best NC value for technique [141] is 0.9965 against Gaussian noise attack. However, lowest NC value is reported as 0.9902 against histogram-equalization attack.

Therefore, it can be seen that proposed method offer better robustness as compared to existing techniques [34,141] with minimum distortion.



Fig. 3.2: (1) cover-image, (2) logo-image, (3) signature-image and (4) watermarked-image.



Fig. 3.3: Extracted watermarks (logo(1) & signature(2))

























Attacks	watermarked image	Logo watermark (Recovered)	Signature watermark (Recovered)
Salt and pepper with density=0.01			
Gaussian-noise(mean=0,var=0.01)			
Median Filtering [2 2]			
JPEG compression having Quality Factor=50			
Histogram- equalization			
Cropping(20 20 400 480)			
Speckle-noise using density=0.05			
Average-filtering			

Fig.3.4: Performance under various attacks

Table 3.1: Performance under bit rate=1, 2, 3 and varying gain

Bit rate	Gain(k)	PSNR (dB)	NC ₁	NC ₂	SSIM values
1	0.01	35.16	0.9880	0.9206	0.995838
	0.1	35.13	0.9998	0.9461	0.995814
	0.5	34.45	1	0.9426	0.995077
	0.9	33.44	1	0.9357	0.993743
2	0.01	36.06	0.9875	0.9204	0.996658
	0.1	36.03	0.9998	0.9460	0.996639
	0.5	35.20	1	0.9424	0.995885
	0.9	34.21	1	0.9354	0.994793
3	0.01	36.51	0.9874	0.9205	0.997002
	0.1	36.48	0.9998	0.9461	0.996982
	0.5	35.54	1	0.9423	0.966211
	0.9	34.50	1	0.9353	0.995148

Table 3.2: Performance under fixed gain (0.5) and various bit rates

Different bit rate values	PSNR(in dB)	NC ₁	NC ₂	Obtained SSIM
1	34.45	1	0.9426	0.995077
1.5	34.81	1	0.9423	0.995487
2	35.20	1	0.9424	0.995885
2.5	35.37	1	0.9423	0.996053
3	35.54	1	0.9423	0.966211

Table 3.3: Performance results of considered cover images

Considered cover images	PSNR (in dB)	NC ₁	NC ₂	SSIM values
MRI	35.53	1	0.9410	0.996254
Barbara	30.52	1	0.9383	0.990362
Baboon	31.11	1	0.9495	0.989492
Boat	33.12	1	0.9412	0.992881
Finger	32.29	1	0.9484	0.981948
Bird	40.97	1	0.9340	0.997978
Cameraman	34.38	1	0.9456	0.997526
Coins	38.89	1	0.9441	0.998765
Moon	40.18	1	0.9364	0.999391
Tire	39.40	1	0.9328	0.998987

Table 3.4: Performance of proposed technique against various attacks

Considered attacks	NC ₁	NC ₂	SSIM
Salt & pepper(den=0.01 and 0.08)	1	0.9409	0.952470
	& 0.9996	& 0.9497	& 0.736758
Gaussian noise(var=0.01 and 0.5)	0.9959	0.9436	0.941818
	& 0.9959	& 0.9436	& 0.181960
Median filter[2 2]	1	0.9432	0.982875
JPEG compression (QF=50)	1	0.9426	0.994507
Histogram equalization	1	0.9378	0.896734
Cropping(20 20 400 480)	1	0.9430	0.229037
Speckle noise	0.9998	0.9494	0.829628
Average filtering	0.9999	0.9485	0.993254

Table 3.5: Reported PSNR, NC's and SSIM values for different filters

Wavelet Filters	PSNR (dB)	NC ₁	NC ₂	SSIM
Sym4	34.63	1	0.9549	0.995285
db4	34.61	1	0.9552	0.995265
Bior 4.4	36.37	1	0.9547	0.997038
Coif4	34.82	1	0.9575	0.995498
Bior6.8	36.16	1	0.9576	0.996742
dmey	35.45	1	0.9539	0.996132
haar	35.54	1	0.9423	0.996211

Table 3.6: Robustness comparison of our technique with [34, 141]

Attacks on watermarked image	Ref.[34]	Ref.[141]	Our scheme			
			Using 'Haar' filter		Using 'Bior 6.8' filter	
			NC ₁	NC ₂	NC ₁	NC ₂
Salt &Pepper (dens =0.01)	0.9867	0.9912	1	0.9409	1	0.9576
Salt & Pepper (dens=0.08)	0.9544	0.9905	0.9996	0.9497	0.9998	0.9573
Gaussian noise(mean=0,var=0.01)	0.8481	0.9965	0.9959	0.9436	0.9999	0.9574
Gaussian noise(mean=0, var=0.5)	0.8481	0.9865	0.9959	0.9436	0.9975	0.9560
Median filter(window size[2 2])	0.9390	0.9949	1	0.9432	1	0.9576
JPEG (QF-50)	0.9935	0.9951	1	0.9426	1	0.9576
Histogram-equalization	0.9942	0.9902	1	0.9378	1	0.9575
Cropping attacks(20 20 400 480)	0.9935	-	1	0.943	1	0.9576
Speckle noise(Den=0.05)	0.9929	0.9948	0.9998	0.9494	0.9999	0.9573
Average filtering	0.9951	-	0.9999	0.9485	1	0.9574

3.3.1 Performance measurement for different form of secret data

The above proposed scheme is also tested for two different forms of the secret data (image and text watermark) instead of the same form of the data (image). In this technique, the text watermark is placed inside image watermark to generate dual watermark. The resulted watermark is imperceptibly placed inside the cover. The detail description of the process is depicted in Fig. 3.5. The method uses text watermark of size 104 bits. Fig. 3.6 depicts the cover image Lena, text watermark, dual watermark(combined) and watermarked images. However, both extracted watermarks are presented in Fig. 3.7. The attacked watermark images and extracted watermarks are shown in Fig 3.8. In addition to the other performance metric as discussed for above method in section 3.3, bit error rate (BER) [75] is used to determine the robustness of the text watermark.

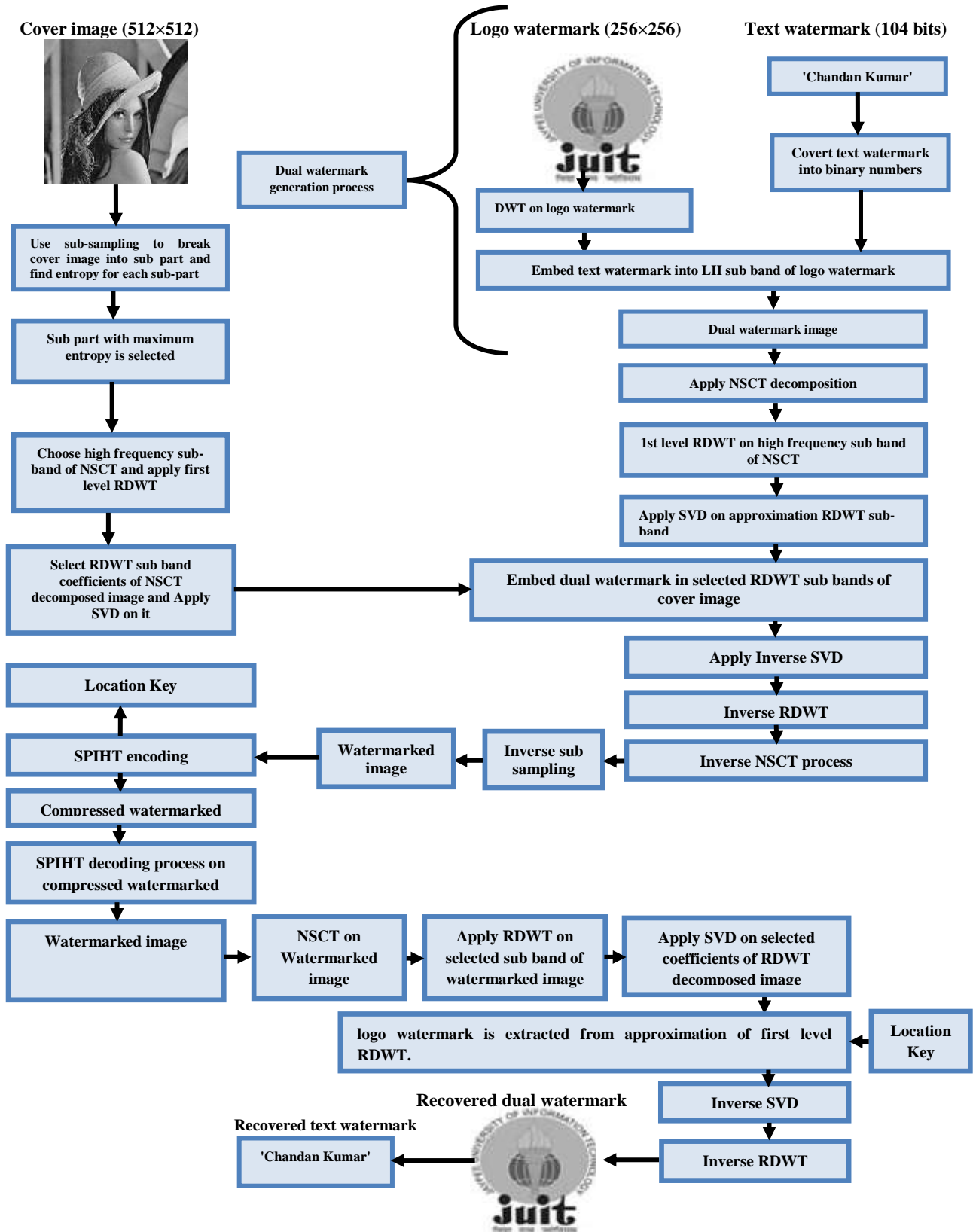


Fig. 3.5: Proposed embedding and extraction process

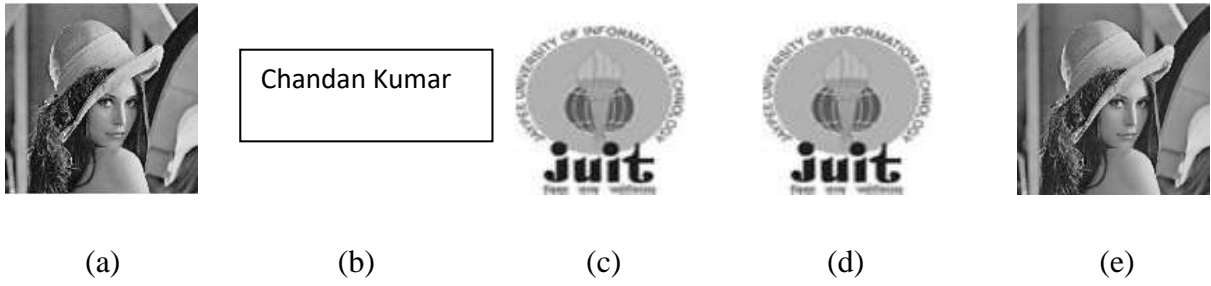


Fig. 3.6: (a) Host image, (b) Text watermark, (c) Logo watermark, (d)Generated dual watermark, and (e) Watermarked image



Fig. 3.7: Recovered watermarks(a)logo and (b) text

















Type of attack	Attacked watermarked image	Recovered Logo watermark	Recovered text watermark
Salt and pepper noise(density=0.01)			Chandan Kumar
Gaussian noise(mean=0, variance=0.01)			Chandan Kumar
Median Filter Attack[2 2]			Chandan Kumar
JPEG compression(QF=50)			Chandan Kumar
Histogram equalization			Chandan Kumar
Cropping(20 20 400 480)			Chandan Kumar
Speckle noise(Density=0.05)			Chandan Kumar
Average filtering[9 9]			Chandan Kumar

Fig. 3.8: watermarked (attacked) and watermarks (extracted) images

Table 3.7 depicts the performance under varying gain and bit rate value. It has been clearly observed from table that value of PSNR, NC, BER and SSIM are greater than 35.68 dB, 0.9999, 0 and 0.9963, respectively. Due to better performance at gain value 0.5 and bit rate 3, all other experiments are evaluated under these values. Further, performance of proposed scheme is checked for various cover images in Table 3.8. From this table, the value of PSNR, NC and SSIM are above 30.81 dB, 0.9918 and 0.9907, respectively. However, BER value is zero for all cover images. Table 3.9 depicts the outcome of the proposed technique for different attacks with respect to NC, BER and SSIM. It can be seen that, highest NC and SSIM results are obtained as 1 and 0.9946, respectively against different attacks. However, best BER value is zero.

Table 3.10 shows the performance of the suggested scheme for 'bird' image at varying bit rate and gain = 0.5. It has been clearly noted from table that significant values of PSNR, NC and SSIM are 45.78 dB, 0.99990 and 0.9996, respectively at bit rate = 3.

Further, NC and BER values of proposed method and other similar approach[141] for well-known attacks are listed in Table 3.11. The best NC value obtained by proposed method is 0.9999 against median filter, JPEG Compression and Histogram equalisation. However, the minimum NC value is 0.9993 under salt and pepper noise and Gaussian noise attack. The NC values clearly indicate that method can extract the hidden watermark at low distortion.

It is further noted that the best NC value obtained by former method[141] is 0.9986 against salt and pepper noise. However, lowest reported NC value is 0.9870 against Gaussian noise attack. Further, BER values of our technique are less than the technique reported in [141].

Therefore, it is established that the proposed method offered better performance as compared to its peers. Due to RDWT, SVD, Arnold transform and SPIHT, our method achieves optimal trade-off between imperceptibility and robustness.

Table 3.7: Performance measurements under different gain and bit rates

Bit rate	Gain factors	PSNR (dB)	NC	BER	SSIM
1	0.01	34.56	0.9999	0	0.9952
	0.1	34.56	0.9999	0	0.9952
	0.5	34.57	0.9999	0	0.9952
	0.9	34.57	0.9999	0	0.9952
2	0.01	35.31	0.9999	0	0.9960
	0.1	35.31	0.9999	0	0.9960
	0.5	35.32	0.9999	0	0.9960
	0.9	35.33	0.9999	0	0.9960
3	0.01	35.67	0.9999	0	0.9963
	0.1	35.67	0.9999	0	0.9963
	0.5	35.68	0.9999	0	0.9963
	0.9	35.68	0.9999	0	0.9963

Table 3.8: Experimental results for different cover images

Cover images	PSNR(dB)	NC	BER	SSIM
MRI	36.66	0.9918	0	0.9965
Barbara	30.81	0.9999	0	0.9880
Baboon	35.52	0.9999	0	0.9907
Boat	33.68	0.9999	0	0.9913
Finger	32.80	0.9999	0	0.9793
Bird	45.83	1	0	0.9996
Cameraman	34.81	1	0	0.9971
Coins	41.15	1	0	0.9988
Moon	42.09	1	0	0.9995
Tire	43.01	1	0	0.9994

Table 3.9: Performance under different attacks for cover image ‘Lena’

Attacks	NC	BER	SSIM
Salt and pepper noise(density=0.01,0.08)	1 & 0.9996	0 & 0.0096	0.9522 & 0.7349
Gaussian noise(mean=0,variance=0.01,0.5)	0.9999 & 0.9960	0.0288 & 0.0192	0.8592 & 0.1817
Median filter[2 2]	1	0	0.9837
JPEG compression (QF=50)	1	0	0.9946
Histogram equalization	1	0	0.8968
Cropping(20 20 400 480)	1	0.0192	0.7667
Speckle noise(Density=0.05)	0.9975	0.0192	0.8291
Average filtering	0.9999	0	0.9930

Table 3.10: Results for image ‘Bird’

Bit rate	PSNR	NC	BER	SSIM
1	45.05	0.9999	0	0.9994
2	45.47	0.9999	0	0.9995
3	45.78	0.9999	0	0.9996

Table 3.11: Comparison of proposed technique under various attacks

Attacks	Singh et al.[141]		Proposed method	
	NC	BER	NC	BER
Salt & pepper noise(density=0.1 ,0.5)	0.9986 and 0.9981	0.0253 and 0.1180	0.9994 and 0.9993	0.0096 and 0.0288
Gaussian noise(mean=0,variance=0.01 and 0.001)	0.9870 and 0.9965	0.0120 and 0.0032	0.9993 and 0.9995	0.0288 and 0
Median filter[2 2] and [3 3]	0.9950 and 0.9949	0.0132 and 0.0131	0.9999 and 0.9999	0 and 0
JPEG compression(QF=10,50)	0.9951 and 0.9951	0.0178 and 0.0126	0.9999 and 0.9999	0 and 0
Histogram equalization	0.9902	0.0098	0.9999	0
Speckle noise(density=0.05)	0.9948	0.0052	0.9995	0.0050

A dual watermarking using SPIHT in NSCT domain is developed in this chapter. The method uses redundant discrete wavelet transform (RDWT), SVD, Arnold transform and SPIHT to makes it more robust than other state-of-the-art approaches. Furthermore, the proposed scheme is also tested for two different forms of the secret data(image and text watermark) instead of the same form of the data. From the results indicated from Table 3.1 to 3.11, it is confirmed that the proposed work is suitable for the digital document security for several applications. Future works will focus on improving the security of the proposed method at low cost.

The work presented in this chapter has been published in *Concurrency and Computation: Practice and Experience*, pp.1-14, doi: 10.1002/cpe.4912 (Wiley) and second paper published in the 5th International Conference on Parallel, Distributed and Grid Computing (PDGC), 2018, pp.111-114 ,doi: 10.1109/PDGC.2018.8745789. This is declared under the list of publications at the end of the Chapter 6.

CHAPTER 4

DUAL WATERMARKING APPROACH THROUGH SECURE FORCE (SF) ENCRYPTION

This chapter presents a robust and secure dual watermarking approach in NSCT domain. The idea is same as our previous technique (RDWT based dual watermarking in NSCT domain as discussed in chapter 3), however, this approach uses secure force (SF) encryption (after compressing the watermarked image via SPIHT) to provide better security at low cost. It is established that secure force algorithm not only provides security, but it has low complexity than other encryption techniques. Extensive assessment of the approach confirmed that the method is secure, robust, distortion-less and has low computational complexity which outperforms the other existing approaches.

4.1 Introduction

Presently, digital data gradually become important references for a variety of notable applications[137]. Due to popularity of internet tools, these data are easily and quickly exchanged via network. However, it is important to see that security of intellectual property and digital information needs more attention for practical applications [138]. For this sake, remarkable encryption, steganography and watermarking schemes have been introduced [138]. Many researchers used joint encryption-watermarking scheme to protect the digital contents and intellectual property [147-149].

A hybrid technique using cryptography and watermarking is introduced by Sonali et al.[147]. After embedding, watermarked image is encrypted by secure force encryption algorithm. The method found good MSE result. However, the PSNR was low. A dual watermarking approach using LSB and DCT along with hybrid cryptography is introduced by Singh et al.[148]. Security is further enhanced by converting text watermark into QR code. The outcome showed that the technique is secure. A robust technique using DWT and SVD is proposed by Kaur et al.[149]. Further, visual cryptography is applied to generate two shares of watermark image. Finally, one share is embedded into cover image and another is shared with users for watermark extraction. Technique is found to be robust and secure against various attacks.

In this chapter, an encryption based multiple watermarking technique in NSCT-RDWT domain is developed. The major role of the work is recognized as follows :

- RDWT provides shift invariance which is required for significant embedding and extraction of watermark. Further, NSCT also provide good directionality along with shift invariance which helps in better reconstruction of images. However SVD provides robustness against geometrical attacks [141].
- SPIHT is optimized for progressive image transmission. It converts the image into sequence of bits based on priority of transform coefficient of image. Most significant coefficient are transmitted first which helps in bandwidth efficient transmission [118].
- Multiple watermarks are placed inside the cover image to increase the security. Simulation results clearly prove better performance of scheme than other similar approaches under consideration [142].
- Used secure force (SF) encryption on compressed watermarked image to provide better security at low cost.

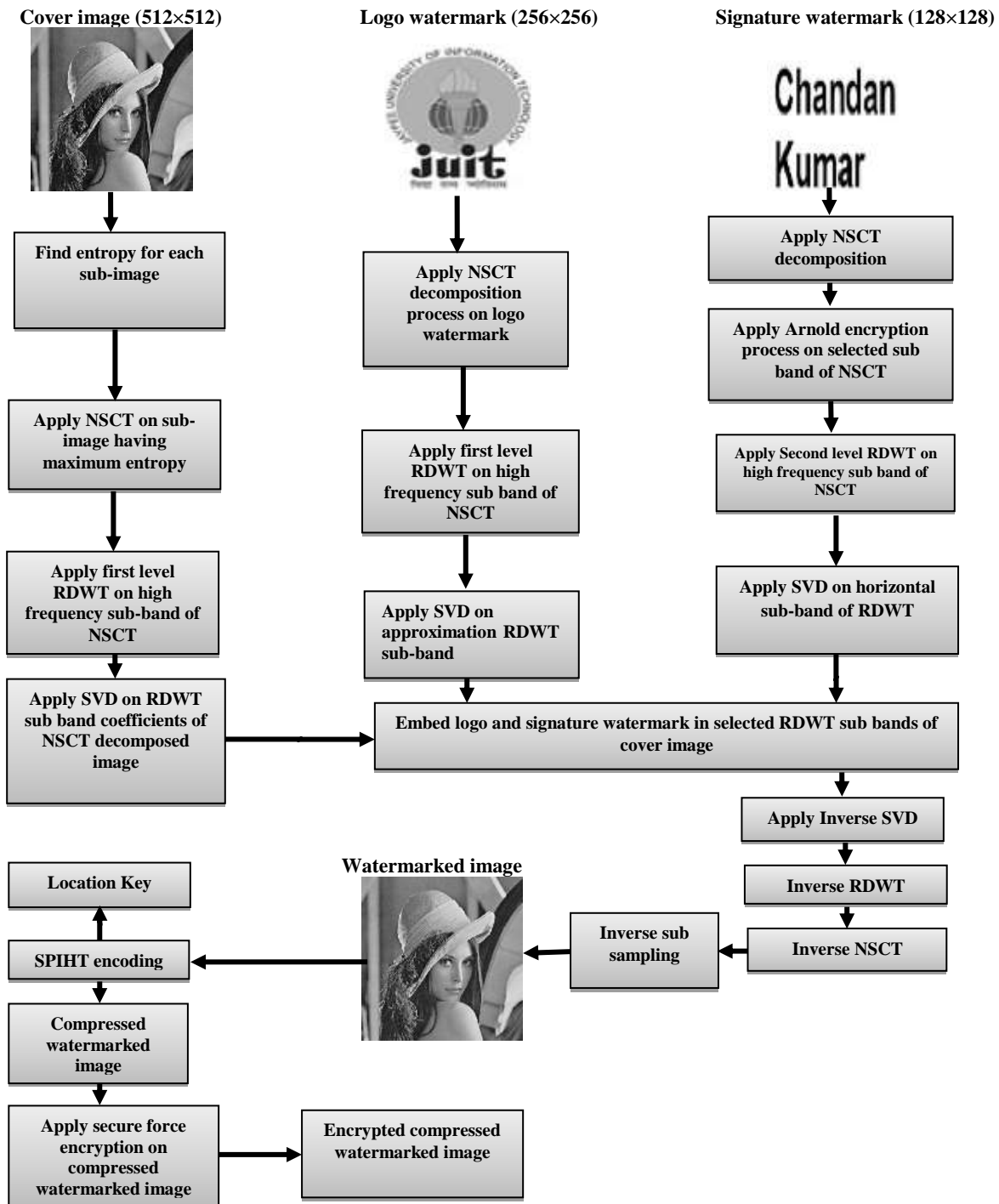
4.2 The proposed method

Our work aim is to provide better authentication of the data. In this work, firstly, NSCT is used to apply on sub-image containing maximum entropy. Next, we apply RDWT to NSCT image and the resulting image is further transform via SVD to obtain the singular value of the cover image. We also obtained the singular value of both watermark by same process. Here, the signature watermark first scrambled via Arnold transform prior to SVD applied on it. Furthermore, the method uses singular vectors of both watermark to modify (embed) the vector of cover. The inverse of SVD, RDWT, NSCT and inverse sub sampling generates a watermarked image. Further, compressed watermarked image is obtained to reduce the bandwidth needs by the channel. Finally, a secure force (SF) encryption is applied on compressed watermark to provide better security at low cost. At the receiver end, user decrypts and decompresses the information first and, then robustly extracts the secret data via appropriate extraction algorithm. The proposed algorithm is depicted in Fig 4.1.

4.3 Experimental results

All simulations are performed with MATLAB 2013b and cover image ('512×512'), logo ('256×256') and signature ('128×128') are considered for experiments [Internet source: https://www.bing.com/images/search?sp=-1&pq=bottlecapswithhinges&sc=1-24&sk=&cvid=E05E08632494486CB86D9B4FA66D5806&q=Bottle caps with hinges &qft= filterui:license-L2_L3_L4&FORM=IRFLTR; http://www.juit.ac.in/]. All results are measured using PSNR, NC, NPCR and UCAI. All these performance metric have discussed in Chapter 1. In this work,

NC_1 and NC_2 is the notation used to determine robustness of logo and signature watermarks, respectively. Fig.4.2 depicts the cover images, logo and signature watermark, and watermarked image. Fig. 4.3 shows the recovered hidden data. The attacked watermarked and recovered watermarks images are shown in Fig. 4.4. Test results under different gains and bit rates are demonstrated in table 4.1. Peak value of PSNR is reported as 36.50 dB.



(a)

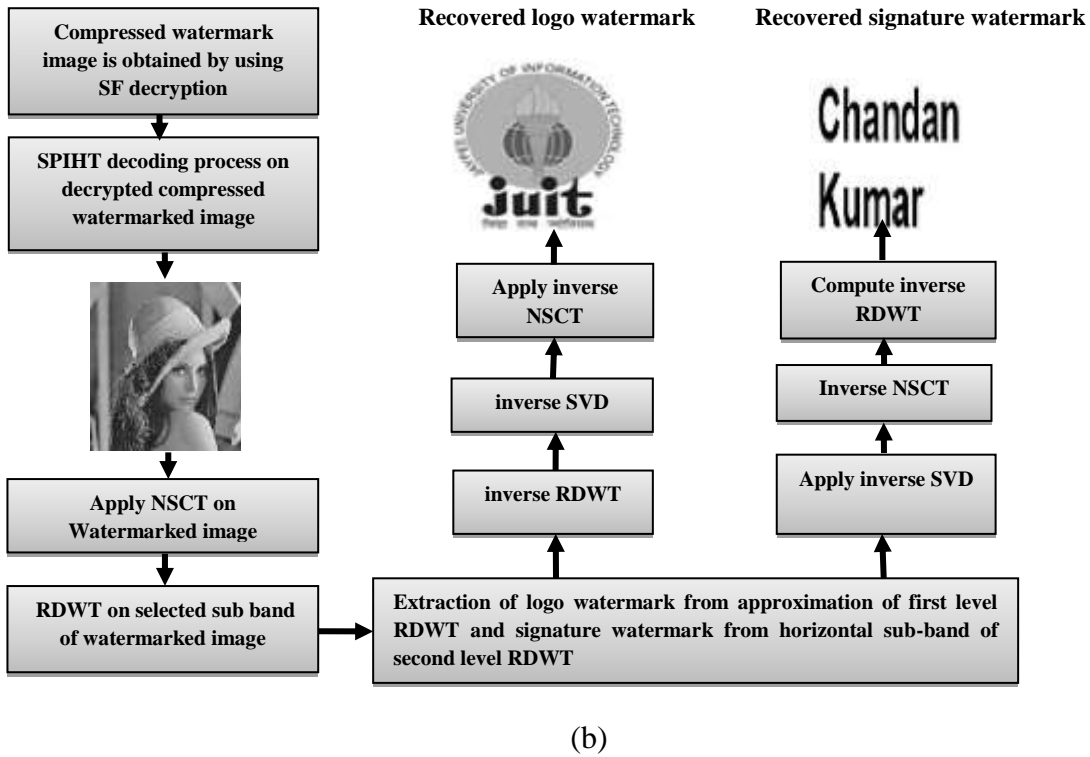


Fig. 4.1: Diagram representing (a)embedding(b)extraction procedure.

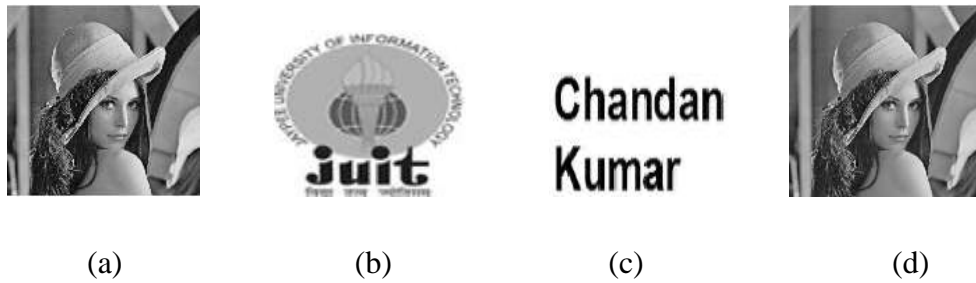


Fig. 4.2: (a) cover image, (b) logo & (c) signature watermark, and (d) watermarked image



Fig. 4.3: Recovered (a) logo & (b) Signature, watermark

























Type of attack	Attacked watermarked image	Recovered watermark 1	Recovered watermark 2
Salt and pepper noise(density=0.01)			
Gaussian noise(mean=0,variance=0.01)			
Median Filter Attack[2 2]			
JPEG compression(QF=50)			
Histogram equalization			
Cropping(20 20 400 480)			
Speckle noise(Density=0.05)			
Average filtering[9 9]			

Fig. 4.4: Watermarked(attacked) and watermarks(extracted) images

Lowest value for PSNR is reported as 35 dB (at gain=0.9 & rate=1). Although best $NC_1=1$ against various gains and bit rate. Next, minimum value for NC_1 is reported as 0.9873. However, the value of NC_2 is greater than 0.8555. From this table, we further seen that the proposed method offer best results at gain =0.5. Table 4.2 demonstrates PSNR, NC_1 and NC_2 values under different cover images at gain = 0.5 and bit rate =3. Best obtained PSNR is 45.83 dB for cover image ‘Bird’. However, highest noted $NC_1 =1$ for cover image ‘Bird’, ‘Cameraman’, ‘Coins’, ‘Moon’ and ‘Tire’ , respectively. Minimum NC_1 is 0.9918 for ‘MRI’ image.

Table 4.3 represents the robustness performance with respect to NC_1 and NC_2 against geometrical and signal processing attacks. It is clear from table that best reported value of $NC_1=1$ under most of the attacks and lowest value of $NC_1=0.9960$ for Gaussian noise. Further, maximum and minimum values of NC_2 are reported as 0.9551 (for Histogram equalization) and 0.9080 (for Gaussian noise attack), respectively.

Table 4.4 illustrate the assessments of NC, NPCR and UACI value for image ‘bird’ at varying rate and fixed gain (0.5). It is noted from table that highest PSNR value is 45.83 dB. However, lowest PSNR = 45.06 dB. Further it has been observed that highest $NC_1= 0.9999$ against all considered bit rates. Best $NC_2 =0.9553$ at bit rate=1 and 3. However, smallest NC_2 value is 0.9552. Furthermore, highest NPCR value is reported as 0.9994. However, maximum and minimum values of UACI are 0.3011(against at bit rate=1) and 0.3006(against at bit rate=3), respectively.

As clearly mentioned in section 4.1, our technique uses combination of RDWT, NSCT and SPIHT along with secure force encryption scheme to provide higher robustness and security at very low cost.

Table 4.5 represents the better performance of our method as demonstrated by comparing its results in terms of NC values with that of the former approach [141]. Highest NC result offered by the approach [141] is 0.9965 against Gaussian noise attack. However, our method maintains the standard score for NC (i.e. 1) for salt and pepper, median filter, JPEG-compression and histogram-equalization attacks.

It can be clearly seen from NC values that the proposed method offer better robustness as compared to former technique [141].

Table 4.1: PSNR, NC1, NC2 values for proposed method

Bit rate	Gain	PSNR (dB)	NC1	NC2
1	0.01	35.16	0.9879	0.8555
	0.1	35.14	0.9998	0.9385
	0.5	35.08	1	0.9426
	0.9	35	1	0.9553
2	0.01	36.06	0.9874	0.8555
	0.1	36.04	0.9998	0.9383
	0.5	35.98	1	0.9547
	0.9	35.90	1	0.9552
3	0.01	36.50	0.9873	0.8555
	0.1	36.49	0.9998	0.9382
	0.5	36.42	1	0.9546
	0.9	36.33	1	0.9552

Table 4.2: Performance of various images against gain=0.5 and bit rate =3.

Cover-images	PSNR(dB)	NC1	NC2
MRI	36.66	0.9918	0.8567
Barbara	30.81	0.9999	0.9548
Baboon	35.52	0.9999	0.9513
Boat	33.68	0.9999	0.9548
Finger	32.80	0.9999	0.9468
Bird	45.83	1	0.9553
Cameraman	34.81	1	0.9537
Coins	41.15	1	0.9539
Moon	42.09	1	0.9547
Tire	43.01	1	0.9551

Table 4.3 : Implementation of various attacks on cover image 'Lena' at constant gain=0.5 and bit rate=3.

Attacks	NC1	NC2
Salt & pepper (den=0.01,0.08)	1 & 0.9996	0.9546 & 0.941
Gaussian noise(mean=0,var=0.01,0.5)	0.9999 and 0.9960	0.9491 and 0.9080
JPEG compression (QF=50)	1	0.9548
Histogram equalization	1	0.9551
Cropping(20 20 400 480)	1	0.9545
Speckle noise(den=0.05)	0.9975	0.9169
Average filtering	0.9999	0.9515

Table 4.4: Performance of considered host image ‘Bird’ at gain=0.5 and changing bit rate.

Bit rate values	PSNR (measured in dB)	NC1for image watermark	NC2 for text watermark	NPCR	UACI
1	45.06	0.9999	0.9953	0.9994	0.3007
2	45.50	0.9999	0.9552	0.9994	0.3006
3	45.83	0.9999	0.9553	0.9994	0.3011

Table 4.5: Performance of proposed method against technique in ref.[141]

Attacks	Singh et al. [141]	NC1	NC2
Salt-Pepper noise(Dens=0.01, 0.08)	0.9912	1	0.9546
	and 0.9905	and 0.9996	and 0.9410
Gaussian-noise(Mean=0, Var=0.01, 0.5)	0.9965	0.9999	0.9491
	and 0.9865	and 0.9960	and 0.9080
Median- filter[2 2]	0.9949	1	0.9550
JPEG-compression(QF=50)	0.9951	1	0.9548
Histogram-equalization	0.9902	1	0.9551

This chapter described embedding of dual watermark in NSCT-RDWT-SVD domain. In this method, NSCT is applied on highest entropy sub-part of the cover image. The resulting image is further transformed by RDWT-SVD to obtain the singular component. Same operation is performed for watermark images. Then, both watermarks are placed inside RDWT domain of the image. Finally, we have applied secure force (SF) encryption algorithm on compressed watermarked image to increase the security of the image and reducing the bandwidth demand during transmission. Extensive assessment with respect to PSNR, NC, NPCR and UACI confirmed that the method is secure, robust, distortion-less at low computational complexity. The results also confirmed that our technique is superior to former schemes. In the future, it would be interesting to develop a more robust and secure algorithm for digital documents. In

addition, how to adapt the proposed framework to solve the noisy channel problem efficiently would also be investigated in future work.

The work presented in this chapter has been published in 2nd International Conference on Advances in Computing, Control and Communication Technology, University of Allahabad, India, September – 2018, pp. 92-96. doi: 10.1109/IAC3T.2018.8674013 (IEEE).

CHAPTER 5

IMPROVED DWT-SVD BASED DIGITAL IMAGE WATERMARKING THROUGH HAMMING ERROR CORRECTION AND ARNOLD TECHNIQUE

In this chapter, an improved DWT-SVD based watermarking approach is developed. The method jointly uses hamming code and Arnold technique to provide robustness and security, respectively. In the embedding process of image and text watermarks, the method uses DWT to decompose the cover image. Second, the selected component of DWT is transform by SVD. The image watermark details first scrambled by Arnold transform and the resulted data is divided into equal parts. Each part is imperceptibly embedded into the two different DWT components of the SVD image. However, hamming code uses to encode the other watermark (in the text form) before embedding into the second level of the DWT cover image. Finally, compressed-watermarked image is obtained after applying SPIHT technique. The extraction procedure is implemented in reverse order. Testing with dual watermarks on ten different host images and under various attacks demonstrates that our scheme yields improved robustness with less distortion than competing methods.

5.1 Introduction

Due to the remarkable growth in internet technologies, large amount of multimedia data is easily generated, transmitted and distributed over the computer networks [70]. However, secure transmission of digital data is one of the major issues related with it. For this sake, image watermarking is a best tool to protect ownership and integrity of digital data [1]. Many digital watermarking techniques have been developed in past decade, and many of them embed only single watermark in spatial or transform domain. However, single watermarking techniques have very limited purpose. Recently, dual watermarking schemes are very promising and have great potentials for many applications [9,48,75,130].

It is established that dual watermarking is more suitable for copyright protection and content authentication at the same time. In [130], Shen and Chen introduced the three different ways of dual watermarks embedding into cover image. In first, fragile watermark is placed inside robust watermark to produce new watermark. The resulted new watermark data is placed inside the cover image. According to second method, watermarks may be inserted one after another dynamically. In third, we can embed two watermarks simultaneously.

Further, it can be seen from [130], the third method of dual watermarking is more suitable for quality of the watermarks.

Singh et al. [9] has introduced a dual watermarking method in LWT and DCT domain. In this work, color cover image is considered and two different watermarks (patient report and signature) are embedded inside the same. Results clearly prove that the technique is highly robust against attacks and there is less degradation in quality of watermarked image. Further, it is observed that technique is also computationally low.

In [48], Liu et al. described a watermarking technique for color images. Further 'Y' channel of 'YCbCr' host image is decomposed by DWT to embed robust watermark. However RGB model is selected to embed fragile watermark in watermarked image using spatial domain method. Finally, the outcome against different color images showed that technique is highly imperceptible, robust and is found to be appropriate for copyright protection.

Singh et al.[75] has described a dual watermark embedding method for telemedicine applications. Further, image watermark is partitioned into two parts and same are embedded into different sub-bands of cover image. However, text information is encoded with error correcting code before embedding into cover image. Test results prove that scheme is not only robust but there is less distortion in watermarked image.

In this chapter, an error correction code based watermarking technique in DWT-SVD domain is developed. The method uses fusion of DWT and SVD to embed multi-watermarks into single cover. The watermark is scrambled and text watermark data is encoded by hamming code prior to embedding into the cover. The key role of the work is recognized as follows :

- Robustness is improved using SPIHT along with DWT and SVD. SPIHT [118] has properties of generating bit string that is beneficial for storage and proficient bandwidth transmission.
- The method embeds dual watermarks simultaneously. Hence, the quality of both watermarks is preserved.
- Dual watermarking used to enhance the security of the proposed technique.
- Finally, confidentiality of watermark is further maintained by Arnold transform [134]. Unauthorized recovery of watermark is not possible even after extraction.

5.2 The proposed method

In this work, two watermark logo (size: 256×256) and signature (size: 96 bits) are embedded into cover. SVD is applied on coefficients obtained by application of second level DWT on host image. Further, logo watermark (scrambled) is obtained by applying Arnold transform. Next, scrambled watermark is partitioned into two sub parts (size: 128×128 each). Further, encrypted subparts are placed inside LH and HL sub-band of 1st level DWT respectively. However text information is placed inside diagonal sub-band of 2nd level DWT after applying hamming code. Finally inverse SVD and DWT are applied on watermarked image followed by application of SPIHT to obtain compressed watermarked image. However in extraction, whole process is applied in reverse order. Fig. 5.1 demonstrates the process of watermark embedding and extraction.

5.2.1 Algorithm for watermarks embedding

The main steps for imperceptibly embedding the watermarks algorithm as follow:

Step 1: Variables are declared as:

Lena (X_z) : cover image

Juit(K_z) : ‘logo’ watermark

k: Scale factor

B1_d, B2_d, B3_d, B4_d : cover image(1st level DWT coefficient)

B1_{d1}, B2_{d1}, B3_{d1}, B4_{d1} : cover image (2nd level DWT coefficients)

Rd₁: diagonal matrix for B2_d

Rd₂: diagonal matrix for B3_d

Q_{d1}& P^T_{d1} :Orthonormalmatrix for B2_d

Q_{d2}& P^T_{d2}: Orthonormal matrix for B3_d

Z^a_z: modified values of Rd_k

Q^a_{dz} and P^{aT}_{dz}: Orthonormal matrices for Z^a_z

R^a_{dg}: Diagonal matrix for Z^a_z

Z_{amodi}: DWT coefficient (modified)

Z_d: Watermarked image

Z_c: Compressed watermarked image

Z_r : Uncompressed watermarked image

Z_g : Encrypted watermark image

Step 2: Input cover and watermark image

$X_z \leftarrow$ Lena.bmp (512×512)

$K_z \leftarrow$ Juit.bmp (256×256) (5.1)

Step3: Scramble the watermark by Arnold encryption technique

$A_g \leftarrow$ Arnold_transform(K_z) (5.2)

Step4: DWT (2nd level) on ‘Lena’

[$B_{1d}, B_{2d}, B_{3d}, B_{4d}$] \leftarrow DWT (X_z , wavelet filter);

[$B_{1d1}, B_{2d1}, B_{3d1}, B_{4d1}$] \leftarrow DWT(B_{1d} , wavelet filter); (5.3)

Step5: Calculate singular value

// Sub band B_{2d} and B_{3d} are selected

If (SVD on B_{2d})

$Q_{d1} R_{d1} P_{d1}^T \leftarrow$ SVD(B_{2d})

End if;

If (SVD on B_{3d})

$U_{d2} S_{d2} V_{d2}^T \leftarrow$ SVD(B_{3d})

End if; (5.4)

Step6: Covert string to binary.

$btext \leftarrow$ binary(*Chandankumar*); (5.5)

Step7: Apply hamming error checking technique

$$Z_n \leftarrow \text{error correcting code } (btext) \quad (5.6)$$

Step8: Replace '(0, 1)' with '(-1,1)'

//If L is length of string then bit stream is changed to Z(1) Z(2)..... Z(L) by changing 0 by -1 & 1 by 1

Step9: Embed encrypted Watermark (s)

// scrambled watermark is divided into two parts $Z=Z_1+Z_2$, singular values is modified in B_{2_d} and B_{3_d} sub band with half of the watermark image

For k \leftarrow 0.01:0.1

$$R_{da} + \mu Z_a = Z_z^a; a, z=1,2 \quad (5.7)$$

// HH_{d1} sub-band is selected to embed text watermark

For k \leftarrow 0.01:0.1

Step10: Calculate singular value for modified coefficients of DWT

If(SVD on Z_z^a)then (5.8)

$$[Q_{dz}^a R_{dz}^a P_{dz}^{aT}] \leftarrow SVD(G_z^a) \quad (5.9)$$

End if;

//modified DWT coefficient

$$Z_{amodi} \leftarrow Q_{da}^a R_{dz}^a P_{da}^T \quad (5.10)$$

Step11: watermarked image

$Z_k \leftarrow$ InverseDWT [$LL_{d1}, HL_{d1}, LH_{d1}, Z_n$, wavelet filter];

$$Z_d \leftarrow$$
 InverseDWT (Z_k, G_1^1, G_2^2, HH_d , wavelet filter); (5.11)

end:

Step12: watermarked image is compressed by SPIHT technique

$Z_c \leftarrow$ SPIHT (Z_d) // Z_c is compressed watermarked image

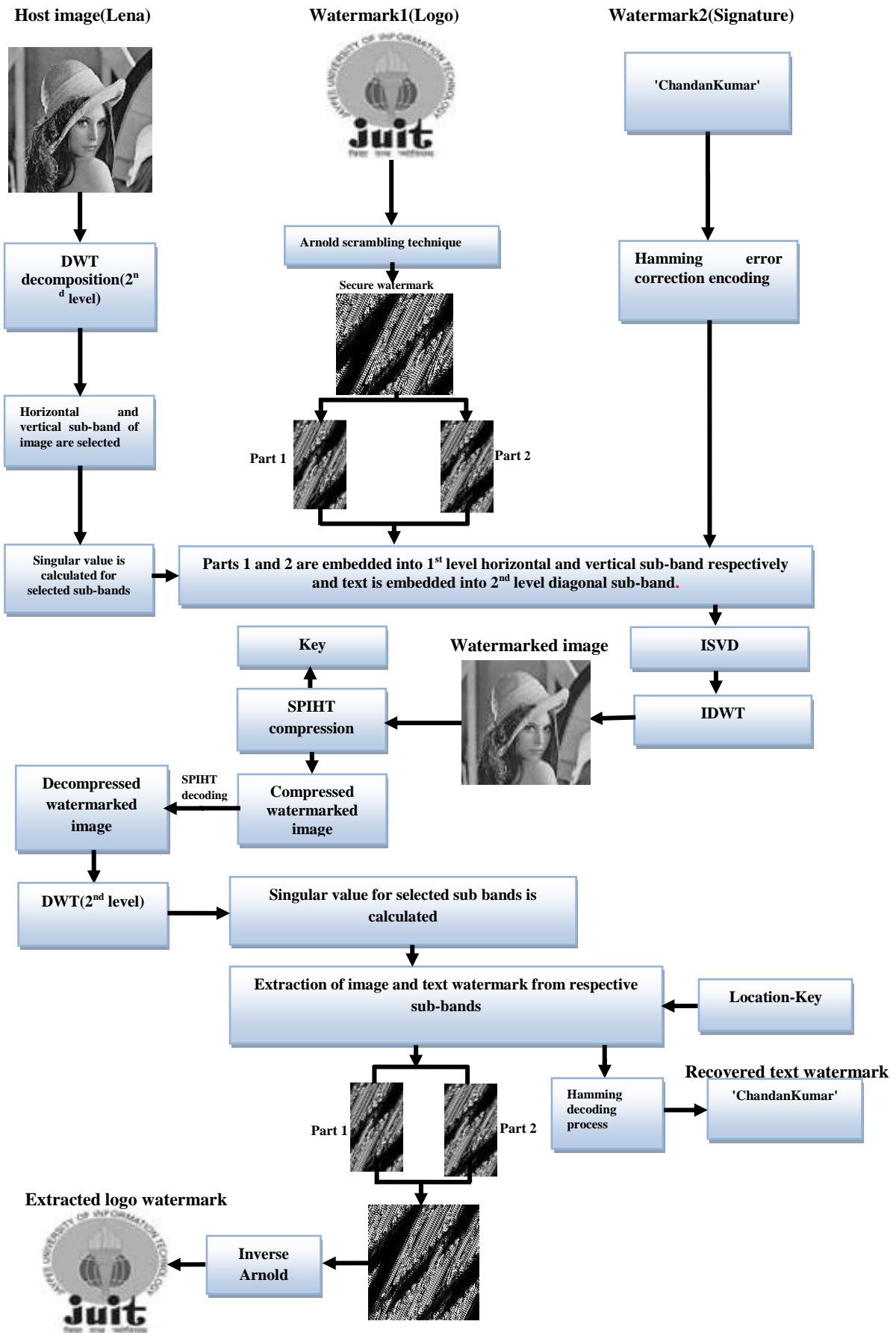


Fig 5.1: Process of embedding and extraction for watermarks

5.2.2 Watermark recovery process

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

Step 1: Variable declared as :

k: Scale-factor

WB1_d, WB2_d, WB3_d,WB4_d:Sub-bands(Watermarked image)

R_{dz1}: Matrices (Orthonormal) for sub-band WB2_d

R_{dz2}: Orthonormal matrices for WB3_d

Q_{dz1} and P_{dg1}^T : Orthonormal matrices for WB2_d

Q_{dg2} and P_{dg2}^T : Orthonormal matrices for WB3_d

DZ: Altered singular value of cover image

Ga: Recovered watermark image

Step 2: SPIHT decoding followed by DWT

SPIHT (Z_c) → Z_r

[WB1_d, WB2_d, WB3_d, WB4_d] ← DWT (Z_r, wavelet filter); (5.12)

Step 3: SVD onWB2_d, WB3_d sub-bands

If (SVD on HL_d) then

Q_{dz1}R_{dz1}P_{dz1}^T ← SVD(WB2_d)

End if;

If (SVD on LH_d) then

Q_{dz2}R_{dz2}P_{dz2}^T ← SVD (WB3_d) (5.13)

Step 4: Calculate value of DZ

DZ ← Q_{dz}^z R_{dza} P_{dz}^{aT}; z=1,2 (5.14)

Step 5: Extract sub-image 1 & 2 and combine them

Z_a = $\frac{Dz - R_{da}}{k}$; a=1,2 (5.15)

end;

//Text watermark extraction

$$Z_{rb} = \frac{f'_{r(p,q)} - f_{r(p,q)}}{\mu f_{r(p,q)}}; f'_{r(p,q)} \text{ represents DWT coefficients}$$

$$Z_{eb} \leftarrow \text{Positive or negative sign } (Z_{rb}); \quad (5.16)$$

Step6: Measure ECC for Z_{eb}

// Final watermark is obtained by replacing '(-1, 1)' by '(0, 1)'.

$$Z_{fb} \leftarrow \text{Ecc}(Z_{eb}) \quad (5.17)$$

Step7: Original watermark is extracted by converting the watermark bits into text

$$\text{Originaltext} \leftarrow \text{convert}(\text{watermarkbits}) \quad (5.18)$$

Step 8: Final logo watermark is applied by applying inverse Arnold transform

end:

5.3 Experimental results and analysis

In this work, ten different types of cover images (with dimensions: 512×512), one watermark, with dimension '256×256' and other text watermark of size 96 bit are considered for experiments [Internet source: [https://www.bing.com/images/search?sp=-1&pq=bottlecapswithhinges&sc=1-24&sk=&cvid=E05E08632494486CB86D9B4FA66D5806&q=Bottle caps with hinges &qft= filterui:license-L2_L3_L4&FORM=IRFLTR](https://www.bing.com/images/search?sp=-1&pq=bottlecapswithhinges&sc=1-24&sk=&cvid=E05E08632494486CB86D9B4FA66D5806&q=Bottle+caps+with+hinges+&qft=filterui:license-L2_L3_L4&FORM=IRFLTR); <http://www.juit.ac.in/>]. Considered cover and watermark images are presented in Fig. 5.2. Extracted logo and signature watermark is demonstrated in Fig. 5.3. Fig. 5.4 represents extracted watermarks and watermarked image after applying attacks.

Table 5.1 depicts the PSNR, NC and SSIM value (without any attack) of our technique at varying gain and bit rate and it has been found that value of PSNR, NC and SSIM is above 30.21 dB, 0.8818 and 0.9864, respectively. However BER is reported as zero in all cases. PSNR, NC, SSIM and BER results are listed in Table 5.2. It can be seen that highest NC and SSIM values are obtained as 0.9950 and 0.9929, respectively. However BER is zero for all bit rates. Table 5.3 depicts PSNR, NC and BER results for different images and fixed gain values and it is found that value of PSNR, NC and SSIM are above 28 dB, 0.9428 and 0.9913, respectively. However, BER is zero for all considered images. NC, SSIM and BER results under various attacks and gain=0.5 is listed in Table 5.4. It can be seen that highest NC and

SSIM are 0.9966 against average filtering and Median filter respectively. However BER is poor under cropping attack. Table 5.5 depicts the PSNR, NC and BER value against 15 and 24 characters and found that value of PSNR, NC and SSIM are above 29.3564 dB, 0.9180 and 0.9855, respectively.

As clearly mentioned in section 5.1, our technique uses fusion of DWT and DCT along with wavelet based compression (SPIHT), hamming error correction and Arnold technique to provide better performance than former techniques [75,118].

Table 5.6 represent the robustness of the proposed method and former technique[75] by performing NC and BER scores.

Highest NC value reported by proposed method is 0.9969 against JPEG compression attack. However, minimum NC value is reported as 0.4158 against salt and pepper noise attack. Further, proposed method achieved 0 scores for BER value for most of the considered attacks. NC and BER values clearly prove successful recovery of hidden watermarks.

It has been further noted that the highest reported NC value by former method [75] is 0.9950 against JPEG compression attack. However, minimum reported NC value is 0.3011 against salt and pepper noise attack.

Table 5.7 represent the robustness of proposed method and former technique [118] for well known attacks. The best NC value obtained by proposed technique is 0.9914 against Gaussian noise attack. However, the minimum NC value is 0.6357 against histogram equalization attack. Therefore, it can be seen that the proposed technique offer better robustness as compared to former method [118].

It is further seen that highest reported NC value reported by existing approach [118] is 0.9771 against Invert attack. However, lowest reported NC value is 0.5034 against sharpening attack.



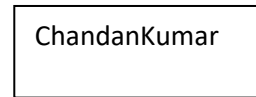
(I)



(II)



(III)

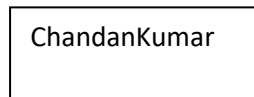


(IV)

Fig. 5.2: (I) Host image, (II) logo (III) signature, and (IV) watermarked image



(I)



(II)

Fig. 5.3: Recovered watermarks, (I) logo and (II) Signature

















Type of attack	watermarked images(after attack)	Logo watermark (extracted)	Signature watermark (extracted)
Salt-pepper(density=0.01)			ChandanKumar
Gaussian noise(mean=0,var=0.01)			ChandanKumar
Median filter [2 2]			ChandanKumar
Jpeg compression(with QF=50)			ChandanKumar
Histogram Equalization			ChandanKumar
Cropping-attack(20 20 400 480)			ChandanKumar
Speckle-noise(having density=0.05)			ChandanKumar
Average filtering attack			ChandanKumar

Fig.5.4: Watermarked (attacked) and watermarks (extracted)

Table 5.1: Performance under various gain factors

Bit rate values	Gain (μ)	PSNR (in dB)	NC	BER	SSIM values
1	0.01	36.79	0.8904	0	0.9968
	0.04	35.11	0.9935	0	0.9957
	0.05	34	0.9939	0	0.9946
	0.1	30.21	0.9936	0	0.9864
2	0.01	36.93	0.8828	0	0.9944
	0.04	35.32	0.9925	0	0.9959
	0.05	34.37	0.9935	0	0.9949
	0.1	30.25	0.9965	0	0.9865
3	0.01	36.97	0.8818	0	0.9969
	0.04	35.35	0.9919	0	0.9959
	0.05	34.39	0.9931	0	0.9909
	0.1	30.27	0.9963	0	0.9866

Table 5.2: Performance against fixed gain value (0.05)

Bit rate	PSNR	NC	BER	SSIM
1	33.15	0.9950	0	0.9929
2	32.49	0.9775	0	0.9924
3	32.52	0.9777	0	0.9925

Table 5.3: Performance evaluation for various cover images

Images	PSNR	NC	BER	SSIM
MRI	32.52	0.9777	0	0.9925
Barbara	28	0.9838	0	0.9926
Baboon	29.6	0.9246	0	0.9533
Boat	29.91	0.9482	0	0.9567
Finger	28.90	0.9428	0	0.9622
Bird	32.45	0.9935	0	0.9834
Cameraman	29	0.9936	0	0.9913
Coins	30.69	0.9947	0	0.9913
Moon	33.20	0.9804	0	0.9974
Tire	32.79	0.9962	0	0.9955

Table 5.4: Performance for image ‘Lena’ against various attacks.

Attacks	NC values	BER	SSIM
Salt & pepper noise attack(with density=0.01,0.08,0.001)	0.5377,0.5175, 0.9914	0	0.9481,0.9462,0.9933
Gaussian noise-attack(mean=0,variance=0.01,0.001,0.002)	0.3765,0.7171,0.5065	0	0.8944,0.9822,0.9687
Median filter[2 2],[3 3]	0.8981,0.8132	0.9432	0.9938,0.9966
JPEG compression (QF=50& QF=80)	0.9871& 0.9959	0	0.9936& 0.9938
Histogram equalization	0.6357	1.4286	0.4363
Cropping(20 20 400 480)	0.7891	4.76	0.2290
Speckle noise attack(at density=0.01, 0.02 &0.005)	0.7421, 0.6119 & 0.8709	0	0.9857, 0.97750 &0.9899
Average filtering	0.9999	0.9485	0.9932

Table 5.5: Performance evaluation for different sized characters under different gain values and fixed bit rate=3.

Gain factor(μ)	24 characters				15 characters			
	PSNR	NC	BER	SSIM	PSNR	NC	BER	SSIM
0.01	36.8822	0.9320	0	0.9964	37.72	0.9180	0	0.9969
0.05	34.1801	0.9958	0	0.9939	34.61	0.9960	0	0.9945
0.1	29.3564	0.9918	0	0.9855	29.49	0.9916	0	0.9859

Table 5.6: Comparison of experimental results against author [75]

Attacks	Author[75]		Proposed method		% improvement (NC)
	NC	BER	NC	BER	
JPEG Compression attack at (QF-100, 60&20)	0.9950,0.9325, 0.9653	0	0.9969,0.9852, 0.9704	0	0.0019
Sharpening mask attack under threshold=0.1, 0.3, 0.5, 0.7 &0.9	0.6073,0.6257, 0.6390,0.6486, 0.6556	0	0.6705, 0.6815, 0.6948, 0.6985	0	0.0654
Median filtering [2 2] and [3 3]	0.9116,0.8885	0	0.8991,0.8132	0	-0.0137
Scaling factor 2&2.5	0.7075,0.6500	0,1.0126	0.7445, 0.6850	0,2.3810	0.0523,0.0538
Gaussian-LPF having standard deviation value= 0.6	0.8780	0	0.8789	0	0.0010
Gaussian noise (with mean = 0 & Var = 0.001, 0.05)	0.7012,0.3150	0,8.5714	0.7171,0.4257	0, 2.3810	0.0227, 0.3514
Salt & pepper (0.001,0.1)	0.7553,0.3011	0	0.9914, 0.4158	0	0.3126
Histogram equalization attack	0.5880	1.4286	0.6357	2.3810	0.0811
Cropping attack(20,20 400,480)	0.7451	4.5714	0.7891	4.7619	0.0590

Table 5.7: Performance of proposed scheme against technique [118]

Attacks applied	Cropping	Noise	Sharpening	Invert-attack	Histogram-Equalization
NC[118]	0.7158	0.7208	0.5034	0.9771	0.5415
NC(proposed work)	0.7891	0.9914	0.6985	0.9821	0.6357
Improvement in percentage	0.1024	0.3754	0.3876	0.0051	0.1739

In this chapter, we developed an improved DWT-SVD based watermarking technique. In our technique, multi-watermark data are placed inside the selected sub-bands of the cover image. The image watermark is scrambled and text watermark data is encoded by hamming code prior to embedding process. Result demonstrations showed that the method is not only robust for various attacks, but also offered superior performance to other competing techniques. In future, we will test the performance of the proposed system for other benchmark attacks such as StirMark, CheckMark, Optimark and Certimark.

The work presented in this chapter has been published in Multimedia Tools and Applications, doi: 10.1007/s11042-019-08314-5 (Springer).

CHAPTER 6

CONCLUSION AND FUTURE DIRECTIONS

In this thesis, we have suggested some improved methods of digital watermarking in wavelet domain. The motivation of this research was to propose some watermarking techniques that produce optimal trade-off among major performance parameters because it is not simple to have any watermarking scheme that produce optimal balance among these parameters.

Initial contribution of chapter 1 start with overview of digital watermarking and review of various robust and secure state-of-the-arts approaches implemented for potential applications. In addition, potential characteristics of digital watermarking, important applications, and different techniques of spatial as well as transform schemes and key metric are discussed.

Chapter 2 presented an improved SPIHT based robust and distortion control digital watermarking for concealing scrambled watermark image in DWT-SVD-DCT domain. Main focus of technique was to improve robustness at acceptable imperceptibility. The scrambled watermark offer extra level of security. By applying the SPIHT compression scheme on the watermarked image, the storage and bandwidth demand is reduced while preserving the visual quality of the image. Performance of technique is evaluated for various gain, bit rate, different cover images and attacks. In addition, subjective evaluation is also performed for the method. Robustness (NC value) of proposed method is up to 0.9992.

A dual watermarking technique using SPIHT in NSCT domain is discussed in Chapter 3. Aim of this chapter was to achieve high capacity, improve robustness and imperceptibility at same time. The method is extensively evaluated for various gain, different bit rate, ten different cover images, seven potential wavelet filters and well known attacks. In addition, subjective evaluation is also performed for the method. Robustness (NC value) of proposed method is up to 1.

Furthermore, the proposed scheme is also tested for two different forms of the secret data (image and text watermark) instead of the same form of the data. Robustness (NC value) of proposed method is up to 1.

Chapter 4 presented an encryption based multiple watermarking in NSCT domain. Main focus of this chapter was to provide enhance security of digital documents at low cost. Extensive assessment of the approach confirmed that the technique is secure, robust,

distortion-less and has low computational complexity which outperforms the other existing approaches. Robustness (NC value) of proposed method is up to 1.

In Chapter 5, we developed an improved DWT-SVD based watermarking technique. In our technique, multi-watermark data is placed inside selected sub-bands of the cover image. The image watermark is scrambled and text watermark data is encoded by hamming code prior to embedding process. Result demonstrations showed that the method is not only robust for various attacks, but also offered superior performance to other competing techniques. Robustness (NC value) of proposed method is up to 0.9999.

Based on the results studies, it can be seen that the PNNR, NC, SSIM, BER are highly depends on gain value, amount of the embedded data and noise variations. The strength of the encryption algorithm is evaluated by NPCR and UACI and it greatly depends on secure force encryption techniques.

We are interesting to observe that the results of our improved techniques are suitable for digital data security in various applications. Further, new technologies such as artificial intelligence, machine learning, deep learning, block chain and turbo code can be included to develop more efficient watermarking algorithm for practical applications. Furthermore, we will extend the proposed technique for other multimedia types such as audio and video.

REFERENCES

- [1] Singh AK, Dave M, Mohan A. Hybrid technique for robust and imperceptible multiple watermarking using medical images. *Multimedia Tools and Applications*. 2016 Jul 1;75(14):8381-401.
- [2] <https://www.comparitech.com/identity-theft-protection/identity-theft-statistics/>
- [3] <https://www.securitas.in/globalassets/india/files/about-us/news---related-documents/identity-theft-is-the-largest-contributor-to-fraud-in-india.pdf>
- [4] Cook J., May (2017) [Online]. Available: <http://www.businessinsider.com/worlds-10-cybercrime-hotspots-in-2016-ranked-symantec-2017-5/#10-vietnam-216-1>.
- [5] Aherrahrou N, Tairi H. A new robust watermarking scheme based on PDE decomposition. In 2013 ACS International Conference on Computer Systems and Applications (AICCSA) 2013 May 27 (pp. 1-5). IEEE.
- [6] Kumar C, Singh AK, Kumar P. A recent survey on image watermarking techniques and its application in e-governance. *Multimedia Tools and Applications*. 2018 Feb 1;77(3):3597-622.
- [7] Mohanty SP. Watermarking of digital images. Submitted at Indian Institute of Science Bangalore. 1999 Jan;1(6).
- [8] Irany BM, Guo XC, Hatzinakos D. A high capacity reversible multiple watermarking scheme for medical images. In 2011 17th International Conference on Digital Signal Processing (DSP) 2011 Jul 6 (pp. 1-6). IEEE.
- [9] 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*. 2019:1-1.
- [10] Giakoumaki A, Pavlopoulos S, Koutsouris D. Multiple image watermarking applied to health information management. *IEEE Transactions on Information Technology in Biomedicine*. 2006 Oct 9;10(4):722-32.
- [11] Kumar B, Singh HV, Singh SP, Mohan A. Secure spread-spectrum watermarking for telemedicine applications. *Journal of Information Security*. 2011 Apr 8;2(02):91.
- [12] Mohanty SP, Sengupta A, Guturu P, Kougiianos E. Everything You Want to Know About Watermarking: From Paper Marks to Hardware Protection: From paper marks to hardware protection. *IEEE Consumer Electronics Magazine*. 2017 Jun 15;6(3):83-91.
- [13] Amirtharajan R, Qin J, Rayappan JB. Random image steganography and steganalysis: Present status and future directions. *Inform. Technol. J*. 2012 May 1;11:566-76.
- [14] Singh AK, Kumar B, Dave M, Ghrera SP, Mohan A. Digital image watermarking: techniques and emerging applications. In *Handbook of research on modern cryptographic solutions for computer and cyber security 2016* (pp. 246-272). IGI Global.

- [15] Irany BM. *A High Capacity Reversible Multiple Watermarking Scheme-Applications to Images, Medical Data, and Biometrics* (Doctoral dissertation).
- [16] Huang HC, Fang WC. Techniques and applications of intelligent multimedia data hiding. *Telecommunication Systems*. 2010 Aug 1;44(3-4):241-51.
- [17] Mohanty SP. Digital watermarking: A tutorial review. URL: <http://www.csee.usf.edu/~smohanty/research/Reports/WMSurvey1999Mohanty.pdf>. 1999.
- [18] Shih FY, Zhong X, Chang IC, Satoh SI. An adjustable-purpose image watermarking technique by particle swarm optimization. *Multimedia Tools and Applications*. 2018 Jan 1;77(2):1623-42.
- [19] Nayak DR, Dash R, Majhi B. Brain MR image classification using two-dimensional discrete wavelet transform and AdaBoost with random forests. *Neurocomputing*. 2016 Feb 12;177:188-97.
- [20] Katzenbeisser, F. A. P. Petitcolas(2000) "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, London, 2000.
- [21] <https://homepages.inf.ed.ac.uk/rbf/HIPR2/fourier.htm>
- [22] Gupta B, Agrawal DP, Yamaguchi S, editors. *Handbook of research on modern cryptographic solutions for computer and cyber security*. IGI global; 2016 May 16.
- [23] Wu Y, Noonan JP, Aghaian S. NPCR and UACI randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*. 2011 Apr;1(2):31-8.
- [24] Horng SJ, Rosiyadi D, Fan P, Wang X, Khan MK. An adaptive watermarking scheme for e-government document images. *Multimedia tools and applications*. 2014 Oct 1;72(3):3085-103.
- [25] Amini M, Ahmad MO, Swamy MN. Digital watermark extraction in wavelet domain using hidden Markov model. *Multimedia Tools and Applications*. 2017 Feb 1;76(3):3731-49.
- [26] Kalantari NK, Ahadi SM. A logarithmic quantization index modulation for perceptually better data hiding. *IEEE Transactions on Image Processing*. 2010 Mar 15;19(6):1504-17.
- [27] Nezhadarya E, Wang ZJ, Ward RK. Robust image watermarking based on multiscale gradient direction quantization. *IEEE Transactions on Information Forensics and Security*. 2011 Aug 4;6(4):1200-13.
- [28] Ghazvini M, Hachrood EM, Mirzadi M. An improved image watermarking method in frequency domain. *Journal of Applied Security Research*. 2017 Apr 3;12(2):260-75.
- [29] Mingzhi C, Yan L, Yajian Z, Min L. A combined dwt and dct watermarking scheme optimized using genetic algorithm. *Journal of multimedia*. 2013 Jun 1;8(3):299-305.
- [30] Wang SH, Lin YP. Wavelet tree quantization for copyright protection watermarking. *IEEE transactions on Image Processing*. 2004 Mar 30;13(2):154-65.

- [31] Yuan Y, Huang D, Liu D. An integer wavelet based multiple logo-watermarking scheme. In First International Multi-Symposiums on Computer and Computational Sciences (IMSCCS'06) 2006 Jun 20 (Vol. 2, pp. 175-179). IEEE.
- [32] Shunqing X, Weihong Z, Yong Z. A new digital watermarking algorithm based on NSCT and SVD. In Advances in Control and Communication 2012 (pp. 49-57). Springer, Berlin, Heidelberg.
- [33] Rosiyadi D, Horng SJ, Fan P, Wang X, Khan MK, Pan Y. Copyright protection for e-government document images. IEEE MultiMedia. 2011 Aug 18;19(3):62-73.
- [34] Singh S, Rathore VS, Singh R. Hybrid NSCT domain multiple watermarking for medical images. Multimedia Tools and Applications. 2017 Feb 1;76(3):3557-75.
- [35] Srivastava A, Saxena P. DWT-DCT-SVD based semiblind image watermarking using middle frequency band. IOSR J Comput Eng. 2013 Jun;12(2):63-6.
- [36] 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. 2019 Oct 15;78(19):27085-107.
- [37] Zhang L, Gao Y, Xia Y, Dai Q, Li X. A fine-grained image categorization system by cellet-encoded spatial pyramid modeling. IEEE transactions on industrial electronics. 2014 Jun 2;62(1):564-71.
- [38] Cao X, Fu Z, Sun X. A privacy-preserving outsourcing data storage scheme with fragile digital watermarking-based data auditing. Journal of Electrical and Computer Engineering. 2016;2016.
- [39] Pan-Pan N, Xiang-Yang W, Yu-Nan L, Hong-Ying Y. A robust color image watermarking using local invariant significant bitplane histogram. Multimedia Tools and Applications. 2017 Feb 1;76(3):3403-33.
- [40] Chen CH, Tang YL, Wang CP, Hsieh WS. A robust watermarking algorithm based on salient image features. Optik-International Journal for Light and Electron Optics. 2014 Feb 1;125(3):1134-40.
- [41] Deng C, Li J, Gao X. Geometric attacks resistant image watermarking in affine covariant regions. Acta Automatic Sinica. 2010;26(2):221-8.
- [42] Seo JS, Yoo CD. Image watermarking based on invariant regions of scale-space representation. IEEE Transactions on Signal Processing. 2006 Mar 20;54(4):1537-49.
- [43] Wang XY, Niu PP, Yang HY, Chen LL. Affine invariant image watermarking using intensity probability density-based Harris Laplace detector. Journal of Visual Communication and Image Representation. 2012 Aug 1;23(6):892-907.
- [44] Abbas NH, Ahmad SM, Ramli AR, Parveen S. A multi-purpose watermarking scheme based on hybrid of lifting wavelet transform and Arnold transform. In 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA) 2016 May 9 (pp. 1-6). IEEE.
- [45] Ansari IA, Pant M, Ahn CW. SVD based fragile watermarking scheme for tamper localization and self-recovery. International Journal of Machine Learning and Cybernetics. 2016 Dec 1;7(6):1225-39.
- [46] Tong X, Liu Y, Zhang M, Chen Y. A novel chaos-based fragile watermarking for image tampering detection and self-recovery. Signal Processing: Image Communication. 2013 Mar 1;28(3):301-8.
- [47] Ansari IA, Pant M. Multipurpose image watermarking in the domain of DWT based on SVD and ABC. Pattern Recognition Letters. 2017 Jul 15;94:228-36.
- [48] Liu XL, Lin CC, Yuan SM. Blind dual watermarking for color images' authentication and copyright protection. IEEE Transactions on Circuits and Systems for Video Technology. 2016 Dec 1;28(5):1047-55.

- [49] Lusson F, Bailey K, Leeney M, Curran K. A novel approach to digital watermarking, exploiting colour spaces. *Signal Processing*. 2013 May 1;93(5):1268-94.
- [50] Su Q, Niu Y, Zou H, Liu X. A blind dual color images watermarking based on singular value decomposition. *Applied Mathematics and Computation*. 2013 Apr 15;219(16):8455-66.
- [51] Sadreazami H, Ahmad MO, Swamy MN. Multiplicative watermark decoder in contourlet domain using the normal inverse Gaussian distribution. *IEEE Transactions on Multimedia*. 2015 Dec 11;18(2):196-207.
- [52] Akhaee MA, Sahraeian SM, Marvasti F. Contourlet-based image watermarking using optimum detector in a noisy environment. *IEEE Transactions on Image Processing*. 2009 Dec 18;19(4):967-80.
- [53] Akhaee MA, Sahraeian SM, Jin C. Blind image watermarking using a sample projection approach. *IEEE Transactions on Information Forensics and Security*. 2011 Apr 21;6(3):883-93.
- [54] Hamghalam M, Mirzakuchaki S, Akhaee MA. Robust image watermarking using dihedral angle based on maximum-likelihood detector. *IET Image Processing*. 2013 Jul 1;7(5):451-63.
- [55] Jamal SS, Khan MU, Shah T. A watermarking technique with chaotic fractional S-box transformation. *Wireless Personal Communications*. 2016 Oct 1;90(4):2033-49.
- [56] Ali M, Ahn CW, Pant M. An efficient lossless robust watermarking scheme by integrating redistributed invariant wavelet and fractional Fourier transforms. *Multimedia Tools and Applications*. 2018 May 1;77(10):11751-73.
- [57] Rawat S, Raman B. A blind watermarking algorithm based on fractional Fourier transform and visual cryptography. *Signal Processing*. 2012 Jun 1;92(6):1480-91.
- [58] Liao X, Li K, Yin J. Separable data hiding in encrypted image based on compressive sensing and discrete fourier transform. *Multimedia Tools and Applications*. 2017 Oct 1;76(20):20739-53.
- [59] Wang RZ, Lin CF, Lin JC. Image hiding by optimal LSB substitution and genetic algorithm. *Pattern recognition*. 2001 Mar 1;34(3):671-83.
- [60] Singh AK, Dave M, Mohan A. Robust and secure multiple watermarking in wavelet domain. *Journal of medical imaging and health informatics*. 2015 Apr 1;5(2):406-14.
- [61] Maheswari S, Rameshwaran K, Malarselvi KM. DCT-PCA based watermarking on E-governance documents. *Research Journal of Applied Sciences, Engineering and Technology*. 2015 Mar 5;9(7):507-11.
- [62] Wang J, Lian S, Shi YQ. Hybrid multiplicative multi-watermarking in DWT domain. *Multidimensional Systems and Signal Processing*. 2017 Apr 1;28(2):617-36.
- [63] Liu N, Li H, Dai H, Guo D, Chen D. Robust blind image watermarking based on chaotic mixtures. *Nonlinear Dynamics*. 2015 May 1;80(3):1329-55.
- [64] Guo Y, Li BZ, Goel N. Optimised blind image watermarking method based on firefly algorithm in DWT-QR transform domain. *IET Image processing*. 2017 Mar 3;11(6):406-15.
- [65] Ghebleh M, Kanso A, Own HS. A blind chaos-based watermarking technique. *Security and Communication Networks*. 2014 Apr;7(4):800-11.
- [66] Su Q, Niu Y, Wang Q, Sheng G. A blind color image watermarking based on DC component in the spatial domain. *Optik*. 2013 Dec 1;124(23):6255-60.
- [67] Xiao D, Deng M, Zhu X. A reversible image authentication scheme based on compressive sensing. *Multimedia Tools and Applications*. 2015 Sep 1;74(18):7729-52.

- [68] Sari CA, Rachmawanto EH. Robust and imperceptible image watermarking by DC coefficients using singular value decomposition. In 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) 2017 Sep 19 (pp. 1-5). IEEE.
- [69] Gunjal BL, Mali SN. MEO based secured, robust, high capacity and perceptual quality image watermarking in DWT-SVD domain. SpringerPlus. 2015 Dec;4(1):126.
- [70] Naheed T, Usman I, Khan TM, Dar AH, Shafique MF. Intelligent reversible watermarking technique in medical images using GA and PSO. Optik-International Journal for Light and Electron Optics. 2014 Jun 1;125(11):2515-25.
- [71] Luo L, Chen Z, Chen M, Zeng X, Xiong Z. Reversible image watermarking using interpolation technique. IEEE Transactions on information forensics and security. 2009 Nov 6;5(1):187-93.
- [72] Yin Z, Luo B, Hong W. Separable and error-free reversible data hiding in encrypted image with high payload. The scientific world journal. 2014;2014..
- [73] Zhang X. Separable reversible data hiding in encrypted image. IEEE transactions on information forensics and security. 2011 Nov 15;7(2):826-32.
- [74] Wang S, Zheng D, Zhao J, Tam WJ, Speranza F. Adaptive watermarking and tree structure based image quality estimation. IEEE Transactions on Multimedia. 2013 Nov 20;16(2):311-25.
- [75] Singh AK, Kumar B, Dave M, Mohan A. Robust and imperceptible dual watermarking for telemedicine applications. Wireless Personal Communications. 2015 Feb 1;80(4):1415-33.
- [76] Bhatnagar G, Wu QM, Atreya PK. Secure randomized image watermarking based on singular value decomposition. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM). 2013 Dec 1;10(1):4.
- [77] Ji F, Deng C, An L, Huang D. Desynchronization attacks resilient image watermarking scheme based on global restoration and local embedding. Neurocomputing. 2013 Apr 15;106:42-50.
- [78] Deng C, Gao X, Li X, Tao D. A local Tchebichef moments-based robust image watermarking. Signal Processing. 2009 Aug 1;89(8):1531-9.
- [79] Seo JS, Yoo CD. Localized image watermarking based on feature points of scale-space representation. Pattern Recognition. 2004 Jul 1;37(7):1365-75.
- [80] Run RS, Horng SJ, Lai JL, Kao TW, Chen RJ. An improved SVD-based watermarking technique for copyright protection. Expert Systems with applications. 2012 Jan 1;39(1):673-89.
- [81] Zhang X. Reversible data hiding in encrypted image. IEEE signal processing letters. 2011 Feb 14;18(4):255-8.
- [82] Bas P, Chassery JM, Macq B. Geometrically invariant watermarking using feature points. IEEE transactions on image Processing. 2002 Nov 7;11(9):1014-28.
- [83] Tang CW, Hang HM. A feature-based robust digital image watermarking scheme. IEEE transactions on signal processing. 2003 Mar 26;51(4):950-9.

- [84] Lai CC, Tsai CC. Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Transactions on instrumentation and measurement*. 2010 Sep 2;59(11):3060-3.
- [85] Thakkar FN, Srivastava VK. A fast watermarking algorithm with enhanced security using compressive sensing and principle components and its performance analysis against a set of standard attacks. *Multimedia Tools and Applications*. 2017 Jul 1;76(14):15191-219.
- [86] Nazari M, Sharif A, Mollaeefar M. An improved method for digital image fragile watermarking based on chaotic maps. *Multimedia Tools and Applications*. 2017 Aug 1;76(15):16107-23.
- [87] Chen F, He H, Tai HM, Wang H. Chaos-based self-embedding fragile watermarking with flexible watermark payload. *Multimedia tools and applications*. 2014 Sep 1;72(1):41-56.
- [88] Huo Y, He H, Chen F. Alterable-capacity fragile watermarking scheme with restoration capability. *Optics communications*. 2012 Apr 1;285(7):1759-66.
- [89] Zhang X, Wang S, Qian Z, Feng G. Reference sharing mechanism for watermark self-embedding. *IEEE Transactions on Image Processing*. 2010 Aug 16;20(2):485-95.
- [90] Cai-Yin W, Xiang-Wei K, Chao L. Process color watermarking: the use of visual masking and dot gain correction. *Multimedia Tools and Applications*. 2017 Aug 1;76(15):16291-314.
- [91] Sayahi I, Elkefi A, Amar CB. Blind watermarking algorithm based on spiral scanning method and error-correcting codes. *Multimedia Tools and Applications*. 2017 Aug 1;76(15):16439-62.
- [92] Badshah G, Liew SC, Zain JM, Ali M. Watermark compression in medical image watermarking using Lempel-Ziv-Welch (LZW) lossless compression technique. *Journal of digital imaging*. 2016 Apr 1;29(2):216-25.
- [93] Yang H, Yin J. A secure removable visible watermarking for BTC compressed images. *Multimedia Tools and Applications*. 2015 Mar 1;74(6):1725-39.
- [94] Hu Y, Kwong S, Huang J. An algorithm for removable visible watermarking. *IEEE Transactions on Circuits and Systems for Video Technology*. 2005 Dec 27;16(1):129-33.
- [95] Yang Y, Sun X, Yang H, Li CT. Removable visible image watermarking algorithm in the discrete cosine transform domain. *Journal of Electronic Imaging*. 2008 Jul;17(3):033008.
- [96] Shieh JM, Lou DC, Chang MC. A semi-blind digital watermarking scheme based on singular value decomposition. *Computer Standards & Interfaces*. 2006 Apr 1;28(4):428-40.

- [97] Hsia SC, Jou IC, Hwang SM. A gray level watermarking algorithm using double layer hidden approach. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*. 2002 Feb 1;85(2):463-71.
- [98] Lee WB, Chen TH. A public verifiable copy protection technique for still images. *Journal of Systems and Software*. 2002 Jun 15;62(3):195-204.
- [99] Lu CS, Huang SK, Sze CJ, Liao HY. A new watermarking technique for multimedia protection. *Multimedia image and video processing*. 2001:507-30.
- [100] Niu XM, Lu ZM, Sun SH. Digital watermarking of still images with gray-level digital watermarks. *IEEE Transactions on Consumer Electronics*. 2000 Feb;46(1):137-45.
- [101] Chang CS, Shen JJ. Features classification forest: a novel development that is adaptable to robust blind watermarking techniques. *IEEE Transactions on Image Processing*. 2017 May 19;26(8):3921-35.
- [102] Horng SJ, Rosiyadi D, Li T, Takao T, Guo M, Khan MK. A blind image copyright protection scheme for e-government. *Journal of Visual Communication and Image Representation*. 2013 Oct 1;24(7):1099-105.
- [103] Patra JC, Phua JE, Bornand C. A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression. *Digital Signal Processing*. 2010 Dec 1;20(6):1597-611.
- [104] Su Q, Niu Y, Wang G, Jia S, Yue J. Color image blind watermarking scheme based on QR decomposition. *Signal Processing*. 2014 Jan 1;94:219-35.
- [105] Zhu X, Ding J, Dong H, Hu K, Zhang X. Normalized correlation-based quantization modulation for robust watermarking. *IEEE Transactions on Multimedia*. 2014 Jul 18;16(7):1888-904.
- [106] Singh HV, Rai S, Mohan A, Singh SP. Robust copyright marking using weibull distribution. *Computers & Electrical Engineering*. 2011 Sep 1;37(5):714-28.
- [107] Singh HV, Singh AK, Yadav S, Mohan A. DCT based secure data hiding for intellectual property right protection. *CSI transactions on ICT*. 2014 Nov 1;2(3):163-8.
- [108] Kumar B, Singh HV, Singh SP, Mohan A. Novel efficient and secure medical data transmission on WIMAX. *Telemedicine and e-Health*. 2008 Dec 1;14(10):1063-9.
- [109] Singh AK, Dave M, Mohan A. Hybrid technique for robust and imperceptible image watermarking in DWT–DCT–SVD domain. *National Academy Science Letters*. 2014 Aug 1;37(4):351-8.

- [110] Khan MI, Rahman M, Sarker M, Hasan I. Digital Watermarking for Image AuthenticationBased on Combined DCT, DWT and SVD Transformation. arXiv preprint arXiv:1307.6328. 2013 Jul 24.
- [111] Harish NJ, Kumar BB, Kusagur A. Hybrid robust watermarking techniques based on DWT, DCT, and SVD. *International Journal of Advanced Electrical and Electronics Engineering*. 2013;2(5):137-43.
- [112] Singh AK. Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. *Multimedia Tools and Applications*. 2017 Mar 1;76(6):8881-900.
- [113] Wang MS, Chen WC. A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography. *Computer Standards & Interfaces*. 2009 Jun 1;31(4):757-62.
- [114] Wu X, Sun W. Robust copyright protection scheme for digital images using overlapping DCT and SVD. *Applied Soft Computing*. 2013 Feb 1;13(2):1170-82.
- [115] Ganic E, Eskicioglu AM. Robust DWT-SVD domain image watermarking: embedding data in all frequencies. In *Proceedings of the 2004 Workshop on Multimedia and Security 2004 Sep 20* (pp. 166-174). ACM.
- [116] Azizi S, Mohrekes M, Samavi S. Hybrid image watermarking using local complexity variations. In *2013 21st Iranian Conference on Electrical Engineering (ICEE) 2013 May 14* (pp. 1-6). IEEE.
- [117] Ramanjaneyulu K, Rajarajeswari K. Wavelet-based oblivious image watermarking scheme using genetic algorithm. *IET image processing*. 2012 Jun 1;6(4):364-73.
- [118] Shivani J, Senapati R. Robust image embedded watermarking using DCT and listless SPIHT. *Future Internet*. 2017 Sep;9(3):33.
- [119] Said A, Pearlman WA. A new, fast, and efficient image codec based on set partitioning in hierarchical trees. *IEEE Transactions on circuits and systems for video technology*. 1996 Jun 3;6(3):243-50.
- [120] Senapati RK, Pati UC, Mahapatra KK. Reduced memory, low complexity embedded image compression algorithm using hierarchical listless discrete Tchebichef transform. *IET Image Processing*. 2014 Feb 13;8(4):213-38.
- [121] Singh S, Singh R, Singh AK, Siddiqui TJ. SVD-DCT based medical image watermarking in NSCT domain. In *Quantum Computing: An Environment for Intelligent Large Scale Real Application 2018* (pp. 467-488). Springer, Cham.

- [122] Narasimhulu CV, Prasad KS. A novel robust watermarking technique based on Nonsampled contourlet Transform and SVD. *The International Journal of Multimedia & its applications*. 2011 Feb;3(1).
- [123] Hua KL, Dai BR, Srinivasan K, Hsu YH, Sharma V. A hybrid NSCT domain image watermarking scheme. *EURASIP Journal on Image and Video Processing*. 2017 Dec;2017(1):10.
- [124] Meenpal T. DWT-based blind and robust watermarking using SPIHT algorithm with applications in tele-medicine. *Sādhanā*. 2018 Jan 1;43(1):4.
- [125] Shahid AR. An image watermarking approach based on Set Partitioning in Hierarchical Trees (SPIHT) algorithm. In *2012 International Conference on Informatics, Electronics & Vision (ICIEV) 2012 May 18* (pp. 487-492). IEEE.
- [126] Singh S, Singh R, Siddiqui TJ. MSVD based image watermarking in NSCT domain. In *2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC) 2016 Dec 22* (pp. 685-688). IEEE.
- [127] Sharma A, Singh AK, Ghrera SP. Robust and secure multiple watermarking for medical images. *Wireless Personal Communications*. 2017 Feb 1;92(4):1611-24.
- [128] Chemak C, Bouhlef MS, Lapayre JC. A new scheme of robust image watermarking: the double watermarking algorithm. In *Proceedings of the 2007 summer computer simulation conference 2007 Jul 16* (pp. 1201-1208). Society for Computer Simulation International.
- [129] Shi H, Li MC, Guo C, Tan R. A region-adaptive semi-fragile dual watermarking scheme. *Multimedia Tools and Applications*. 2016 Jan 1;75(1):465-95.
- [130] Shen H, Chen B. From single watermark to dual watermark: a new approach for image watermarking. *Computers & Electrical Engineering*. 2012 Sep 1;38(5):1310-24.
- [131] Xie G, Shen H. Toward improved wavelet-based watermarking using the pixel-wise masking model. In *IEEE International Conference on Image Processing 2005 2005 Sep 14* (Vol. 1, pp. I-689). IEEE.
- [132] First E, Qi X. A composite approach for blind grayscale logo watermarking. In *2007 IEEE International Conference on Image Processing 2007 Sep* (Vol. 3, pp. III-265). IEEE.
- [133] Sharma A, Singh AK, Kumar P. Combining haar wavelet and Karhunen-Loeve transform for robust and imperceptible data hiding using digital images. *Journal of Intelligent Systems*. 2018 Jan 26;27(1):91-103.

- [134] Joshi AM, Gupta S, Girdhar M, Agarwal P, Sarker R. Combined DWT–DCT-based video watermarking algorithm using Arnold transform technique. In Proceedings of the international conference on data engineering and communication technology 2017 (pp. 455-463). Springer, Singapore.
- [135] Nisha and Sunil Kumar “Image Quality Assessment Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 7, pp 636-640.
- [136] Cheddad A, Condell J, Curran K, Mc Kevitt P. Digital image steganography: Survey and analysis of current methods. Signal processing. 2010 Mar 1;90(3):727-52.
- [137] Potdar VM, Han S, Chang E. A survey of digital image watermarking techniques. In INDIN'05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005. 2005 Aug 10 (pp. 709-716). IEEE.
- [138] Podilchuk CI, Delp EJ. Digital watermarking: algorithms and applications. IEEE signal processing Magazine. 2001 Jul;18(4):33-46.
- [139] Celik MU, Sharma G, Saber E, Tekalp AM. Hierarchical watermarking for secure image authentication with localization. IEEE Transactions on Image Processing. 2002 Aug 7;11(6):585-95.
- [140] Bhatnagar G, Raman B. A new robust reference watermarking scheme based on DWT-SVD. Computer Standards & Interfaces. 2009 Sep 1;31(5):1002-13.
- [141] Singh S, Rathore VS, Singh R, Singh MK. Hybrid semi-blind image watermarking in redundant wavelet domain. Multimedia Tools and Applications. 2017 Sep 1;76(18):19113-37.
- [142] Singh AK, Kumar B, Dave M, Mohan A. Multiple watermarking on medical images using selective discrete wavelet transform coefficients. Journal of Medical Imaging and Health Informatics. 2015 Jun 1;5(3):607-14.
- [143] Singh AK, Kumar B, Singh G, Mohan A, editors. Medical image watermarking: techniques and applications. Springer; 2017 Aug 11.
- [144] Ernawan F, Kabir MN. A block-based RDWT-SVD image watermarking method using human visual system characteristics. The Visual Computer. 2018:1-9.
- [145] Khare P, Srivastava VK. Robust Digital Image Watermarking Scheme Based on RDWT-DCT-SVD. In 2018 5th International Conference on Signal Processing and Integrated Networks (SPIN) 2018 Feb 22 (pp. 88-93). IEEE.

- [146] Gaur S, Srivastava VK. A RDWT and Block-SVD based Dual Watermarking Scheme for Digital Images. *International Journal of Advanced Computer Science and Applications*. 2017 Apr 1;8(4):211-9.
- [147] Mishra S, Dastidar A. Hybrid Image Encryption and Decryption using Cryptography and Watermarking Technique for High Security Applications. In 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT) 2018 Mar 1 (pp. 1-5). IEEE.
- [148] Singh RK, Shaw DK. A Hybrid Concept of Cryptography and Dual Watermarking (LSB_DCT) for Data Security. *International Journal of Information Security and Privacy (IJISP)*. 2018 Jan 1;12(1):1-2.
- [149] Kaur KN, Gupta I, Singh AK. Digital Image Watermarking Using (2, 2) Visual Cryptography with DWT-SVD Based Watermarking. In *Computational Intelligence in Data Mining 2019* (pp. 77-86). Springer, Singapore.

LIST OF PUBLICATIONS

Journal(s)

- [1] Kumar C, Singh AK, Kumar P. A recent survey on image watermarking techniques and its application in e-governance. *Multimedia Tools and Applications*. 2018 Feb 1;77(3):3597-622.
- [2] Kumar C, Singh AK, Kumar P. Improved wavelet-based image watermarking through SPIHT. *Multimedia Tools and Applications*. 2018 Jun 1:1-4.
- [3] Kumar C, Singh AK, Kumar P, Singh R, Singh S. SPIHT-based multiple image watermarking in NSCT domain. *Concurrency and Computation: Practice and Experience*. 2018:e4912.
- [4] Kumar C, Singh AK, Kumar P. Dual watermarking: An approach for securing digital documents. *Multimedia Tools and Applications*. 2019 Dec 23:1-6.

Conference(s)

- [1] Kumar C, Singh AK, Kumar P, Singh R. A low complexity secure force encryption based multiple image watermarking in NSCT domain. In 2018 Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T) 2018 Sep 21 (pp. 92-96). IEEE.
- [2] Kumar C, Singh AK, Kumar P. SPIHT based dual watermarking technique in NSCT domain. In 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC) 2018 Dec 20 (pp. 111-114). IEEE.