SECURITY OF DIGITAL DOCUMENTS FOR REMOTE MEDICAL CONSULTANCY

Thesis submitted in fulfilment for the requirement of the Degree of

Doctor of Philosophy

By

SRITI THAKUR

Department of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology

Waknaghat, Solan-173234, Himachal Pradesh, INDIA

December 2019

TABLE OF CONTENTS

ACKNOWLEDGEMENT

I would like to convey my utmost reverence and gratefulness to my supervisors, **Prof. (Dr.) Satya Prakash Ghrera and Dr. Amit Kumar Singh** for their unconditional support supervision, and providing their guiding light at every phase of the proposed study. I will always stay indebted to them for bearing my shortcomings with their immense sense of awareness, compassion, maturity, thorough knowledge of the specific field and consistency. I would also like to pay my gratitude to the DPMC members **Dr. Pradeep Kumar Gupta, Dr. Suman Saha and Dr. Rajiv Kumar** for their thought provoking interactive assessments, queries and opinions. I would also be thankful to all the faculty members and staff of Department of Computer Science and Engineering, JUIT, Waknaghat- Solan for their scholarly support and guidance. My aim of accomplishing merit in higher education at JUIT Waknaghat, Solan would not have completed without the unflinching support of my family, near and dear ones.

This milestone in the journey of my life would have not been completed without the unwavering love, constant guidance and support of my parents. Last but not the least; I would like to thank the almighty for providing me constant strength and will power to complete my work successfully.

Sriti Thakur

Date: 20 Dec, 2019 (Sriti Thakur)

DECLARATION BY THE SCHOLAR

I hereby declare that the work presented in this thesis titled **"Security of Digital Documents for Remote Medical Consultancy"** in fulfilment of the requirement for the award of the degree of Doctor of Philosophy in Computer Science Engineering, submitted in the **Department of Computer Science and Engineering & IT, Jaypee University of Information Technology (JUIT),Waknaghat, Solan, Himachal Pradesh** India is a genuine documentation of my research work under the guidance of **Prof. Dr. Satya Prakash Ghrera and Dr. Amit Kumar Singh.** The content presented in the thesis has not been produced by me for the award of any other degree in this institute or other institute. I am fully responsible for the contents of my PhD thesis.

Sriti Thakur

(Signature of the Scholar)

Sriti Thakur

Department of computer science and engineering & IT Jaypee University of Information Technology (JUIT), Waknaghat, Solan, Himachal Pradesh India

Date: **Dec 20, 2019**

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY

(Established by H.P. State Legislature vide Act No. 14 of 2002)
P.O. Waknaghat, 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 **"Security of Digital Documents for Remote Medical Consultancy"**, submitted by **Sriti Thakur** at **Jaypee University of Information Technology, Waknaghat, Solan, India,** is a bonafide record of his / her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree or diploma.

(Signature of Supervisor-1)
Dr. Satya Prakash Ghrera
Professor
Deptt. of CSE & IT
JUIT, Waknaghat, Solan, India

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

Date: **Dec 20, 2019**

PREFACE

Widespread utilization of e- health services across the globe has been made possible due to efficient use of modern communication and information systems. This has resulted in smooth dissemination of tele-medical services to the far flung areas. Earlier when there stood no means for patients in inaccessible locations to access medical services, the notion of telemedicine seemed impossible. However, in the present setting it has proved to be a successful cure to provide diagnostic aid via networked devices. Although it has yielded in efficient exchange of information with high speeds yet it carries a potent security threat with it. Privacy, reliability, integrity and secrecy are some of the risks that automatically arise within such recurrent transmission of information. Further, the nature of data exchanged also need close attention since it involves highly confidential diagnostic data whose leakage cannot be afforded. Diagnostic data can comprise of EPR, patient's disease history/ analysis, medical record, patient identification code, medical images etc. Therefore digital watermarking proves to be one of the effective options to secure and safeguard the authenticity of such vital information. The data which requires secrecy is represented in the form of watermark which is inserted within some cover object and transmitted covertly.

Taking the above discussion into consideration, the analysis presented in this research work directs towards medical image watermarking techniques which ensure validity of the exchanged data with the right amount of fidelity. The key target behind medical image watermarking is to provide adequate level of payload capacity, robustness and imperceptibility without compromising with the security, processing /transmission and bandwidth requirements.

Initially, starting with the scrutiny of current watermarking techniques, the thesis introduces few enhanced techniques for medical images that result in better security, robustness and imperceptibility.

The thesis is segregated into six chapters. Chapter 1 presents the fundamental theory behind digital watermarking, categorization of watermarks, significant qualities, performance metrics, key attacks and current applications. Moreover, literature survey of related medical image watermarking techniques is presented including its open issues and probable solutions.

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

PSNR- peak signal to noise ratio

MSE- mean square error

NC- normalized correlation

SSIM-structural similarity index

BER- bit error rate

WPSNR-weighted peak signal to noise ratio

EPR-electronic patient record

ROI- region of interest

RONI- region of non-interest

NROI- non –region of interest

Bpp-bits per pixel

MDE-modified difference expansion

LSB-least significant bit

GA- genetic algorithm

PSO-particle swarm optimization

DWT-discrete wavelet transforms

SVD-singular value decomposition

ECC-error correcting code

DCT-discrete cosine transforms

LWT-lifting wavelet transformation

FAR-false acceptance rate

FRR- false rejection rate

SHA-secure hash algorithm

QIM-quantization index modulation

ABC-artificial bee colony

JND-just noticeable distortion

AES-advanced encryption standard

IWT-integer wavelet transforms

CDCS- class dependent coding scheme

TPE- total perceptual error

TPR- true positive rate

NSCT-non subsampled contourlet transform

RDWT-redundant discrete wavelet transforms

CHAPTER 1

INTRODUCTION AND REVIEW OF LITERATURE

In recent time, implementing e-healthcare paradigm has become a popular trend between various research communities at universal level [1].The e-healthcare solution transmits the useful patients' information to remote healthcare centre and appropriate medical experts via modern information and communication technologies. However, the transmission and access technologies of sensitive information over the unsecured channel are risky and raise critical security issues [2]. According to standard agencies, it is essential to protect patient medical information security from unauthorized access/users [3]. In addition to this, research established that medical related identity theft is a rising and dangerous offense [4]. There are three different ways to protect medical information viz. cryptography, steganography and watermarking. Out of these approaches, watermarking is the most popular and having great potential [5]. The key differences between related concepts are shown in Table 1.1. The major advantages of watermarking in the field of medical are (i) saves bandwidth and storage space (ii) maintains confidentiality of the secret medical information (iii) defence against tampering and (iv) provides efficient archiving and fast medical information retrieval via hidden watermark (s).It is established that confidentiality, reliability and availability are the mandatory security requirements of medical data, as shown in Fig. 1.1.

1.1. Important characteristics of watermark

Fig. 1.2 shows the key characteristics of digital watermarking. These characteristics introduced below [1, 6, 8-9].

- **Imperceptibility** – It computes the level of image quality as perceivable to the human eyes. This measures the similarity scale among the cover and marked image.
- **Embedding capacity**– This is the maximum amount of watermark information which is inserted into the cover object without any distortion.
- **Robustness**– This measures the ability of the secret watermark to withstand image-processing transformations, such as legitimate or illegitimate modifications. Illegitimate attacks are intended to obliterate the watermark, while legitimate attacks do not cause any kind of modification to the watermark.
- **Fragility**- This metric ensures content authentication for specific applications which demand utmost fidelity. These are categorized as fragile and semi-fragile watermarks.

The first are intended in accomplishing absolute integrity. However, the second watermarks are utilized to detect any illegitimate alteration permitting modest image-processing conversions.

- **Tamper resistance** – It gauges the integrity and legitimacy of a digital watermarking scheme. Watermarks that are tamper resistant are sensitive to content modifications, substitution and variations thus ensuring dependability and content integrity.
- **Computational complexity** – It comprises the cost connected to embedding and extraction of digital watermarks into/from the cover object. Computational complexity differs from application to application. Some applications require fast watermark insertion while others demand prolonged time for extraction. Ideally the cost of computation should be zero [6].
- **Key restrictions**– It is established that the placement of restricted /unrestricted-key depends on the ability to gain watermark/hidden data. The choice of key length majorly depends on the applications and security.
- **Security** –The security is measured through analyzing the difficulty in eradicating /altering watermark without visually degrading the cover object.
- **False positive rate** - the possibility of recognizing un-watermark part of information as containing a watermark is defined by this metric. This error relies on applications.

Table 1.1: Key differences between related protection schemes

Digital watermarking	Steganography	Cryptography
It protects the ownership information of digital information instead of protecting the data itself.	It hides the modified message so that only the corresponding parties identify the secret message.	It deals with protection of transmitted data over an unprotected path.
The sole idea behind it is to hide a ciphered message into a digital signal without bringing about noticeable distortion.	The objective behind steganography is to hide a message intended for point to point communication.	It transforms the data in a way that it becomes unintelligible for unauthorized recipients.
The method of watermark insertion requires good skill and should be done in a manner which is not noticeable to human eyes.	The bandwidth of secret message is a primary issue with it.	Sender validation is a major concern in this case.

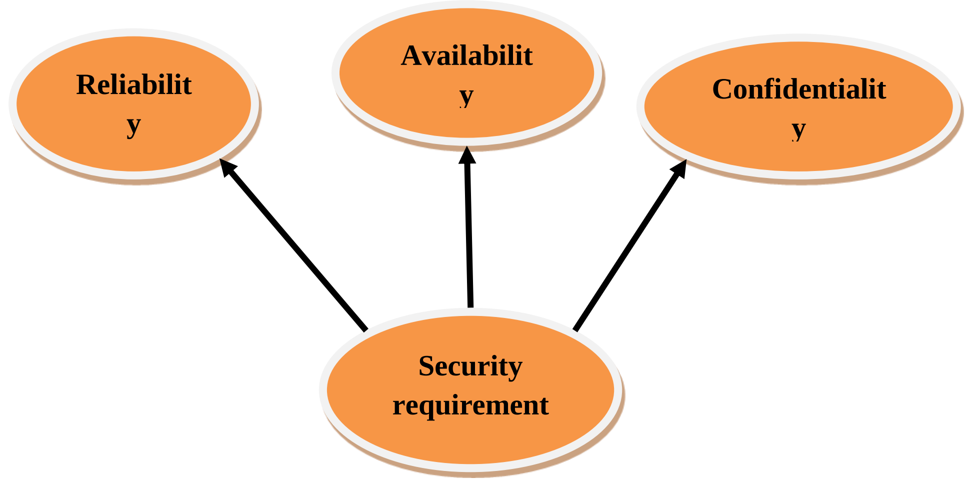


Figure 1.1: key security requirements [6]

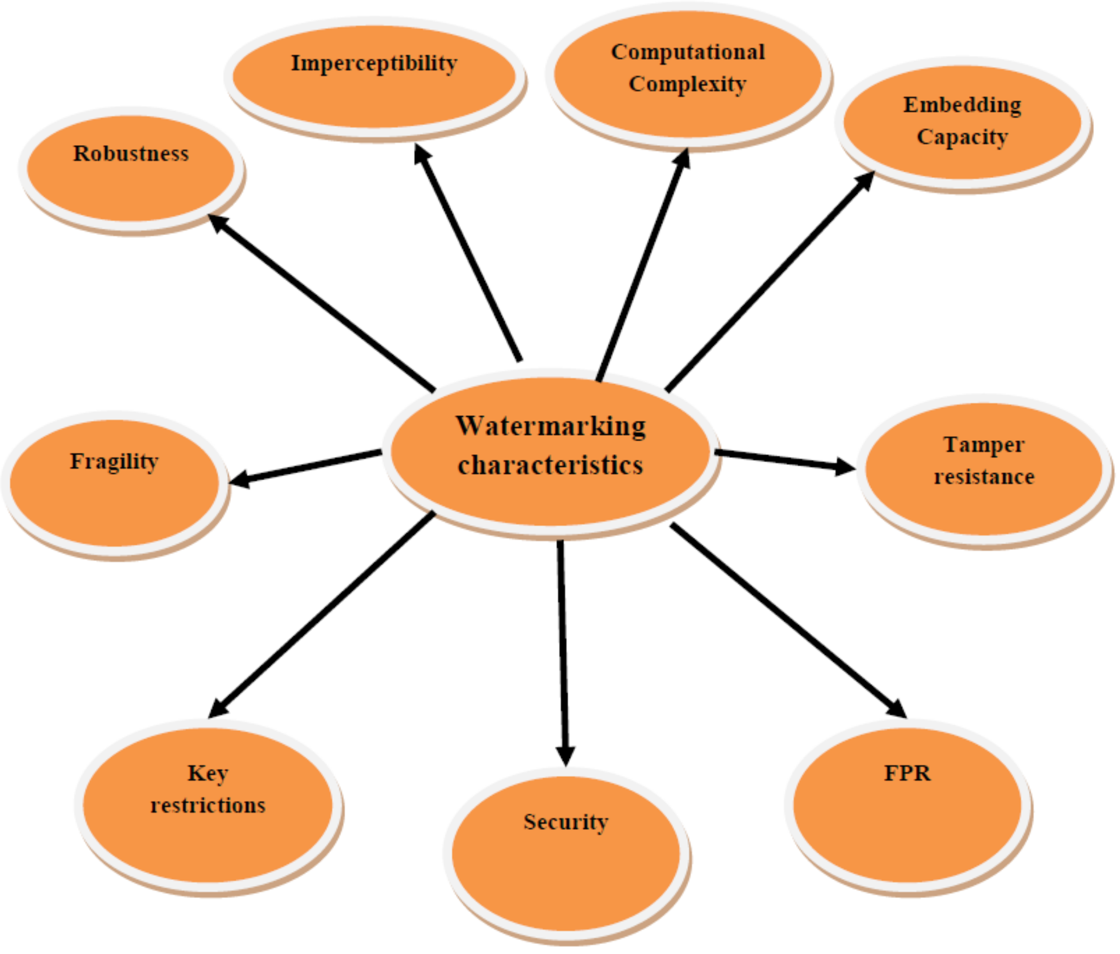


Figure: 1.2 major characteristics of digital watermark (s)

1.2. Potential applications of digital watermarking

Currently, digital watermarking is being utilized in telemedicine, e-governance, chip and hardware protection, military, digital cinema, copyright protection and content authentication. [1, 6, 8-9]. Fig. 1.3 shows the key applications of digital watermarking.

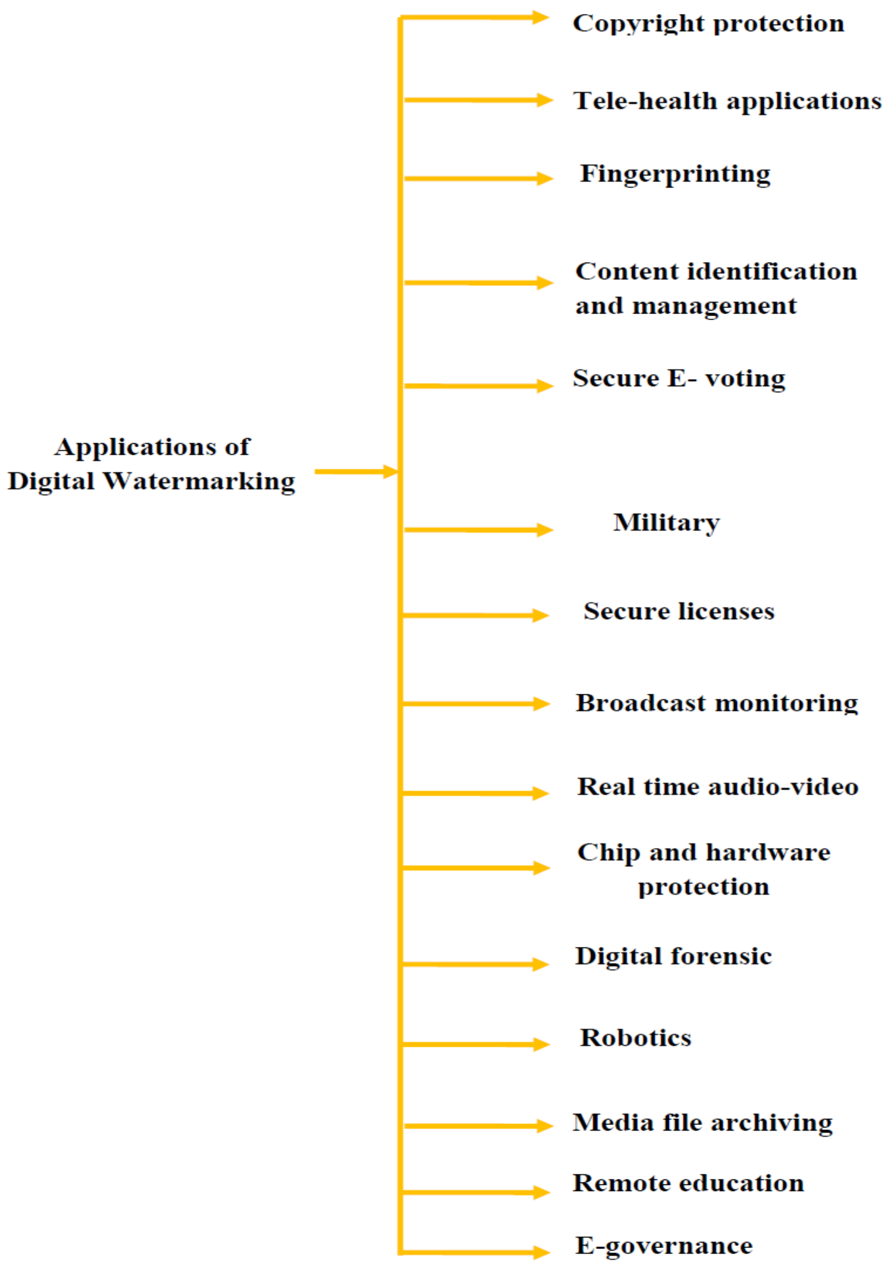


Figure: 1.3: key applications of digital watermarking

1.3. Standard framework of watermark embedding and extraction procedure

The fundamentals behind a watermarking system are introduced in detail in [6] [10]. Fig. 1.4 depicts the insertion and recovery scheme. The encoder takes two inputs such as - an input image (I_m) and a watermark (WT_{mk}). The output is obtained in the form of an image containing the watermark (W_{mkd}). The watermarked image (W_{mkd}) is the product of the function $E(I_m, WT_{mk})$

$$W_{mkd} \ = Enc(I_m, WT_{mk}) \qquad (1)$$

Likewise, the decoder takes test image (I_{tst}) and original image (I_m) as input and produces the output in the form of extracted watermark (W_{ext}). Therefore, the extracted watermark (s) is the product of the function$Dec(I_{tst}, I_m)$.

$$(W_{ext} = Dec(I_{tst}, I_m) \qquad (2)$$

At last, the original watermark (s) is equated with possibly deformed recovered watermark (s).

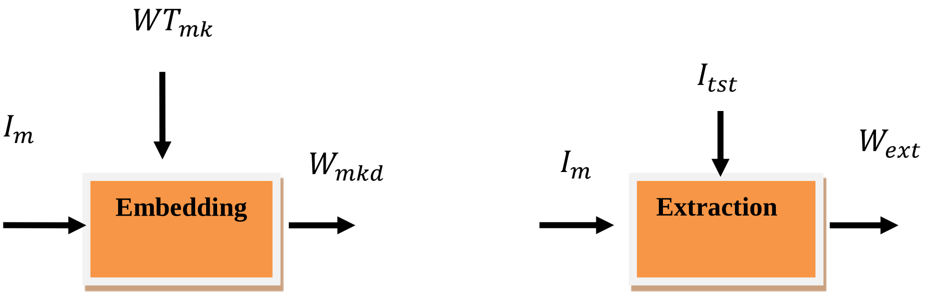
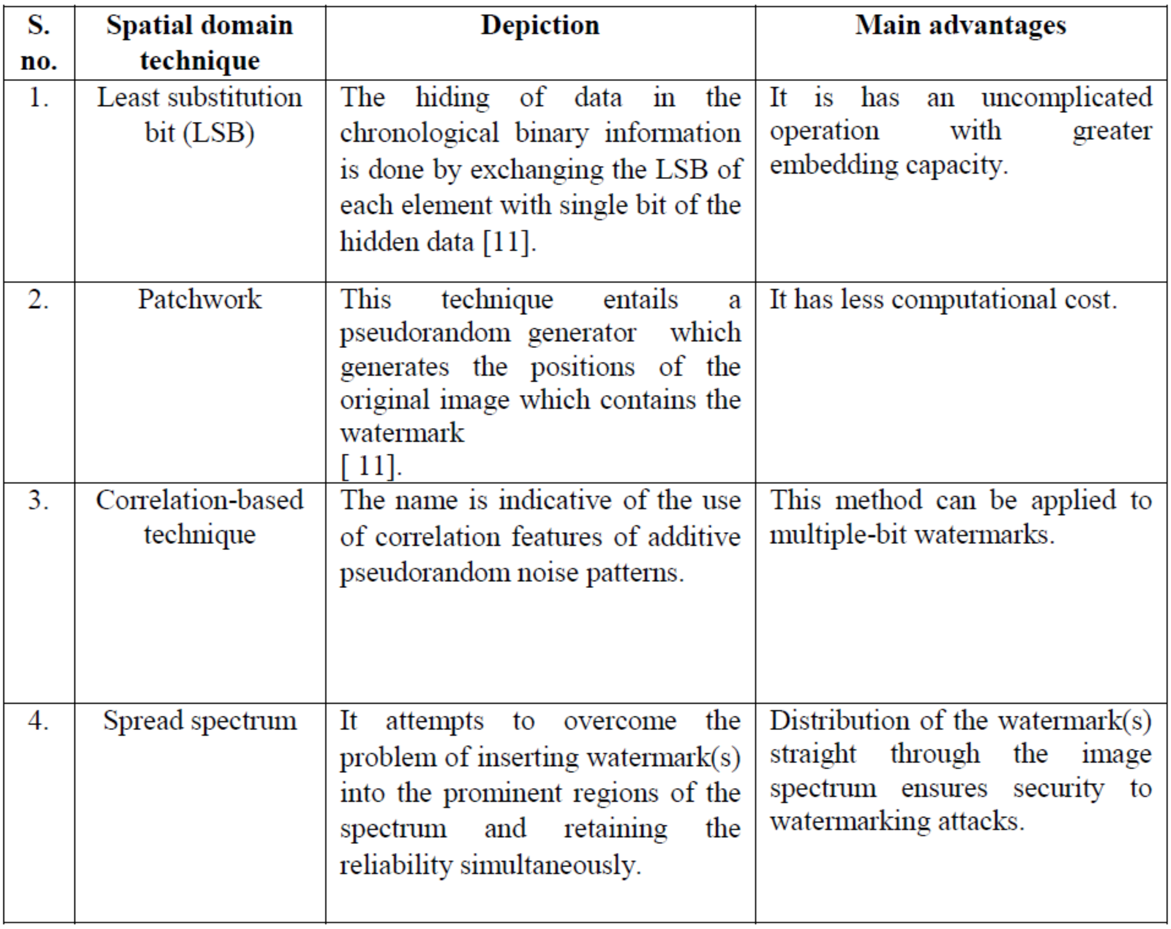


Figure: 1.4: watermark insertion and recovery scheme

1.4. Spatial and transform domain techniques

It is observed from Fig. 1.5, that spatial and transform domain are two different techniques of image watermarking [1].The spatial domain techniques are simple and have less computational cost though these are not so robust to attacks. Through research it is deduced that thetransform domain techniques gives good attack resistance to different attacks. However, these techniques bear higher computational cost. Few common techniques for the above mentioned domains are explained in table 1.2 and table 1.3, respectively.

Table 1.2: general spatial domain watermarking techniques



S. no.	Spatial domain technique	Depiction	Main advantages
1.	Least substitution bit (LSB)	The hiding of data in the chronological binary information is done by exchanging the LSB of each element with single bit of the hidden data [11].	It is has an uncomplicated operation with greater embedding capacity.
2.	Patchwork	This technique entails a pseudorandom generator which generates the positions of the original image which contains the watermark [11].	It has less computational cost.
3.	Correlation-based technique	The name is indicative of the use of correlation features of additive pseudorandom noise patterns.	This method can be applied to multiple-bit watermarks.
4.	Spread spectrum	It attempts to overcome the problem of inserting watermark(s) into the prominent regions of the spectrum and retaining the reliability simultaneously.	Distribution of the watermark(s) straight through the image spectrum ensures security to watermarking attacks.

Table 1.3: general transform domain watermarking technique

S no.	Transform domain technique	Depiction	Main advantages
1.	Discrete cosine transform (DCT)	It segregates an image into low, high and middle frequency coefficients. Additionally,the secret watermark data can be inserted into selected coefficients of the DCT applied image by potential researchers.	-DCT acquires low volume and time. -the energy compaction feature of DCT is excellent.
2.	Discrete wavelet transform (DWT)	It partitions the image and produces set of four non-converging components with different resolution.	-common method in use since it gives good space-frequency localization, offers different resolution and scale analysis etc.
3.	Singular value decomposition (SVD)	Partitions an image into two ortho-normal vectors and diagonal vector with singular values in descending order.	- It gives distinct singular values which are stable in nature and demonstrate excellent energy compaction properties.
4.	Karhunen- Loeve transform (KLT)	It is a reversible linear transform that takes the advantage of statistical properties of a vector representation and optimally de-correlates the input data.	The demand for cross channel smoothing is removed using it.
5.	Discrete Fourier transform (DFT)	It decomposes an image into a set of orthogonal functions and converts the spatial intensity of the image into its frequency domain.	-phase modulation used by it instead of magnitude components for data hiding results in improved robustness against noise attacks.

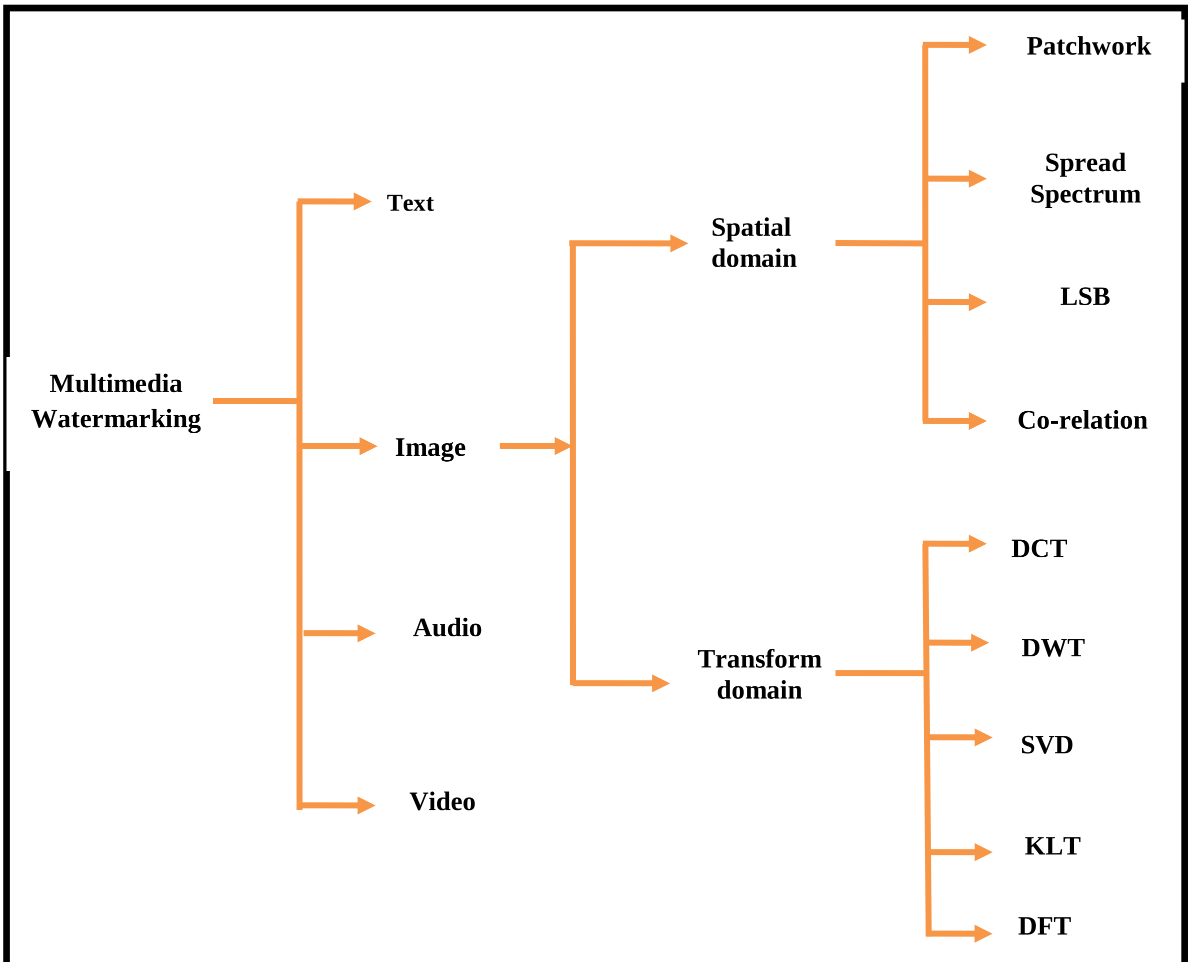


Figure 1.5: watermarking techniques in spatial and transform domain

1.5. Fundamental performance metrics in digital watermarking

There are several parameters used by researchers for assessing the outcome of watermarking algorithms/systems. Some of the significant metrics are explained as follows [1, 12]:

***(i)* Peak signal to noise ratio (PSNR)**

It gives the ratio of highest probable power of a signal to the power of degrading noise. It evaluates the perceptible quality of the watermarked images. Preferably PSNR value higher than 28 dB is regarded allowable for watermarking systems. Thus greater value of PSNR implies better imperceptibility i.e. similarity to cover image.

$$PSNR = 10log\frac{(255)^2}{MSE} \qquad (3)$$

The mean square error (MSE) is defined as

$$MSE = \frac{1}{P\times Q} = \sum_{r=1}^{s=1}\sum_{r=1}^{s=1}(S_{rs} - T_{rs})^2 \qquad (4)$$

Where $P \times Q$ = size of the cover image / watermarked image,S_{rs} = pixel of the original image and T_{rs}= pixel of the watermarked image.

(ii) Normalized correlation (NC)

The normalized correlation (NC) determines the differences and the similarities between the original and derived watermark (s) images. The value of NC ranges between 0 to 1 and preferably it should be 1. Generally NC value of 0.7 is considered to be acceptable [9]. It is defined as

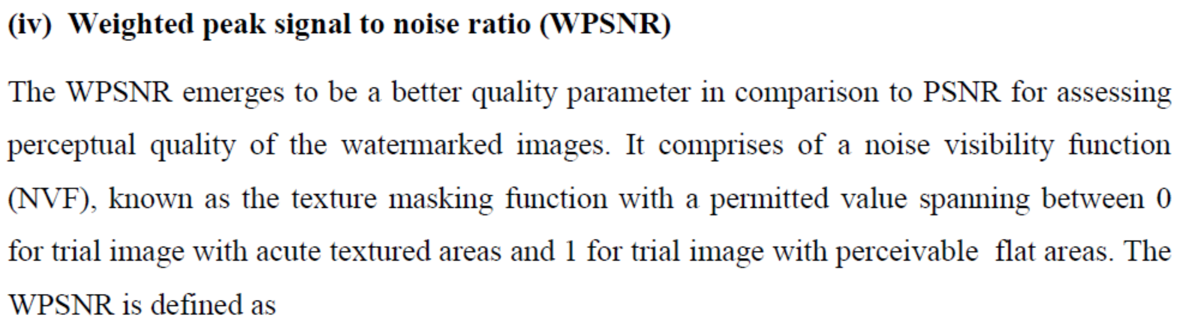
$$NC = \frac{\sum_{r=1}^{P}\sum_{s=1}^{Q}(A_{originalrs}\times A_{recoveredrs})}{\sum_{r=1}^{P}\sum_{s=1}^{Q}A_{originalrs}^2} \qquad (5)$$

Where $A_{originalrs}$= original watermark pixel, $A_{recoveredrs}$= extracted watermark pixel.

(iii) Bit error rate (BER)

It gives the ratio of wrongly decoded bits to the total number of bits [1]. The acceptable value of bit error rate is 0.

$$\text{BER} = \frac{\text{Number of wrongly deco ded bits}}{\text{Total number of bits}} \qquad (6)$$



(iv) Weighted peak signal to noise ratio (WPSNR)

The WPSNR emerges to be a better quality parameter in comparison to PSNR for assessing perceptual quality of the watermarked images. It comprises of a noise visibility function (NVF), known as the texture masking function with a permitted value spanning between 0 for trial image with acute textured areas and 1 for trial image with perceivable flat areas. The WPSNR is defined as

$$WPSNR = \frac{255^2}{NVF \times MSE} \qquad (7)$$

Where $$NVF = NORM\left\{\frac{1}{1+\delta^2_{block}}\right\}$$

NVF is a normalization function where ‘δ’ is luminance variance of the blocks used in calculations [13].

(v) Structural similarity index (SSIM)

It is one of the new performance metrics which enables evaluation of visual quality amidst marked object and original object. Permitted value of SSIM ranges between -1 and 1, where SSIM equal to 1 indicates that the watermarked image and original image are alike [1, 14].

$$\text{SSIM (h, g) =u (h, g) v (h, g) w (h, g)} \qquad (8)$$

Where

$$u(h,g) = \frac{2\mu_h\mu_g + Co_1}{\mu_h^2 + \mu_g^2 + Co_1} \qquad (9)$$

$$v(h,g) = \frac{2\sigma_h\sigma_g + Co_2}{\sigma_h^2 + \sigma_g^2 + Co_2} \qquad (\,10\,)$$

$$w(h,g) = \frac{\sigma_{hg} + Co_3}{\sigma_h\sigma_g + Co_3} \qquad (11\,)$$

The variables u (h, g), v (h, g) and w (h, g) are three functions definedas estimation functions for brightness, contrast and structure respectively. Further Co1, Co2 and Co3 are constants with chosen positive values.

1.6. Watermarking attacks

Attacks with regards to digital watermarking are explained as any ill-intentioned action carried out to perform illegitimate insertion, removal and extraction of a (legitimate/illegitimate) watermark [16].An attack is said to be successful if it distorts the watermark past tolerable limits while keeping intact the perceptible quality of the attacked data [17]. It can be primarily divided into two parts such as deliberate and unintended attacks.

In the initial category, attackers spitefully try to obstruct the operational capacity of the watermark(s) for fulfilment of his / her objectives, e.g. geometric attacks, cryptographic attacks, and protocol attacks. However, in the next category, attacker has no mean intent behind obstructing the operational power of the watermark, e.g. signal processing attacks. Further, some significant attacks are characterized and explained in table 1.4. Fig. 1.6 shows few major attacks prevalent in watermarking.

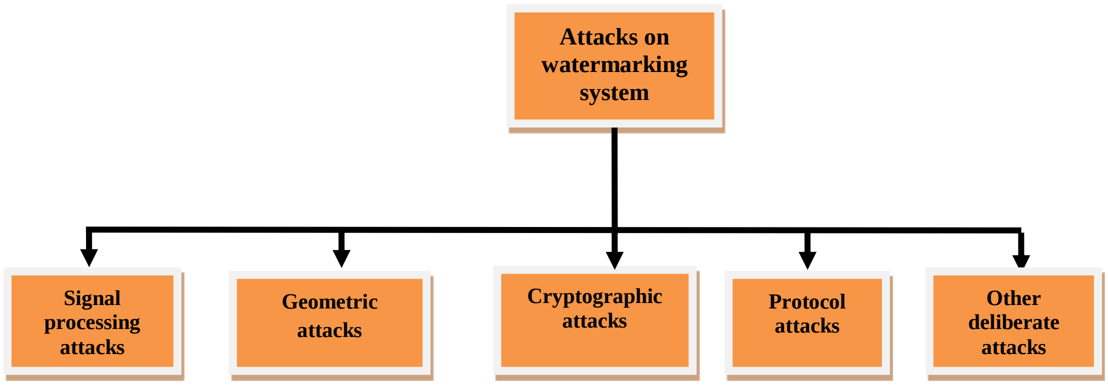


Figure 1.6: key watermark attacks [17]

Table 1.4: attacks on watermarking systems

S no.	Attack type	Explanation	Key examples
1.	**Signal-processing**	These are not intentional attacks and fall under unintended attacks.	Filtering, re-modulation, JPEG coding distortion and JPEG 2000 compression.
2.	**Geometric**	Instead of removing hidden data these attacks try to visually degrade the digital information.	Linear transformation, clipping, scaling, rotation, perspective projection, warping, bending, template and collage.
3.	**Cryptographic**	This attack prevents the protection methods from guarding the watermark. It has higher operational cost hence are used less.	Oracle attack and collusion attack.
4.	**Protocol**	The primary objective for these attacks is to get a hint of the watermark rather than changing or	Copy attack and invertible attack.

		eliminating it. As a result, it causes the attacker to claim the ownership of cover and watermarked image.	
5.	**Other deliberate attacks**	These consist of attacks which aim to harm the authenticity of ownership information.	Rescanning, printing, re-watermarking, IBM attack, forgery attack, unzign and stirmark attacks.

1.7. Some related techniques of watermarking for medical applications

Some potential approaches of watermarking for medical application is discussed below.

In [18] the authors introduced a medical image watermarking method comprising a blend of modified difference expansion and least significant bit (LSB). In the beginning, the original medical image is split into numerous sections and the marked data is inserted only into the cover object border pixels. Additionally, detection of tampered portions is done by the method meticulously which does not rely on the size of the ROI of the host image. Experimental findings established the outcome using metrics such as PSNR and (true positive rate) TPR which are found to be better than similar methods [19-24].

A blind watermarking technique is proposed in [25] for tele- health services. Dual dissimilar type of secret data is inserted to a single cover object. The security of the watermark information is strengthened through chaotic encryption.The tamper recognition and localization, resistance to attacks and imperceptibility are some of the parameters which performed good in the scenario of telemedicine services.

The authors in [26] presented a secure and attack defiant DWT watermarking process. Primarily, the cover object is partitioned into ROI and RONI. DWT transformation is applied to both the regions. The encrypted version of the secret data is placed inside the RONI section of the cover image. The performance is estimated using SSIM and PSNR.

A blind watermarking scheme is developed in [27]. This method uses particle swarm optimization (PSO) to insert the watermark into the RONI of cover object. DWT is utilized to decompose the RONI region of the cover and to the chosen DWT sub components SVD is applied to determine the singular values. Further, the singular values are processed using DCT and the central frequency sub-bands are chosen for hiding of watermark. Experimental analysis reveals the method’s good capacity and imperceptibility. Gao et al. [28] introduced a blind watermarking scheme. Firstly region based splitting of the medical image is performed. The ROI is utilized to generate the feature-bit matrix and is inserted into the least substitution bits of RONI. This helps in tamper detection at the receiver side. Experimental assessment is carried out in terms of SSIM, relative contrast error (RCE) and PSNR. The authors in [29] introduced a logistic map based fragile watermarking method. The watermark is created in terms of absolute difference (between pixel of cover and key element) and binary bits which are embedded into cover. Experimental results show better performance assessment through false detection rate, PSNR, FPR and FNR as compared to [30-31]. A pixel based medical image watermarking is presented in [32] using transform domain techniques. The ROI and RONI are determined initially, bit replacement method is utilized to embed the ROI data into the RONI region of the original image. It is seen from results that the method performs well than similar existing methods [33-36]. A watermarking procedure using region based approach is proposed by the authors in [37] which insert the ROI information to the LSB's of RONI cover medical image through JPEG compression and hashing (SHA-256). The performance is estimated using elapsed time for embedding of watermark and gives better outcomes in comparison to former technique [38].

The authors in [39] proposed a twofold data hiding scheme using IWT for content verification and safeguarding copyright information. In order to ease out the differing necessities of watermark artificial bee colony (ABC) algorithm is used for it. These differing necessities comprise of capacity, imperceptibility and robustness. The insertion of fragile and robust watermarks is done into particular sub components of the IWT decomposed original image. SVD is used to modify the low frequency IWT sub bands prior to embedding. Experimental findings show the method's resistance to variety of attacks with good robustness and imperceptibility. The technique discussed in [40] introduces watermarking technique for medical images using DCT based just noticeable distortion (JND). The low frequency sub bands of original image generated through DCT are selected for insertion of watermark data. Moreover, Chou's JND scheme [41] is utilized to improve the imperceptibility of the technique. The robustness performance indicates better NC values in comparison to similar technique [42].

A watermarking scheme using a fusion of DWT and SVD in the scenario of tele- health applications is reported in [43]. Firstly ROI region is determined for the cover to which DWT is applied followed by SVD on chosen DWT sub bands. The watermark data is inserted into chosen SVD 'U' vector of determined DWT component. In addition to it, watermark information in the form of EPR is processed using error correction code and is inserted into RONI image. Extensive evaluation of the proposed scheme is done and is found to be better than similar schemes [44-45]. Pandey et.al in [46] introduced a region based e-ophthalmology method which is robust and secure at the same time. Multiple watermark data are inserted into the RONI region of original image. The EPR data is transformed with ROI (hash value generated through SHA-512) region prior to insertion into the RONI image. Experimentally analysing the suggested scheme exhibited excellent outcomes in terms of perceptible quality, security and robustness. It also showed improved outcomes against Checkmark attacks and other common attacks. Moreover, perceptual quality and robustness values of the method proved better in comparison to existing method [45].

A blind procedure for watermarking health images is introduced in [47] which are based on genetic programming and integer wavelet transform (IWT). The theory of companding is utilized for the embedding procedure. The proposed method was tested for PSNR and SSIM and was found to show improved performance when compared to the method given in [48]. Liu et al. in [49] presented a blind medical image watermarking scheme with ROI and RONI. Initially, MD5 is used for generating a ROI hash of cover image. This value is merged with border region and RONI part of original image. The covert data (watermark) is implanted into the ROI section in the LSB part of cover. The proposed method illustrated enhanced performance in comparison to similar methods [50-53].

A secure tele-medical watermarking technique for DICOM data is presented by the authors in [54].The first step begins by calculating the hash of secret data /DICOM information and ROI section of cover object which is further scrambled using an encryption scheme. This encrypted data is inserted in to the ROI section of cover through LSB method. Moreover, the technique provided security and good perceptual quality simultaneously.

Anusudha et al. in [55] also stated a joint watermarking and cryptographic method for tele-medical services. DWT transform separates the medical image into different sub- bands and the watermark data is embedded into particular DWT sub component. The stated method is analyzed for robustness using different kinds of attacks. Moreover, concept of DNA and GA is utilized for determining an optimum solution during encryption. A watermarking method utilising two transforms i.e. DWT and SVD is reported by the authors in [56].The cover object is separated into ROI and RONI region of original image after which DWT is applied. Further, SVD is performed upon the RONI section of chosen DWT sub-components. The hidden data in the form of (EPR data, hash value, and logo image) is implanted to high frequency component of SVD vector obtained through particular DWT derivatives of cover object. Outcomes of the proposed method are calculated through perceptual quality, attack resistance and detection of tamper. Amri et.al in [57] reported a watermarking technique based on lossless compression method. Performance estimation of the proposed technique is estimated through PSNR, SSIM, compression ratio and count of bits per pixel. The authors in [58] proposed a robust watermarking scheme to counter salt and pepper attack. The proposed scheme uses LSB, noise filtering and channel coding methods for inserting EPR data using ROI pixel values into RONI pixel values of cover object. The assessment of the technique is done using SSIM, PSNR and BER. DCT based watermarking procedure is reported in [59] by the authors in which the embedding process occurs in two ways. The watermark data is implanted to the cover object in first method whereas it is embedded into the RONI region only in second method. The outcome of the procedure is tested using several attacks and analyzed for payload capacity. The authors in [60] stated a dual watermarking approach using transform domain methods. Different set of ECC's further test the operation of the stated approach. Imperceptibility and robustness analysis showed the proposed procedure's improved performance. Moreover, a transform domain based watermarking technique is introduced by the authors in [61] which is secure and robust at the same time. In this technique the secret information is inserted at particular wavelet sub components through secure spread-spectrum scheme. The procedure is comprehensively tested by BCH and found to have resistance to attacks and shows good visual image quality. In addition to it, the performance of proposed procedure yielded better outcomes when compared to latest reported techniques given in [62-63].The authors in [23] stated a region specific watermarking scheme which validates medical modalities. The watermark information is produced from the ROI part of cover object and inserted into RONI part. Extensive analysis when subject to various attacks revealed the proposed scheme's enhanced robustness and perceptual quality.

The authors in [24] reported a watermarking technique based on ROI and RONI in transform domain using IWT. In this technique, the hash value, recovered component of ROI and EPR data is placed into RONI area of the cover. The outcome of the experimental verification revealed that the reported technique showed accurate tamper detection and robustness to attacks. A watermarking method which is robust and automatically marks ROI is proposed in [64] by the authors. Experimental evaluation proved that the stated method can counter different attacks. A region oriented watermarking technique is introduced by the authors in

[65] for tele-medical applications. The partitioning of the cover object into ROI and RONI is done initially after which two watermark data scrambled using a cryptographic procedure is implanted into both sections of host image. Extensive testing of the introduced technique using SSIM and PSNR is found to be better when compared with existing method mentioned in [66]. Authors in [67] stated a region oriented watermarking technique which uses a blind watermark. The stated technique detects tampering attempts and inserts two dissimilar watermarks into the RONI and ROI section of host image. The technique is tested for SSIM, payload capacity and PSNR. The comparative analysis showed good performance when compared with [68-69]. A reverse dither modulation (RDM) and differential evolution based blind watermarking scheme is introduced in [70]. To begin with, the original medical image is partitioned into sub components followed by DWT transformation on each component and then it's SVD. Particular SVD vector values are utilized for inserting watermark data post encryption. Experimental testing is carried out using MSSIM and PSNR and demonstrates the progress in results when compared to other comparable techniques [71-76]. LSB and DWT-SVD based watermarking approach is presented in [77]. The proposed approach partitions the cover object into ROI and RONI sections. Further three separate watermarks are implanted into chosen DWT sub-blocks (RONI portion) of medical image and altered through SVD. On investigating the competence of the proposed approach it is observed that it is secure with respect to e-health systems. The authors in [78] reported a robust watermarking method using sparse coding. In this method sparse coding is operated on the combined watermark, which is done with the help of ROI part of cover and EPR data. The embedding of the watermark information is done using singular vectors of RONI of cover. The reported method offers good quality images with good robustness to attacks.

The authors in [79] stated a DWT-KLT based watermarking technique for health services. Both transforms are used in modifying the host image further, watermark data is modified using turbo code ahead of embedding. The performance is estimated through WPSNR, NC and PSNR and showed to be fit for medical services. A fragile watermarking procedure is reported by the authors in [80].The procedure splits the original image in three regions such as RONI, ROI and boundary section. The ROI data and watermark data for the purpose of authentication is inserted in the boundary section. Furthermore, extracted data (ROI) is implanted into RONI region of cover object. A DWT-SVD and RDM based watermarking technique is offered in [81]. Firstly, the watermark data is produced using a combination of ROI vertices, ROI hash (SHA 256), recognition code and symbol image. This watermark is encrypted using AES and embedded into (singular values) DWT component. Simulation outcomes proved that the technique yielded optimum balance among key performance metrics.

The authors in [82] stated a watermarking technique that uses a blind watermark, particle swarm optimization (PSO) and genetic algorithm (GA). Experimental outcomes are analyzed using PSNR, embedding capacity and SSIM. Comparison with [83-86] showed improved results when compared with stated technique. A blind-fragile watermarking scheme is reported by the authors in [20]. The watermark information in the form of hash generated using ROI and ciphered EPR data is inserted in the medical image. Experimental evaluation shows that the scheme is appropriate for tele-medical applications.

The authors in [87] introduced a robust watermarking method which uses transform techniques. The proposed method directly inserts the watermark into the singular values of chosen DWT sub components. Experimental analysis revealed that presented method withstands attacks with improved robustness. A watermarking scheme with improved capacity and attack resistance is reported by the authors in [88]. The ROI hash and EPR is embedded into RONI of medical image. The EPR is encoded using class dependent coding scheme (CDCS) prior to insertion process .The introduced method counters different kind of attacks.

A fragile medical image watermarking procedure using Arnold transform and SVD through a fragile watermark is proposed in [89]. The procedure illustrated good resistance against a set of attacks and is assessed using tamper detection accuracy and PSNR. The comparative evaluation of the proposed procedure is done with similar techniques [90-93].

A double layer security mechanism in the form of crypto- watermarking is presented by the authors in [94]. For implementing watermarking non-tensor wavelet filter banks are used to provide multi directional analysis. Further, AES, RC4 and RSA cryptographic methods are utilized separately to secure the watermarking system. Performance metrics used to analyze the performance are SSIM, NC, CV and PSNR.

A transform domain technique through a blend of DWT-DCT and SVD is introduced in [95] which embed multiple watermarks into same host image for owner verification. The embedding process begins with DWT transformation of cover followed by DCT and SVD decomposition of approximation sub- band. The singular vector of watermark data is inserted into singular vector of the host image. The text watermark is encrypted using a simple encryption scheme before embedding. The introduced technique shows good progress using payload capacity, robustness and bandwidth when compared with similar techniques [96-99].

A hybrid procedure for watermarking in medical imaging has been proposed by the authors in [100] which utilize a combination of NSCT, RDWT and SVD. Further two separate watermarks have been inserted into the same cover image to increase the security. Both the cover and the watermark(s) have been processed using the above mentioned transforms before embedding. The analysis of the outcomes is determined for robustness and transparency and showed superior performance to similar techniques [96-99, 101]. The authors in [102] presented a watermarking scheme for use in tele-care services which utilizes DWT-DCT and SVD. .In order to address the issue of integrity and authenticity three different kinds of watermarks (tumor image, physician's signature and EPR data) have been inserted into the same host image. Prior to embedding, Arnold transform is used for additional security. Further, BPNN and ECC have been implemented to enhance the attack resistance of the scheme significantly. The experimental evaluation indicates better performance [103].

In [104], author developed an encryption based watermarking scheme in wavelet domain. Prior to embedding, even and odd character of text watermark data is encrypted by different encryption scheme and the encrypted data is embedded into DWT cover image. The experimental outcome showed that the usefulness of the system in medical domain and establish superior to former technique [105]. In [106], author developed a watermarking scheme in tele-health application. After embedding through transform schemes, the encrypted version of marked data is transmitted over the network. The method offered more robustness to other schemes [45, 107].

1.8 Aim and significant contributions of the work

Based on the presented literature survey, it was identified that some of the preliminary requirements such as imperceptibility, robustness, capacity and security are mandatory for any watermarking algorithm [108]. However, it is difficult to maintain these requirements (at the same time) and is challenging area for researchers. Many of researchers used robust watermarking techniques but they are compromising with other equally important requirements. Some are very secure but computationally complex.

Therefore, motivated by such interesting issues in the area of e-healthcare, this research work aims to propose some solutions for medical information by secure watermarking techniques. Therefore, the key objectives of the present work are stated below-

(i) To examine the performance of different state-of-the-art medical image watermarking schemes to identify most prospective one.

(ii) To develop the watermarking technique (s) for medical data security that offers better performance in terms of significant factors against attacks.

(iii) To cater to the issue of robustness, imperceptibility, security and computational complexity of secret medical information at the same time.

(iv) To determine the performance of offered technique (s) by standard metric against well-known signal processing attacks.

In the first method a robust, secure and transparent watermarking is proposed for medical images. In order to do this, a transform domain based watermarking for e-healthcare is proposed. The suggested technique uses DWT, DCT and SVD to imperceptibly embed patient report/identity in to host image. Further, the method uses chaos based encryption technique to provide confidentiality of the patient medical data. Effectiveness and importance of the method is validated through both subjective and objective methods. In addition to this, experimental evaluation showed that the scheme is robust and secure for different attacks and found improved performance than former techniques. Due to importance of dual watermarking in medical domain, a secure dual watermarking approach in NSCT domain is developed in our next contribution. The method uses redundant discrete wavelet transforms (RDWT), SVD and chaotic encryption to make it efficient watermarking approach for healthcare applications. From the experimental evaluation, our method gives better performance than existing approaches. Next contribution of the thesis is development of a secure watermarking approach using low-complexity cryptographic mechanism. The aim of this proposed work is to provide robust and secure watermarking at low cost. The idea is same as our previous technique (dual watermarking approach in NSCT domain); however, this cryptographic mechanism uses Fiestel network and substitution-permutation network to provide security at low cost. 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.

Further, an improved DWT-SVD based approach for medical applications is developed in another contribution. The goal of our work is to address health data management issues. The method jointly uses hamming error correction code and chaotic encryption to provide robustness and security of the technique, respectively. Based on health data management policy, we have imperceptibly embedded more robust data at high DWT level and less robust data into the low DWT level of the cover image. The performance comparisons confirmed that our technique is superior to existing techniques for various attacks. Subsequently, the proposed technique is tested with rotation-13 encryption algorithm instead of chaotic encryption. We observed that this approach performed better than other approaches.

1.9Thesis organization

The thesis comprises of six chapters structured as follows. Chapter 1 presents the basic concept of digital watermarking, novel characteristics of digital watermark, potential applications, essential spatial and transform domain techniques, vital performance metrics, and major watermarking attacks. This is followed by literature review of various former watermarking approaches in medical domain along with performance comparison in tabular format. The transform domain and chaotic encryption based secure watermarking for e-healthcare is proposed in Chapter 2. Chapter 3 discusses a secure dual watermarking approach in NSCT domain. A secure medical image watermarking approach using low-complexity cryptographic mechanism is developed in Chapter 4. Chapter 5 presents an improved DWT-SVD, hamming error correcting code, chaotic and substitution cipher based watermarking approach. Finally, we have summarized the entire work along with future scope presented in Chapter 6.

CHAPTER 2

MEDICAL DATA SECURITY THROUGH WATERMARKING AND CHAOTIC ENCRYPTION

In this chapter, we present a transform domain based watermarking for e-healthcare. The method uses DWT, DCT and SVD to imperceptibly embed patient report/identity in to host medical image. Further, the method uses chaos based encryption technique to provide confidentiality of the medical data. Effectiveness and importance of the method is validated through both subjective and objective methods. In addition to this, experimental evaluation indicated that the scheme is resistant to dissimilar attacks and yielded improved performance than current techniques.

2.1 Introduction

The present scenario is witnessing widespread use of telemedicine services which is being accepted globally [109-110]. The ever growing health industry requires latest technological advancements for its proper sustenance and keeping up with the needs of the people related with health sector [4 and 11]. A survey on theft of identity was conducted and revealed it to be a serious offence and a prime source of fraud around the world [108, 111, 5, 47 and 112]. Moreover, security maintenance of patient/ health data is a key concern in tele-care implementations. These kinds of applications require tamper resistant and authentic dispensing of health information which is guaranteed through inserting some visible / invisible piece of data (watermark) which is capable of resisting all forms of attacks and is secure at the same time. The capability of the watermarking systems to withstand attacks and simultaneously sustaining security is a prevalent domain for researchers [47]. Off late, researchers are incorporating fusion of encryption –decryption schemes with digital watermarking to tackle the concerns regarding management of health data [47, 100 and 113]. The watermarking methods are categorized according to the domains such as transform and spatial method. Analytic research has established the superiority of transform domain methods to spatial methods [47].

Similar watermarking techniques for medical images related to the presented procedure can also be found in chapter 1[25, 27, 29-36, 43-45, 56, 66, 77, 93, 97].

The authors in [27] proposed a ROI and RONI based watermarking method for tele- health applications using transform domain techniques. The method uses PSO to imperceptibly embed the watermark into RONI portion of cover. Moreover, DWT and SVD are used for decomposing RONI section of cover. This is followed by DCT transformation of the singular vector for embedding process. Experimental analysis reveals good performance in terms of payload capacity and imperceptibility.

A spread spectrum and selective DWT based medical image watermarking technique is formulated by the authors in [45]. The formulated technique uses second level DWT to decompose the cover object followed by embedding of the two watermarks into first and second decomposition levels respectively. Experimental evaluation of the formulated technique offers good results in the form of transparency and robustness.

A robust watermarking scheme utilizing DWT, DCT and SVD is introduced in [107]. The singular coefficients of watermark are modified with singular coefficients of host image to generate a marked image. The outcomes are estimated for transparency and robustness.

Due to importance of joint encryption and watermarking in medical domain, a chaotic encryption based watermarking scheme in transform domain is proposed. The major contribution of the work as follows.

- It is evident that combination of DWT, DCT and SVD based watermarking technique performed better than the technique based on DWT, DCT, or SVD individually or the fusion of any two of them [27, 45, 107 and 109].
- Used chaos based encryption to apply on marked image prior to transmission on open channel. The encryption with watermarking enhances confidentiality of the patient medical data.
- As results indicated in Table 2.5-Table 2.6, our technique offer excellent performance for various attacks and found superior robustness to other DWT based techniques [45, 107].
- Refer Table 2.7; Subjective method is used to estimate the visual quality of the marked image.
- Medical image watermarking is used to reduce the extra bandwidth demand of digital data transmission over open channel and hidden data acts as a keyword for fast retrieval [110].

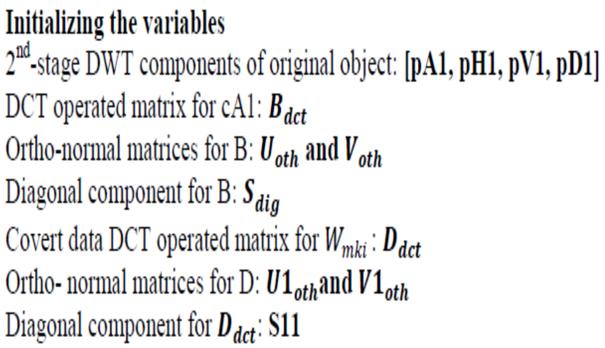
Another section of the chapter is summarized as follows. Section 2.2 describes the proposed method in detail. Experimental outcomes and result study is presented in Section 2.3.

2.2. The proposed method

The fusion of watermarking with chaos encryption is used to provide robust, secure and distortion control watermarking technique using medical image. The complete process of hiding and recovery process of the watermark is depicted in Figure 2.1. Firstly, the method uses DWT to decompose the cover image (of size 512 × 512) into four non overlapping sub-components [cA1, cH1, cV1, cD1]. Then, due to excellent energy compaction property of DCT, it is applied to approximation sub-band [cA1] of the DWT image. Further, SVD is applied on DCT image to produce singular value of the cover image. The method uses singular vector of DCT watermark data to modify (embed) the singular vector of the cover image. The imperceptibility and robustness of the method is tuned at various gain factors. The inverse of the applied techniques is used to obtain the watermarked image. Finally, encrypted watermarked image obtained via chaos based encryption is transmitted on open (unsecure) channel. At the receiver end, user decrypts the information and extracts the secret data via appropriate extraction algorithm

2.2.1 Algorithms for inserting watermark

Important steps of insertion of the watermark as follows:



Initializing the variables

2^{nd}-stage DWT components of original object: **[pA1, pH1, pV1, pD1]**

DCT operated matrix for cA1: B_{dct}

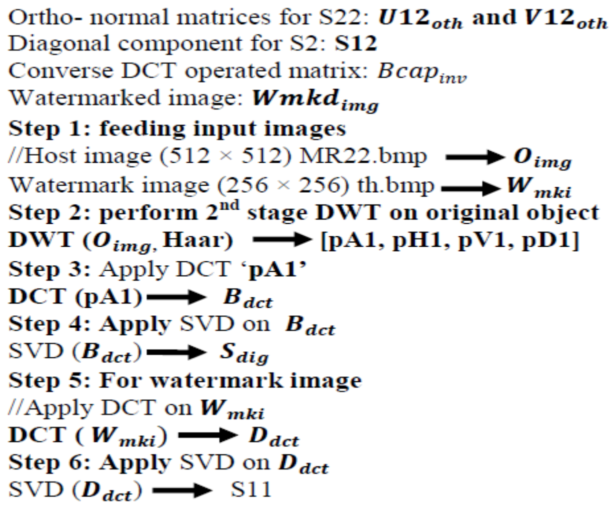
Ortho-normal matrices for B: U_{oth} and V_{oth}

Diagonal component for B: S_{dig}

Covert data DCT operated matrix for W_{mki} : D_{dct}

Ortho- normal matrices for D: $U1_{oth}$and $V1_{oth}$

Diagonal component for D_{dct}: S11



Ortho- normal matrices for S22: $U12_{oth}$ **and** $V12_{oth}$

Diagonal component for S2: **S12**

Converse DCT operated matrix: $Bcap_{inv}$

Watermarked image: $Wmkd_{img}$

Step 1: feeding input images

//Host image (512 × 512) MR22.bmp $\longrightarrow$ O_{img}

Watermark image (256 × 256) th.bmp $\longrightarrow$ W_{mki}

Step 2: perform 2^{nd} stage DWT on original object

DWT (O_{img}, Haar) $\longrightarrow$ **[pA1, pH1, pV1, pD1]**

Step 3: Apply DCT '**pA1**'

DCT (pA1) $\longrightarrow$ B_{dct}

Step 4: Apply SVD on B_{dct}

SVD (B_{dct}) $\longrightarrow$ S_{dig}

Step 5: For watermark image

//Apply DCT on W_{mki}

DCT (W_{mki}**)** $\longrightarrow$ D_{dct}

Step 6: Apply SVD on D_{dct}

SVD (D_{dct}) $\longrightarrow$ S11

Step 7: Embedding of covert data using gain factor k.
S22 = $\boldsymbol{S_{dig}}$+ k × S11; where k = gain factor
//Post embedding procedure converse of SVD followed by converse of DCT and DWT is applied to achieve ($\boldsymbol{Wmkd_{img}}$).

Step 8: Chaotic cryptographic method is performed over ($\boldsymbol{Wmkd_{img}}$ through a confidential key (KY) to get a image with jumbled pixels.
Chaotic cipher **(** $\boldsymbol{Wmkd_{img},\ KY}$) $\longrightarrow$ $\boldsymbol{C_{ho}EWmkd_{img}}$

2.2.2 Recovery steps

Important steps of recovery of the watermark as follows:

Step 1: decryption is done on the encrypted to achieve decrypted image
$\boldsymbol{C_{ho}EWmkd_{img}} \longrightarrow \boldsymbol{DecWmkd_{img}}$
Step 2: DWT decomposition is done on decrypted image.
($\boldsymbol{Dec_{img}}$, Haar) $\longrightarrow$ [pA11, pH11, pV11, pD11]
Step 3: Apply DCT on pA11
DCT (pA11) $\longrightarrow$ $\boldsymbol{A_{dct}}$
Step 4: Apply SVD on $\boldsymbol{A_{dct}}$
SVD ($\boldsymbol{A_{dct}}$) $\longrightarrow$ S_{wm}
Step 5: Recovered the embedded watermark
S_{rec}= (S_{wm} **-** $\boldsymbol{S_{dig}}$)/k
// after this process the converse of operated techniques i.e. converse of SVD and DCT is applied over the obtained parts for watermark extraction.

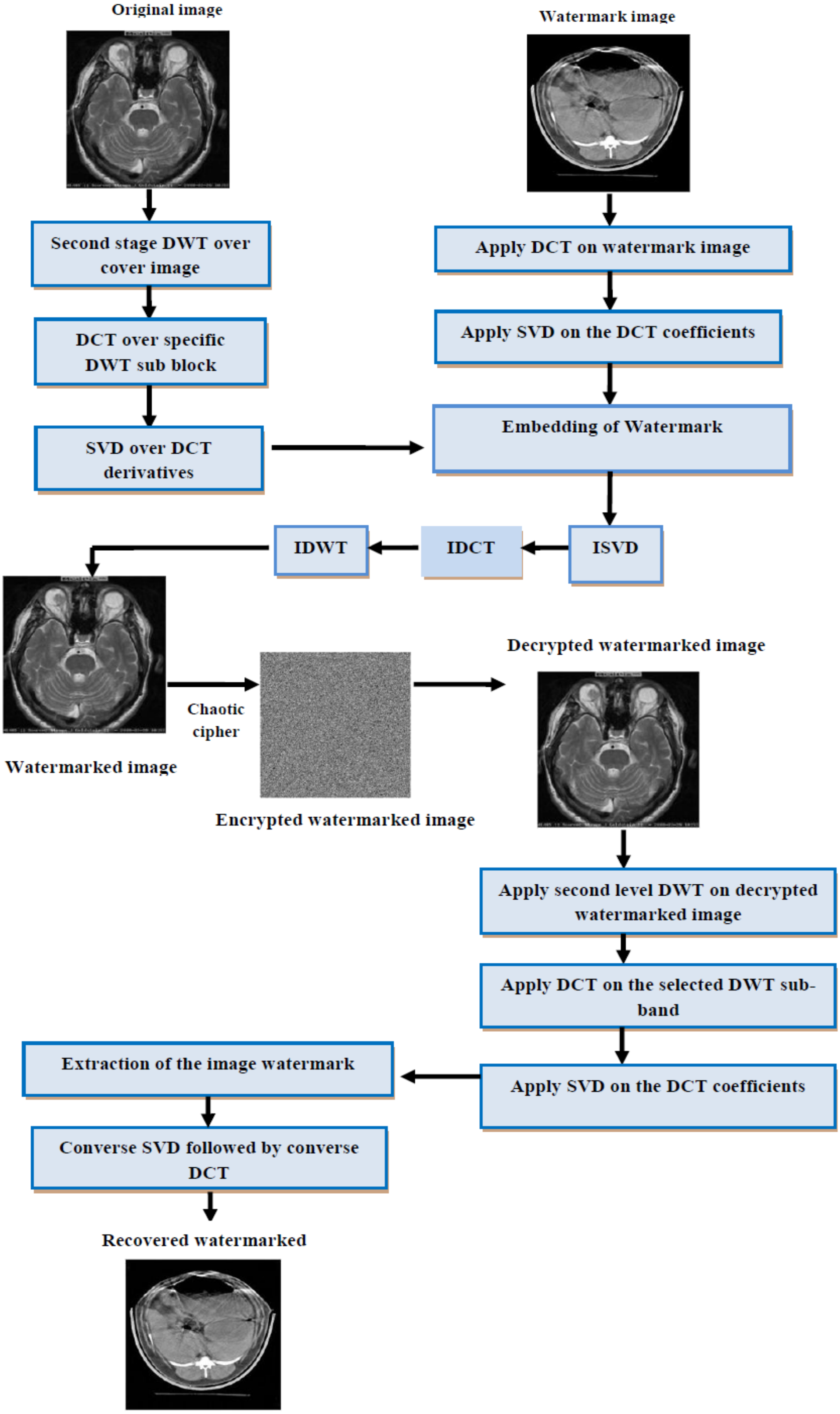

Original image
Watermark image
Second stage DWT over cover image
Apply DCT on watermark image
DCT over specific DWT sub block
Apply SVD on the DCT coefficients
SVD over DCT derivatives
Embedding of Watermark
IDWT
IDCT
ISVD
Decrypted watermarked image
Chaotic cipher
Watermarked image
Encrypted watermarked image
Apply second level DWT on decrypted watermarked image
Apply DCT on the selected DWT sub-band
Extraction of the image watermark
Apply SVD on the DCT coefficients
Converse SVD followed by converse DCT
Recovered watermarked

Figure: 2.1 Flow diagrams of watermark embedding and extraction

2.3Experimental results and performance analysis

All the experiments were conducted using MATLAB (R2013a). The host and watermark image of size 512×512 and 256× 256 respectively are used for experiments. The PSNR [107], SSIM [47] and NC [47] are used to determine the impact of our technique. Additionally, NPCR and UACI [115] are two new metrics used to determine the strength of the encryption scheme.

NPCR stands for number of changing pixel rate and UACI stands for unified averaged changed intensity. These two performance metrics are used to test the effectiveness of the encryption algorithm in resisting differential attack [115]. Differential attack the attacker always tries to capture some useful information from the encrypted image.

In other words an attacker tries to determine a relationship between the plain text image and the corresponding encrypted image. Hence encryption algorithms try to produce a large difference between the plain text image and corresponding encrypted image so that no information is available to the attacker [115].

NPCR and UACI are defined as-

Let I_m1 and I_m2 be two cipher text images before and after one pixel change in the corresponding plain text image.

The pixel value at grid (m, n) in I_m1 and I_m2 are given as I_m1 (a, b) and I_m2 (a, b)

$$NPCR = \sum\nolimits_{ab} \frac{T(a\,,b)}{R} \times 100\%$$

Where R= total number of pixels in the cipher text image and T (a, b) is defined as

$$T(a\,,b) = \begin{cases} 0, if\ I_m1(\mathrm{a,b}) = \ I_m2(\mathrm{a,b}) \\ 1, if\ I_m1(\mathrm{a,b}) \neq \ I_m2(\mathrm{a,b}) \end{cases}$$

$$UACI = \sum\nolimits_{ab} \frac{|I_m1(\mathrm{a,b}) - I_m2(\mathrm{a,b})|}{F \times R} \times 100\%$$

Where F = largest sported pixel value of cipher text image.

The proposed method has been thoroughly assessed for selected gain factor values, seven gray scale medical images [116], encryption –decryption time and various image processing attacks. Further, a comparison of our method is done with two similar techniques [45] and [107]. Some important results are depicted in fig. 2.2- fig.2.7. The fig 2.2 and fig. 2.3 show the NC and SSIM values of proposed method when subjected to different attacks, respectively. Fig. 2.4 and Fig. 2.5 show the NPCR and UACI value for different medical images, respectively. Fig. 2.6 and Fig. 2.7 show the comparative analysis of NC values with [45] and [107], respectively. The metric PSNR, SSIM, NC, NPCR and UACI of our technique at various gain is presented in table 2.1. From this table, it is interesting to see that the best value of PSNR, SSIM and NC is 74.60 dB, 1 and 0.99891, respectively. We can see that the performance highly depends on the value of gain. Further, it is determined that the value of NPCR and UACI are mostly within the permissible range [115]. These metrics are also evaluated and demonstrated in table 2.2 for seven medical images at gain value of 0.09. From table 2.2, the obtained PSNR, SSIM and NC value are greater than 35 dB, 0.76, and 0.80, respectively. The obtained value of NPCR and UACI are greater than 0.99 and 0.34, respectively.

The time taken for encrypting and decrypting various medical images is shown in table 2.3. From the table, the average encryption and decryption time (in seconds) for all medical images is 29.6547 and 29.4738respectively. The metrics NC and SSIM used to determine the robustness of our technique against various attacks are depicted in table 2.4. From table 2.4, it is clearly noticed that the NC and SSIM values are greater than 0.73 and 0.81 respectively. Therefore, it can be concluded that our technique is robust to different attacks. Further, in order to determine the improvement in the performance of our technique, the NC values of our technique is compared with similar techniques [45] and [107] given in table 2.5 and 2.6.From table 2.5, it is noticed that our technique reached a maximum NC of 0.9888 though the maximum NC in case of[45] is 0.9872. Likewise, the minimum NC value in case of [45] is 0.9496, though in case of our technique it is 0.9522 (speckle noise). From table 2.6 it can be seen for our technique that the best NC for JPEG compression is 0.9991 though it is 0.9983 in case of [107]. This assessment clearly indicates that our technique emerges to be sufficiently robust and secure when compared to existing reported techniques [45] and [107].

Table 2.1: Performance of proposed technique under different gain

Gain factor	**PSNR**	**SSIM**	**NC**	**NPCR**	**UACI**	**Average value of NPCR and UACI**
0.001	74.6099	1.0000	0.7457	0.9962	0.3468	0.6715
0.005	60.6305	0.9999	0.8820	0.9958	0.3471	0.6714
0.01	54.6099	0.9999	0.8954	0.9960	0.3469	0.6715
0.05	40.6305	0.9991	0.9750	0.9959	0.3460	0.6709
0.1	34.6099	0.9967	0.9989	0.9960	0.3442	0.6701
0.5	20.6305	0.9374	0.99990	0.9961	0.3394	0.6677

Table 2.2: Performance of proposed technique under different cover image

Image modality	**PSNR**	**SSIM**	**NC**	**NPCR**	**UACI**
X-ray	35.5250	0.9987	0.9665	0.9961	0.3636
Ultrasound	35.5250	0.9988	0.8082	0.9961	0.4835
MRI	35.5250	0.9973	0.9989	0.9962	0.3447
PET-scan	35.5250	0.9964	0.9942	0.9960	0.4460
CT-scan	35.5250	0.9991	0.9572	0.9959	0.4564
SPECT	35.5250	0.9987	0.9279	0.9962	0.4574
PET-CT	35.5250	0.7673	0.9979	0.9961	0.4701

Table 2.3 Assessment of Encryption and decryption time under different medical images

Medical image (s)	**Encryption time (in seconds)**	**Decryption time (in seconds)**
X-ray	29.6230	29.2142
Ultrasound	29.4237	29.1841
MRI	30.1990	30.7440
PET-scan	29.5713	29.0127
CT-scan	29.4558	29.21426
Average encryption/decryption time	**29.6547**	**29.4738**

Table 2.4: Assessment of SSIM and NC value under different attacks

Attack	**Noise density**	**SSIM**	**NC**
Salt and pepper noise	0.0001	0.9975	0.9983
	0.0005	0.9963	0.9990
	0.01	0.9682	0.9758
	0.05	0.8660	0.8540
	0.1	0.7531	0.8193
Gaussian noise	0.0001	0.9969	0.9979
	0.0005	0.9938	0.9980
	0.01	0.9281	0.9144
	0.05	0.7332	0.8319
	0.1	0.5863	0.8170
JPEG Compression	Q= 10	0.8627	0.9804
	Q= 50	0.9562	0.9896
	Q= 90	0.9962	0.9975
Cropping	Top left corner	0.9949	0.9966
	Top left corner	0.9966	0.8458
	Centre of image	0.8518	0.8972
	Centre of image	0.9298	0.8812
Rotation	1°	0.6335	0.9460
Gaussian low-pass filter	Mean =1, Var =0.2	0.9978	0.5406
Image scaling	×1.1	0.9823	0.9309
	×1.5	0.8594	0.8016
sharpening mask	0.8	0.9080	0.8898
	0.9	0.9044	0.8875
	0.7	0.9043	0.8916
	0.6	0.8981	0.8943
median filter	[1×1]	0.9978	0.9982
	[2×2]	0.8338	0.6973
Histogram equalization		0.8176	0.6038

Table 2.5: Comparing NC values of our method with method [45]

Attack	**Noise density**	**Gain factor**	**NC values [45]**	**NC values by proposed method**
Salt and pepper	0.04	0.7	0.9734	0.9736
	0.06	0.9	0.9641	0.9646
Gaussian noise	0.01	0.7	0.9841	0.9849
	0.01	0.9	0.9872	0.9888
Speckle noise	0.06	0.7	0.9496	0.9522
	0.08	0.7	0.9275	0.9285

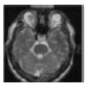
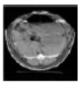
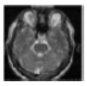
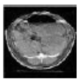
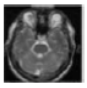
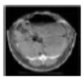
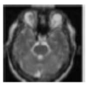
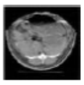
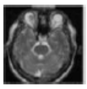
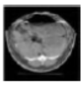
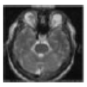
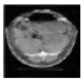
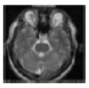
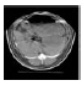
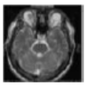
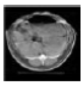
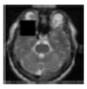
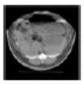
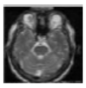
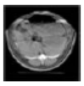
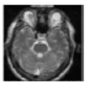
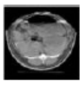
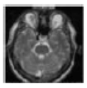
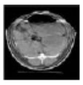
Table 2.6: Comparing NC values of our method with method [107]

Attack	**NC values [107]**	**NC values by proposed method**
Salt and pepper noise	0.9894	0.9990
JPEG Compression (25)	0.9983	0.9939
JPEG Compression (50)	0.9882	0.9896
JPEG Compression (75)	0.9983	0.9991

Table 2.7: Assessment of visual quality through subjective measure

Gain factor	Visual quality of cover image after embedding of the watermark
0.001	Excellent
0.05	Very good
0.1	Average/acceptable
0.5	Poor

Table 2.8: Some attacked watermarked and recovered watermark image under different attacks

Attacks	**Attacked image**	**Obtained NC values**	**Recovered watermark image**
Salt and pepper noise (density = 0.0001)		0.9983	
Salt and pepper noise (density = 0.0005)		0.9990	
Salt and pepper noise (density = 0.01)		0.9758	
Gaussian noise (density = 0.0001)		0.9979	
Gaussian noise (density = 0.0005)		0.9980	
Gaussian noise (density = 0.01)		0.9144	
JPEG Compression (Q = 90)		0.9975	
JPEG Compression (Q = 10)		0.9804	
Cropping (top left corner)		0.9966	
Rotation 1°		0.9460	
Image Scaling [× 1.1]		0.9309	
Median filter [1×1]		0.9982	

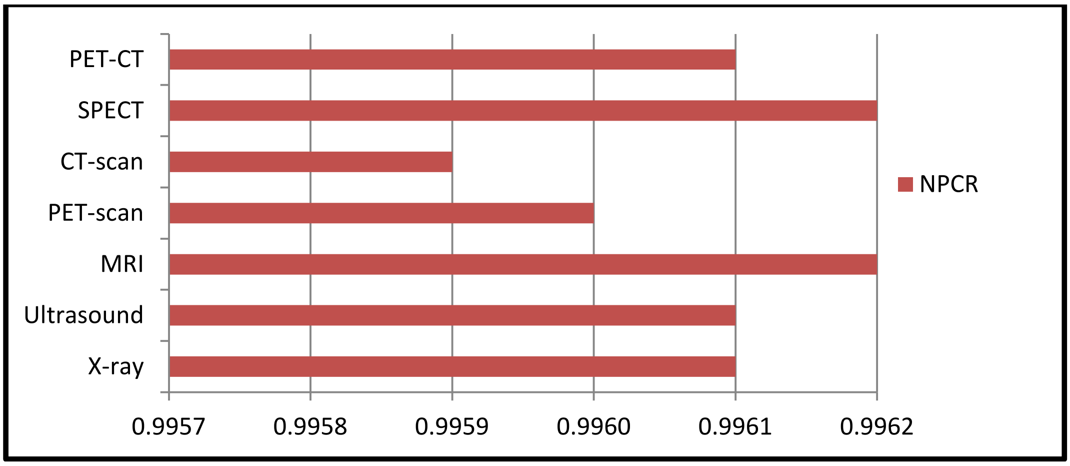


Figure 2.2: NPCR values for different medical images

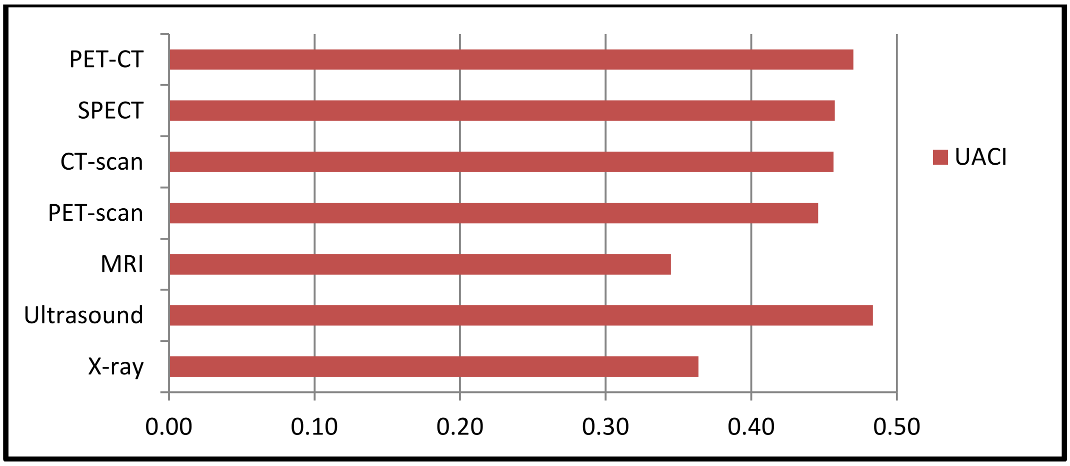


Figure 2.3: UACI values for different medical images

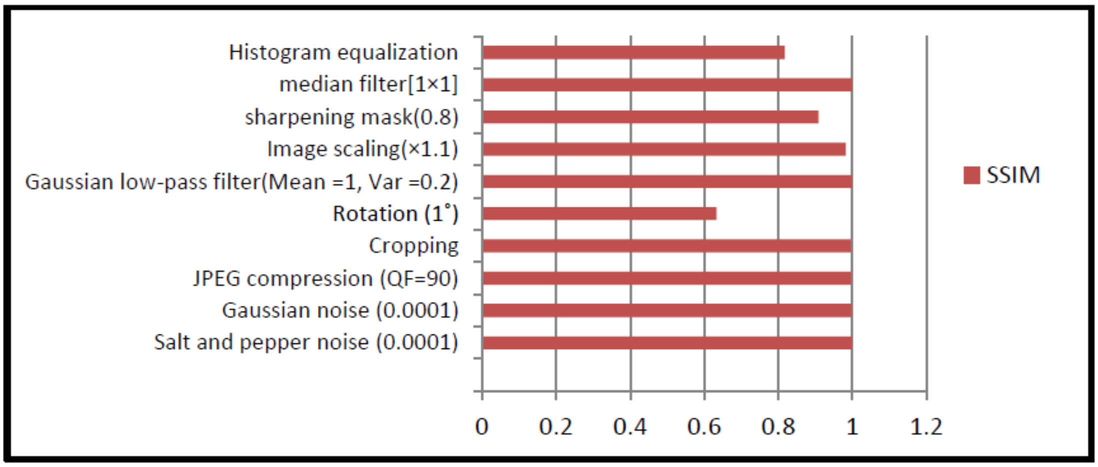


Figure 2.4: SSIM values for a range of signal processing attacks

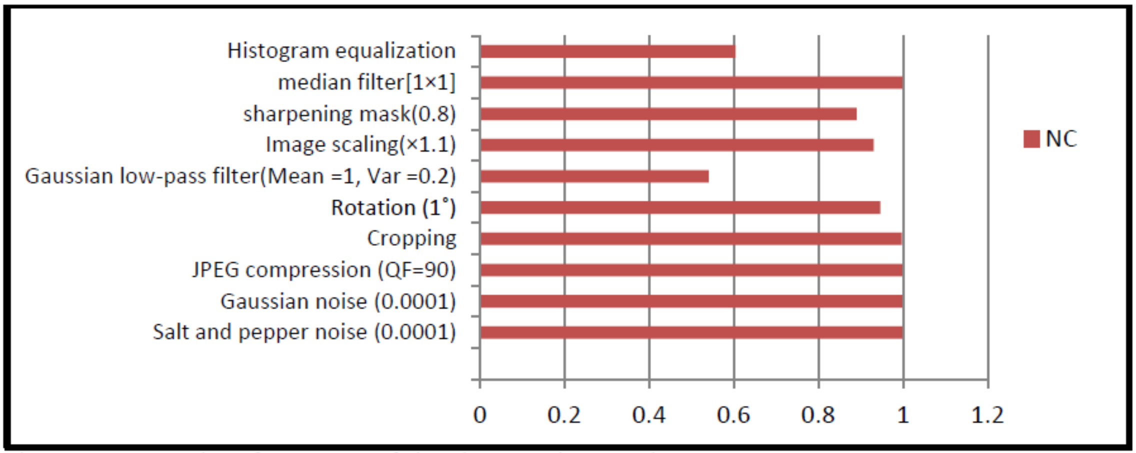


Figure 2.5: NC values for a range of signal processing attacks

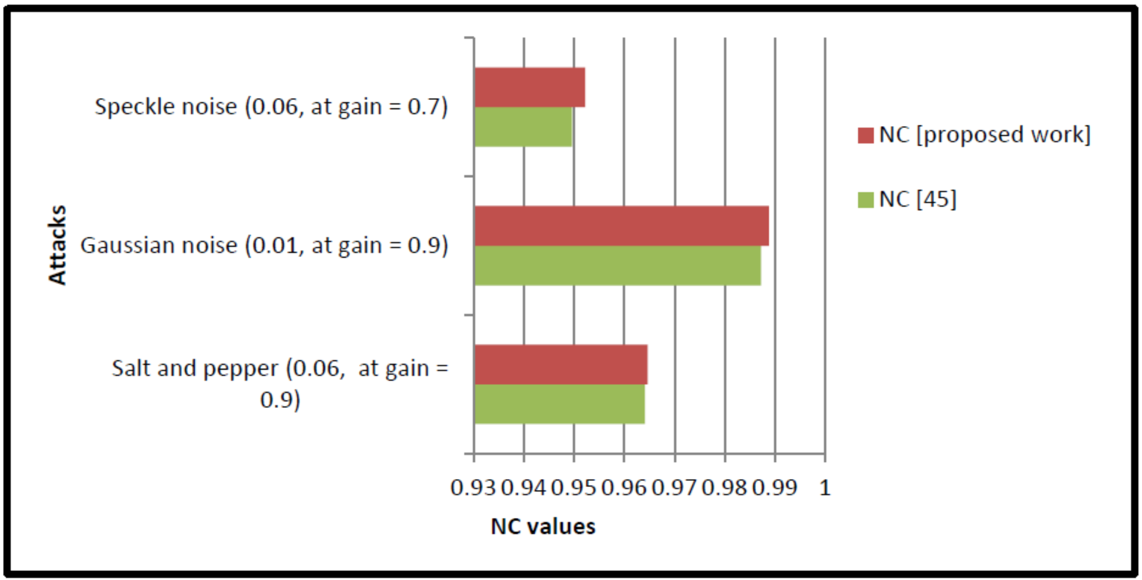


Figure 2.6: comparative estimation through NC with [45]

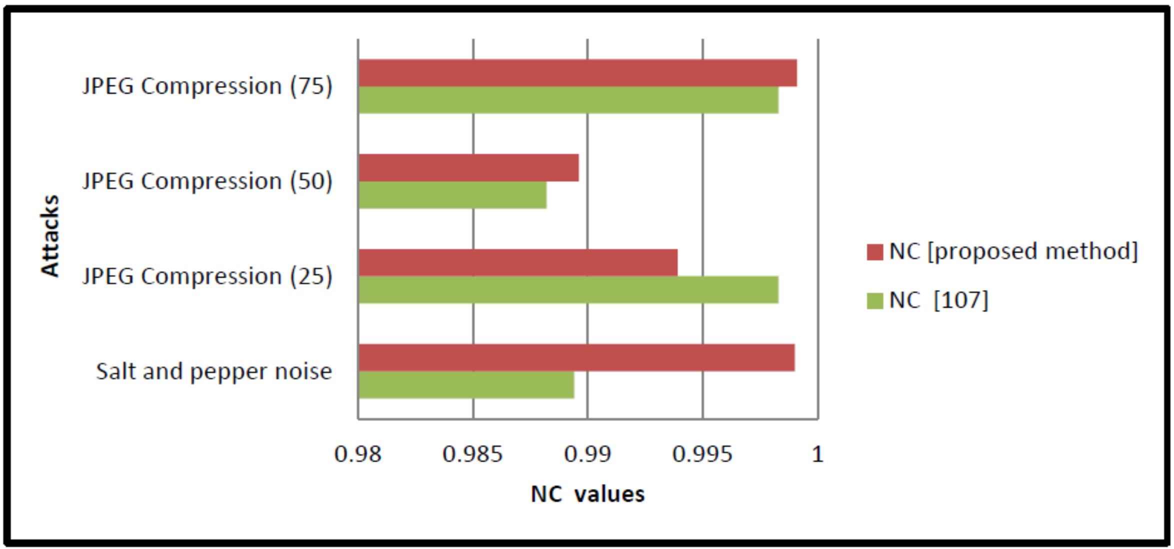


Figure 2.7: comparative estimation through NC with [107]

This chapter presented an efficient medical image watermarking scheme for embedding watermark in DWT-DCT and SVD domain. A chaos based encryption used to protect medical data. The results demonstration in terms of objective and subjective showed that the scheme is robust for different attacks and found improved the NC value than former approaches. Yet the outcome depends upon the value of gain factor, degree of noise and the watermark size. The developed technique attempts to offer a possible solution to address security issue of EPR data.

The outcomes of the chapter have been published in Multimedia Tools and Applications: Vol. 78, Issue 3, pp. 3457-3470, 10.1007/s11042-018-6263-3, Springer, stated in list of publications at the end of the Chapter 6.

CHAPTER 3

DUAL WATERMARKING APPROACH IN NSCT DOMAIN

In this chapter, a secure dual watermarking technique in NSCT domain is developed. Due to great importance of dual watermarking in the medical application, we have imperceptibly embedded both watermarks into the cover medical image. The method uses redundant discrete wavelet transform (RDWT), SVD and chaotic encryption to make it efficient watermarking for healthcare applications. Firstly, the method uses the sub-image having supreme entropy and NSCT is applied on it. Next, we apply RDWT to NSCT image to obtain the RDWT image. RDWT image is further transformed via SVD to obtain the singular vector of the image (cover).The method obtained singular vector for both watermarks with similar procedure. Furthermore, the method uses singular vectors of both watermarks to modify (embed) the vector of cover image. The inverse of SVD, RDWT, NSCT and inverse sub sampling generates a watermarked image. Finally, encrypted watermarked image is obtained via chaos based encryption and is transmitted over open (unsecure) channel. At the receiver end, user decrypts the information and extracts the secret data via appropriate extraction algorithm. The result demonstration confirms the usefulness of the proposed technique in medical application. Further, the technique provides better robustness at acceptable imperceptibility when compared with other similar approaches.

3.1 Introduction

In tele-health services, a lot of medical data transferred via information and communications technology (ICT) for the purpose of consultation and examination, and sometimes for remote diagnosis [109-110]. However, transmission of such medical data/record in open environment requires high degree of security and privacy [109-110, 4]. Due to the high security and privacy concern of medical application, we strongly need a potential tool to protect patient related sensitive data. Additionally, it is interesting to establish that medical related thefts are growing and serious crime [109]. Encryption and watermarking is the popular tool to provide security of the medical related data. Many researchers have developed encryption based watermarking technique for medical applications [20, 24, 25, 26, 37, 46, 49, 54, 55, 70, 81, 88, 89, 94, 95 and 98, 104]. However, few studies have been developed in direction to dual watermarking using encryption [24, 25, 46, 56, 60, 65, 67, 77, 80, 94, 100, 102 and 106].

Standard watermarking schemes focus towards achieving the goal of secure exchange of secret information over open channels via single watermark [108-110]. When the focus is extended in the form of copyright protection and integrity verification simultaneously the use of multiple watermarks is considered [109]. In multiple watermarking more than single watermarks are embedded to achieve many goals together. In general there are three ways in which dual watermarking is performed [108]. In the first scheme, the watermarks are either embedded one after the other or together. In the second scheme, the watermarks are embedded back to back in a continuous manner. The third scheme involves embedding of the two watermarks at the same time rather than one after the other [109]. In [20], author reported a blind watermarking technique which uses a fragile watermark. The watermark data is generated as a hash value of ROI and EPR information which is encrypted and placed inside the cover image. The results indicate that the reported technique is useful for tele-care applications.

In [24], author developed a watermarking scheme using IWT. This technique embeds the hash value, extracted portion of ROI and EPR information is placed inside the RONI area of cover. The experimental estimation shows accurate tamper detection with better accuracy and improved robustness.

In [95], author developed the embedding of multi-watermarks in wavelet domain. A simple encryption scheme is used to encrypt the EPR data prior to embedding process. Experimental demonstration on various images showed that the method offer better results with respect to NC and BER to former approaches [96-99].

To address the health data issue, author proposed a watermarking scheme using neural networks. The scrambled and compressed version of multi-watermarks is place inside the cove image. Neural network is used to improve the robustness of the scheme. Experimental demonstration on various images showed that the method offer better results with respect to NC to former approach [103].

In this chapter, a secure dual medical image watermarking technique in NSCT domain is developed. The major contribution of the work is recognized as follows.

- RDWT provides shift invariance which is required for significant hiding and recovery of watermark [117]. Further, NSCT also provide good directionality along with shift invariance which helps in better reconstruction of images [117]. The SVD provides robustness against attacks [109]. However, it is computationally high once applied individually to images. Therefore, it is preferred to use it with combination with other techniques.

- Multi-watermarks are embedded into cover image to increase the security. Simulation results clearly prove better performance of scheme than other similar approaches under consideration [95, 102].
- Used chaos based encryption [113] to apply on marked image prior to transmission on open channel. The pseudo randomness associated with chaos is used to provide a secure watermarking system [114]. Hence, encryption with watermarking enhances confidentiality of the patient medical data.
- The suggested technique also reports the medical information management issues [109].

The rest parts of the chapter are structured as follows: The chapter provide the detail description of the proposed work in Section 3.2. The outcome and analysis is presented in Section 3.3.

3.2 Proposed method

Our proposed method uses RDWT and SVD to embed dual watermarks in cover image. Firstly, the method considers the sub-image having supreme entropy and NSCT is applied on it. Next, we apply RDWT to NSCT image to obtain the RDWT image. RDWT image is further transformed via SVD to obtain the singular value of the image (cover).The method obtained singular vector for both watermarks with similar procedure. Finally, dual watermarks are imperceptibly placed inside the cover image. The inverse of SVD, RDWT, NSCT and inverse sub sampling generates a watermarked image. At last, chaos based encryption is used to protect our watermarked data prior to transmission over network. At the receiver end, user decrypts the information and robustly extracts the hidden data via appropriate extraction algorithm.

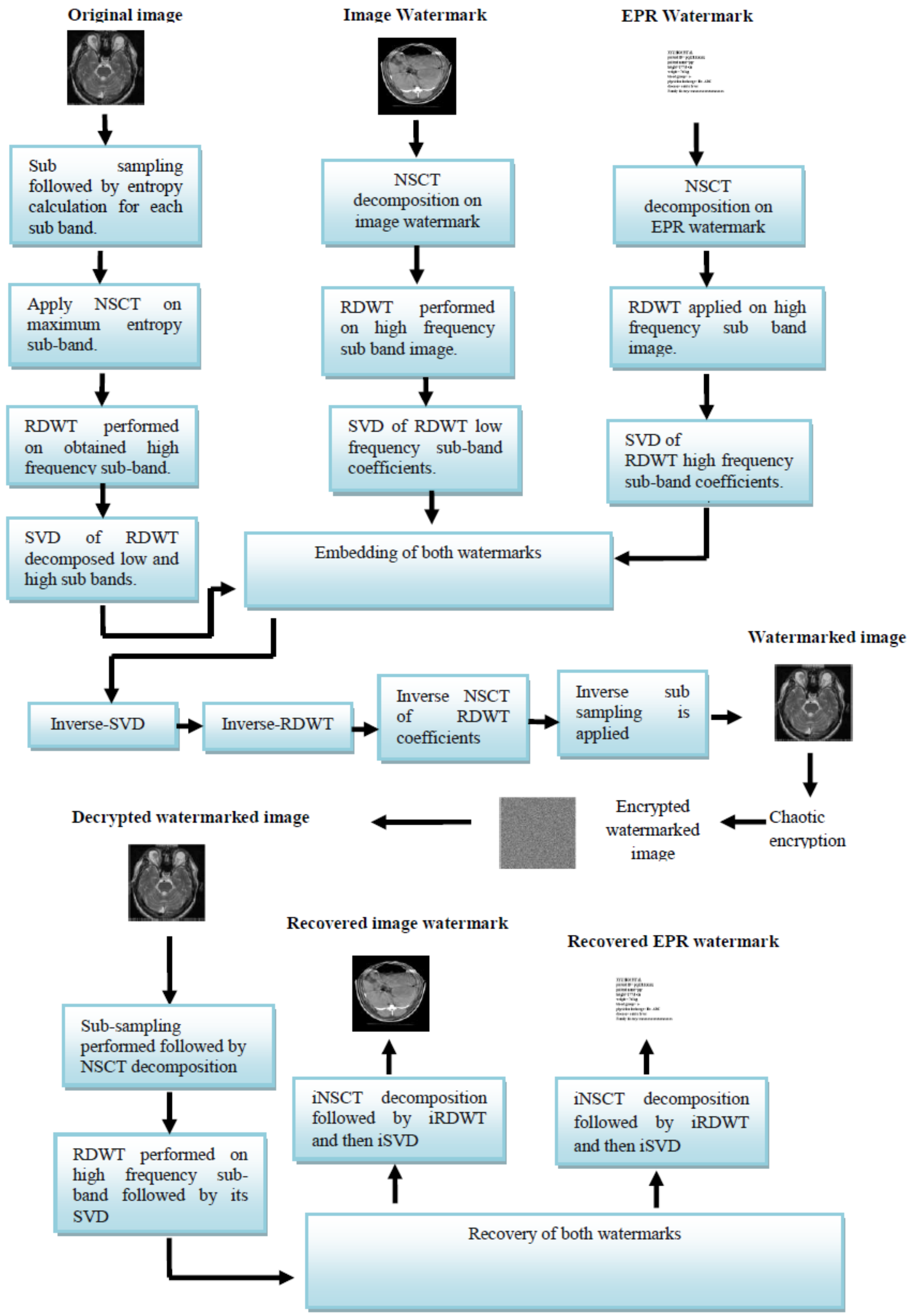

Original image
Image Watermark
EPR Watermark
Sub sampling followed by entropy calculation for each sub band.
NSCT decomposition on image watermark
NSCT decomposition on EPR watermark
Apply NSCT on maximum entropy sub-band.
RDWT performed on high frequency sub band image.
RDWT applied on high frequency sub band image.
RDWT performed on obtained high frequency sub-band.
SVD of RDWT low frequency sub-band coefficients.
SVD of RDWT high frequency sub-band coefficients.
SVD of RDWT decomposed low and high sub bands.
Embedding of both watermarks
Watermarked image
Inverse-SVD
Inverse-RDWT
Inverse NSCT of RDWT coefficients
Inverse sub sampling is applied
Chaotic encryption
Encrypted watermarked image
Decrypted watermarked image
Recovered image watermark
Recovered EPR watermark
Sub-sampling performed followed by NSCT decomposition
iNSCT decomposition followed by iRDWT and then iSVD
iNSCT decomposition followed by iRDWT and then iSVD
RDWT performed on high frequency sub-band followed by its SVD
Recovery of both watermarks

Figure 3.1: Schematic diagram of the proposed method

3.3 Experimental results and analysis

All the experiments were conducted using MATLAB R2013a. For the experimental purpose, we are using a cover image of size 512 × 512 and two watermark images of size 256×256 and 128×128 are used. Based on the robustness demand, the EPR and thorax watermark are placed inside the different level of RDWT cover image. We have extensively evaluated our method for different gain values, nine medical [116] and five non-medical cover images [118] with different size of watermarks, six wavelet filters and different signal processing attacks. Further, we have compared our method with two recent reported techniques [95] and [102].

Standard metric such as PSNR, NC, NPCR and UACI are considered to determine the performance of our technique. These metric are discussed in detail in chapter 1. Here, 'NC1' denotes similarity between original and recovered thorax watermark, and 'NC2'denotes similarity between original and recovered EPR watermark. The performance of our method in terms of standard metric is provided in Table 3.1-Table 3.9. Few important results are depicted in Fig. 3.2- Fig.3.7. The Fig 3.2 and Fig. 3.3 illustrate the NPCR and UACI scores of proposed method for different medical images used as cover. Fig. 3.4 and Fig. 3.5 respectively illustrate 'NC1' and 'NC2' values of the proposed method when subjected to different attacks. Fig. 3.6 and fig. 3.7 show the comparative analysis of NC values with [95] and [102] respectively.

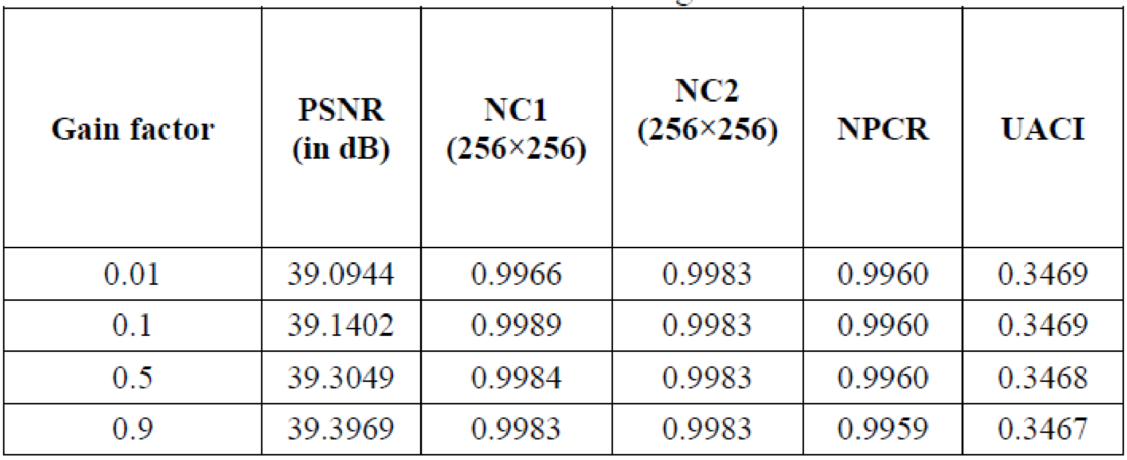
The metric PSNR, 'NC1, 'NC2', NPCR and UACI of our technique at various gain values for different size watermarks is presented in Table 3.1 and Table 3.2 respectively. From these tables, it is worth noticing that the best value of PSNR, 'NC1' and 'NC2' is 39.39 dB, 0.9989 and 0.9983, respectively. We can see that the performance highly depends on the value of gain. Further, it is determined that the value of NPCR and UACI are mostly within the permissible range [115].

These metrics are also evaluated and depicted in table 3.3 and table 3.4 for nine medical and five non- medical images at a gain value of 0.1 respectively. From table 3.3, the obtained PSNR, 'NC1'and 'NC2' values are greater than 26 dB, 0.99 and 0.95, respectively. From table 3.4, the obtained PSNR, 'NC1'and 'NC2' values are greater than 37 dB, 0.99 and 0.96, respectively.

The obtained value of NPCR and UACI for table 3.3 and table 3.4 are roughly reaching the acceptable limits [115] respectively. The listed metrics are also evaluated and presented in table 3.5 for five different wavelet filters at a gain value of 0.1. From table 3.5 the obtained PSNR, ‘NC1’and 'NC2’ values are greater than 36 dB, 0.99 and 0.95, respectively. However, the NPCR and UACI values for table 3.5 are within the acceptable range [115].

The metrics ‘NC1’ and ‘NC2’used to determine the robustness of our technique against various attacks is depicted in table 3.6. From table 3.6, it is clearly noticed that the ‘NC1’ and ‘NC2’ values are greater than 0.95 and 0.93 respectively. Therefore, it can be concluded that our technique is robust to different attacks. Performance comparison of our method with former reported approaches [95,102] is depicted in Table 3.7 and Table 3.8. From these tables it is clearly noticed that our technique offer superior robustness. Moreover, some of the watermarked images under attack and its corresponding recovered images are depicted Table 3.9.

Table 3.1: Performance measures at different gain and same size of watermarks



Gain factor	PSNR (in dB)	NC1 (256×256)	NC2 (256×256)	NPCR	UACI
0.01	39.0944	0.9966	0.9983	0.9960	0.3469
0.1	39.1402	0.9989	0.9983	0.9960	0.3469
0.5	39.3049	0.9984	0.9983	0.9960	0.3468
0.9	39.3969	0.9983	0.9983	0.9959	0.3467

Table 3.2: Performance measures at different gain and size of the watermarks

Gain factor	PSNR (in dB)	NC (256×256)	NC (128×128)	NPCR	UACI
0.01	37.0894	0.9959	0.9211	0.9958	0.3462
0.1	37.0596	0.9989	0.9624	0.9960	0.3471
0.5	36.8035	0.9983	0.9625	0.9958	0.3466
0.9	36.3747	0.9982	0.9623	0.9960	0.3475

Table 3.3: Performance measures for different medical cover images

Image modality	PSNR (in dB)	NC1 (256×256)	NC2 (128×128)	NPCR	UACI
Hand X-ray	38.6088	0.9988	0.9623	0.9963	0.4025
Ultrasound	26.9343	0.9990	0.9551	0.9958	0.4126
Brain MRI	37.0596	0.9989	0.9624	0.9960	0.3471
Breast MRI	36.6541	0.9989	0.9625	0.9962	0.3502
PET-scan	29.4585	0.9991	0.9632	0.9960	0.4461
SPECT	32.4592	0.9992	0.9633	0.9959	0.4262
Kidney stones	32.7698	0.9993	0.9629	0.9961	0.3538
Abdomen CT	32.5664	0.9989	0.9624	0.9962	0.4126
Chest CT	32.3148	0.9993	0.9546	0.9962	0.3220

Table 3.4: Performance measures for non-medical images

Image modality	**PSNR (in dB)**	**NC1 (256×256)**	**NC2 (128×128)**	**NPCR**	**UACI**
Zelda	42.0123	0.9988	0.9632	0.9958	0.2971
Lena	37.0323	0.9990	0.9632	0.9961	0.2853
Barbara	38.4987	0.9987	0.9631	0.9959	0.4206
Cell	54.4978	0.9982	0.9626	0.99603	0.2555
Coins	41.7215	0.9988	0.9632	0.9962	0.3076

Table 3.5: Performance measures for different wavelet filters

Wavelet filter	**PSNR (in dB)**	**NC (256×256)**	**NC (128×128)**	**NPCR**	**UACI**
Coif2	36.4631	0.9985	0.9604	0.9959	0.3469
db2	37.7835	0.9985	0.9574	0.9960	0.3472
db10	36.5857	0.9983	0.9593	0.9960	0.3472
Bior1.3	37.0593	0.9985	0.9637	0.9959	0.3469
Bior6.8	37.4758	0.9980	0.9618	0.9963	0.3475

Table 3.6: Robustness test for different attacks

Attack	**Noise density**	**NC 1**	**NC 2**
Salt and pepper noise	0.01	0.9528	0.9633
	0.08	0.9610	0.9586
Gaussian noise	0.01	0.9539	0.9625
	0.5	0.9666	0.9324
JPEG Compression	Q= 10	0.9986	0.9633
	Q= 50	0.9666	0.9324
	Q= 90	0.9988	0.9632
Rotation	2°	0.9986	0.9633
Gaussian low-pass filter	Var =0.4	0.9989	0.9624
	Var=0.6	0.9989	0.9624
Image scaling	×1.1	0.9986	0.9632
Median filter	[2 2]	0.9826	0.9318
Histogram equalization		0.9980	0.9626

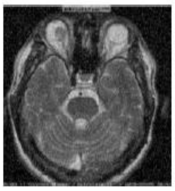
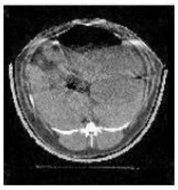
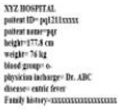
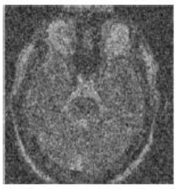
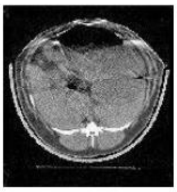
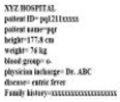
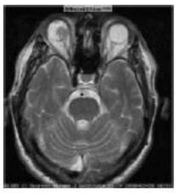
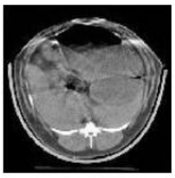
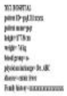
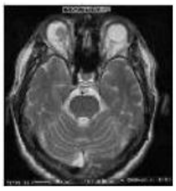
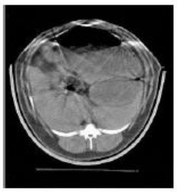
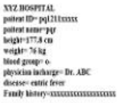
Table 3.7: Robustness comparison of our method with 'Singh' approach [95]

Attack	Noise density	Singh [95]	NC values by proposed method
Gaussian noise	mean=0,Var-0.5	0.6569	0.9329
Gaussian noise	mean= 0,Var-0.01	0.9604	0.9626
Salt & pepper noise	0.08	0.8859	0.9558
Histogram equalization		0.931	0.9632

Table 3.8: Robustness (determined by NC) comparison of our method with [102]

Attack	Noise density	NC [102]	NC [proposed method]
JPEG Compression	Quality factor =10	0.3120	0.9986
Salt and pepper noise	0.01	0.7747	0.9633
Gaussian noise	Mean =0, Var = 0.001	0.9466	0.9989
Speckle noise	Var =0.01, 0.02 and 0.005	0.9286, 0.8673and 0.9886	0.9988, 0.9990 and 0.9988
Rotation	2°	0.4442	0.9986

Table 3.9: Attacked watermarked and recovered watermark image under different attacks

Attacks	Attacked image	Obtained NC1 values	Obtained NC2 values	Recovered watermark image 1	Recovered watermark image 2
Salt and pepper noise (density = 0.08)		0.9610	0.9586		 XYZ HOSPITAL patient ID= pq1211xxxxx patient name=pqr height=177.8 cm weight= 76 kg blood group= o- physician incharge= Dr. ABC disease= entric fever Family history=xxxxxxxxxxxxxxxxxx
Gaussian noise (density = 0.5)		0.9666	0.9324		 XYZ HOSPITAL patient ID= pq1211xxxxx patient name=pqr height=177.8 cm weight= 76 kg blood group= o- physician incharge= Dr. ABC disease= entric fever Family history=xxxxxxxxxxxxxxxxxx
JPEG Compression (Q = 90)		0.9988	0.9632		 XYZ HOSPITAL patient ID= pq1211xxxxx patient name=pqr height=177.8 cm weight= 76 kg blood group= o- physician incharge= Dr. ABC disease= entric fever Family history=xxxxxxxxxxxxxxxxxx
Rotation 2°		0.9986	0.9633		 XYZ HOSPITAL patient ID= pq1211xxxxx patient name=pqr height=177.8 cm weight= 76 kg blood group= o- physician incharge= Dr. ABC disease= entric fever Family history=xxxxxxxxxxxxxxxxxx

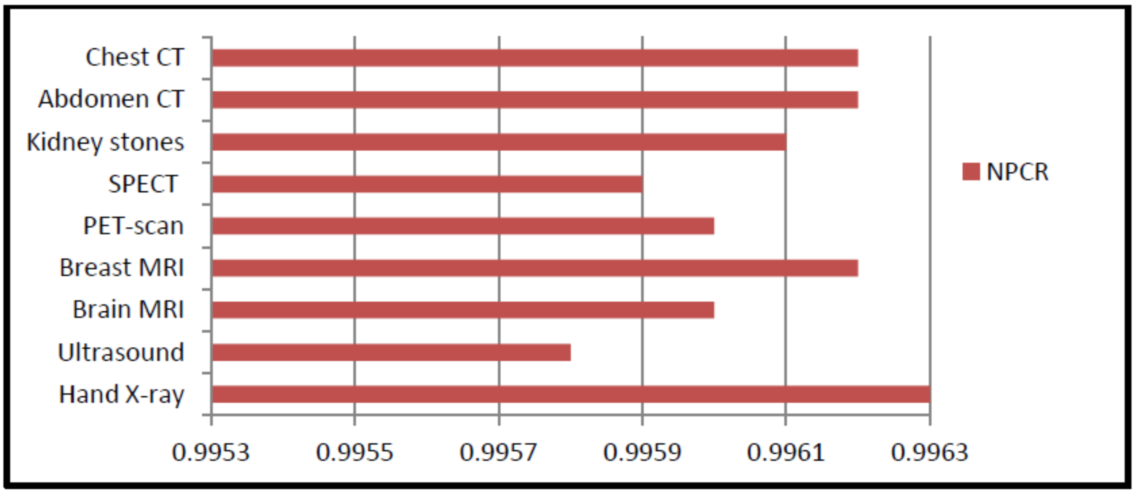


Figure 3.2: NPCR values for different medical images

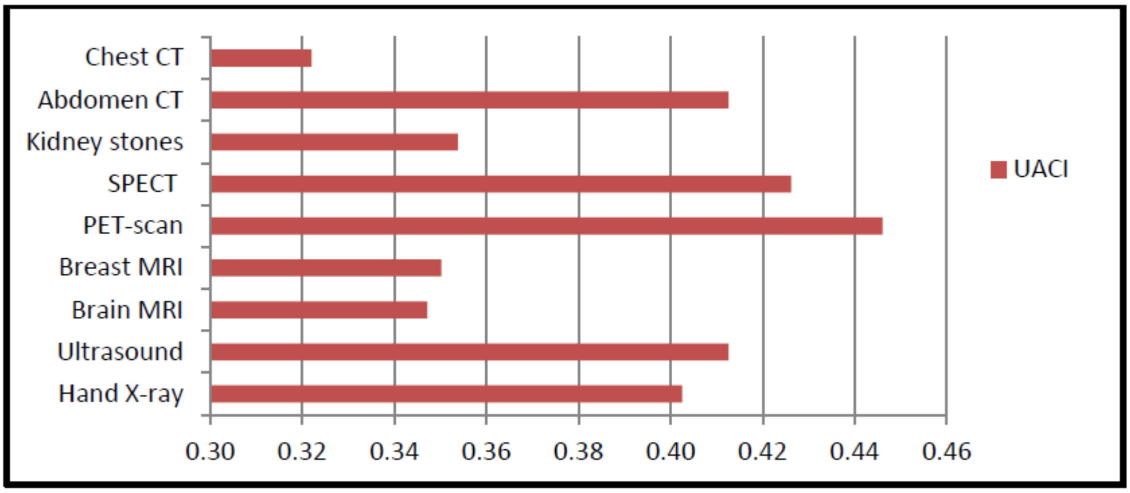


Figure 3.3: UACI values for different medical images

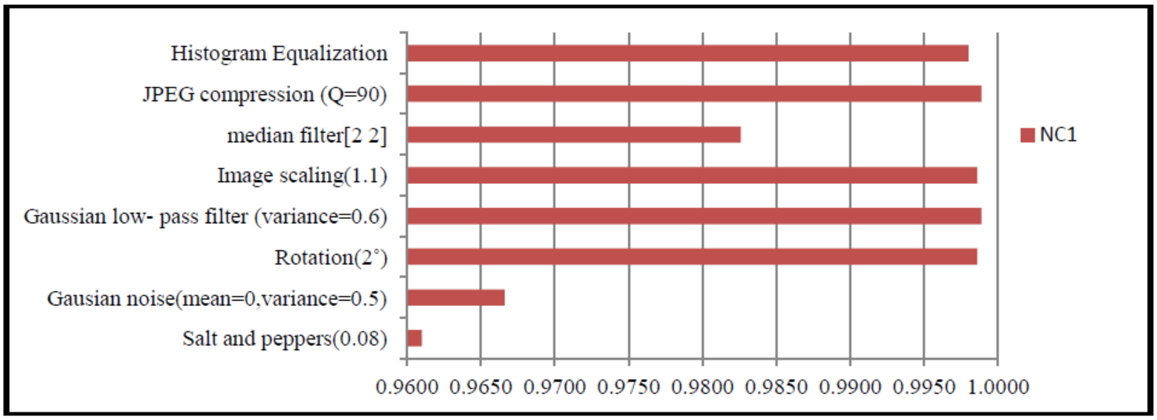


Figure 3.4: NC1 values for different attacks

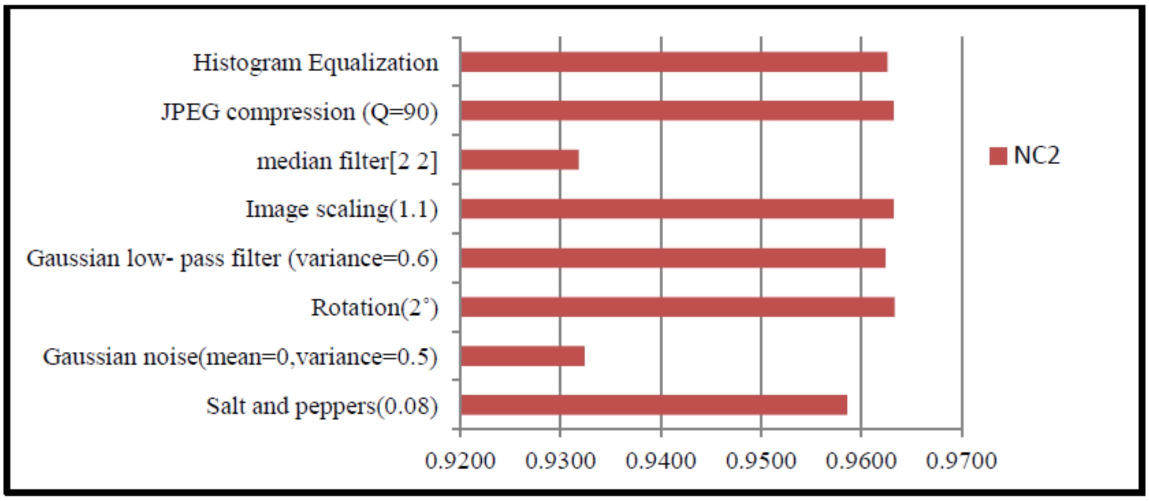


Figure 3.5: NC2 values for different attacks

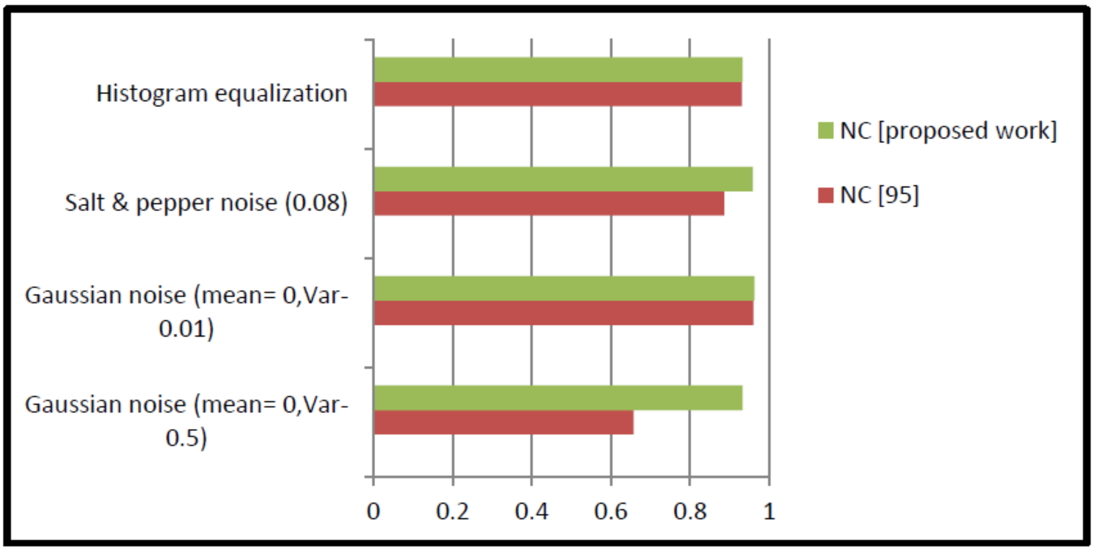


Figure 3.6: comparative estimation through NC with [95]

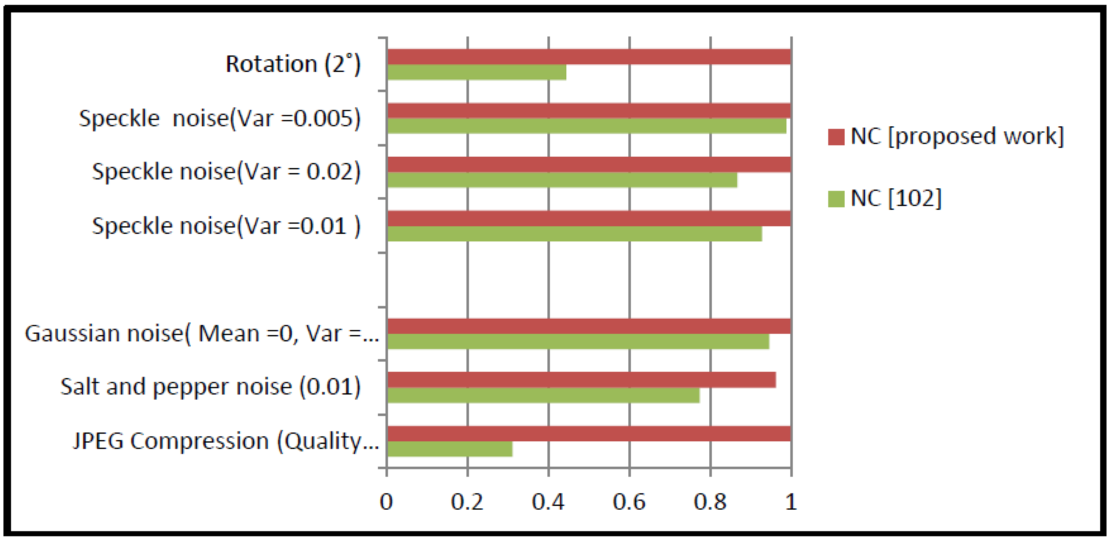


Figure 3.7: comparative estimation through NC with [102]

In this chapter, a robust and secure watermarking scheme is developed for embedding multi-watermarks (dual) in NSCT- RDWT and SVD domain. By applying chaos based encryption on watermarked image, the security of the proposed technique is improved. The developed technique offer better robustness when compared to the other approaches. Our examination and results confirm that the technique is appropriate data security for medical application.

The work presented in this chapter has been published in Multimedia Tools and Applications, pp.1-14, doi: 10.1007/s11042-018-6691-0, Springer indicated in list of publications at the end of the Chapter 6

CHAPTER 4

DUALWATERMARKING APPROACH USING LOW-COMPLEXITY CRYPTOGRAPHIC MECHANISM

In this chapter, we present a secure watermarking technique using low-complexity cryptographic mechanism. The idea is same as our previous technique (dual watermarking approach in NSCT domain as discussed in chapter 3), however, this cryptographic mechanism uses Fiestel network and substitution-permutation network to provide security at low cost. Simulation results conducted on six wavelet filters, various medical and non-medical images disclose that the technique is secure, robust, distortion-control and has low computational complexity which outperforms the other existing approaches.

4.1 Introduction

Digital augmentation of contemporary healthcare has directed the expansion of ICT based systems. Presently, tele-medical services in different forms are being exploited for distribution of medical amenities [56]. The three security necessities such as privacy, integrity and authenticity [56] call for close attention and remedial actions. Therefore, watermarking and cryptographic techniques are providing a probable way out for adequately handling the above mentioned issues [108, 112]. Cryptographic approaches consist of cipher codes, digital signatures, hash based algorithms and codes for error correction and detection [56, 8, 119 and 11]. While watermarking methods comprises of blind, robust, semi- fragile and fragile watermarks to provide content protection [27, 9]. Hence the joint approach proves to be better in security and reliability for tackling coercion to security.Similar state-of-the-art watermarking techniques associated with our approach are presented in [26, 29, 37, 55, 54, 65, 70, 94, 95, and 96]. A secure watermarking technique using DWT which is able to resist attacks is reported in [26]. Initially the original image is divided on the basis of ROI and RONI to which DWT is applied. The ciphered watermark information is inserted into the RONI segment of the original image. The performance is realised in terms of SSIM, PSNR and NC.

In [95], author developed the embedding of multi-watermarks in wavelet domain. A simple encryption scheme is used to encrypt the EPR data prior to embedding process. Experimental demonstration on various images showed that the method offer better results with respect to NC and BER to former approaches [96-99].

A multiple watermarking scheme using a fusion of NSCT-RDWT and SVD transforms is proposed by the authors in [117]. The scrambled version of the watermark is embedded into cover. The performance analysis reveals improved results for transparency and robustness.

In this chapter, a secure watermarking technique using low-complexity encryption scheme is developed. The key contribution of the work is identified as

- Combination of RDWT and NSCT provides shift invariance, good directionality and better reconstruction of images which makes our system efficient for medical domain [95,117]. The SVD provides robustness against attacks [109]. However, it is computationally high once applied individually to images. Therefore, it is preferred to use it with combination with other techniques.
- Multi-watermarks are embedded into cover image to increase the security. Simulation results clearly prove better performance of scheme than other similar approaches under consideration [95, 117].
- Used lightweight symmetric encryption [120] on marked image prior to transmission over open channel. The cipher scheme instead of using multiple rounds works on only five rounds to provide low computational cost [120]. Hence, encryption with watermarking enhances confidentiality of the patient medical data at low cost.
- The method also addresses the medical data management issues [109].

The rest parts of the chapter are structured as follows: The chapter provide the detail description of the proposed work in Section 4.2. The outcome and analysis is presented in Section 4.3.

4.2. Proposed method

The idea is same as the developed technique in Chapter 3. However, the proposed method offers not only good robustness, but also security at low cost. The method uses RDWT and SVD to embed dual watermarks in cover image. In the first step, the method considers the sub-image having supreme entropy and NSCT is applied on it. Next, we apply RDWT to NSCT image to obtain the RDWT image. RDWT image is further transformed via SVD to obtain the singular value. The scheme obtains singular vector for both watermarks with similar procedure. Finally, both watermarks are imperceptibly placed inside the cover image. The inverse of SVD, RDWT, NSCT and inverse sub sampling generates a watermarked image. At last, Fiestel network and substitution-permutation network based encryption is used to apply on watermarked data prior to transmission over open environment. At the receiver end, user decrypts the information and robustly extracts the hidden data via appropriate extraction algorithm. The flow diagram of the complete process of the proposed work is depicted in Fig. 4.1 a-b.

4.2.2 **Step by step process of inserting watermark**

Step 1: let an input image of size (512×512) be read as input and sub-sampling operation of original image is done in the following way:

$$I_1(i,j) = I[2(i-1),2(j-1)] \qquad (2)$$
$$I_2(i,j) = I[2(i-1),2(j-1)]$$
$$I_3(i,j) = I[2(i-1),2(j-1)]$$
$$I_4(i,j) = I[2(i-1),2(j-1)]$$

Step 2: Calculation and selection of highest entropy score of sampled cover image derivative (E_{nt}).

Step 3: first stage NSCT transformation upon E_{nt} is given below-

$$NSCT(E_{nt}) = [E_{ntl1}, E_{ntl2}, E_{nth111}, E_{nth112}, E_{nth121}, E_{nth122}] \qquad (3)$$

Where, E_{ntL1} and E_{ntL2} denotes components with low frequency.
$E_{nth111}, E_{nth112} E_{nth121}andE_{nth122}$ denotes components with high frequency.

Step 4: To E_{ntH121} , first stage RDWT is performed

$$RDWT(RE_{H121}) = [\,RE_{A1}, RE_{H1}, RE_{V1}, RE_{D1}] \qquad (4)$$

Step 5: applying singular value decomposition (SVD) of Re_{a1} and Re_{h1} sub bands.

$$SVD(Re_{a1}) = [Ru_{ea1} Rs_{ea1} Rv_{ea1}] \qquad (5)$$

$$SVD(Re_{h1}) = [Ru_{eh1} Rs_{eh1} Rv_{eh1}] \qquad (6)$$

For watermark images:

Step 6: Reading first watermark W_{m1} of height and width of 256 and second watermark W_{m2} height and width of 128 respectively as input. To these watermark images NSCT is applied.

(256×256) and second watermark W_{m2} (128×128) for

$$NSCT(W_{m1}) = [W_{m1l1}, W_{m1l2}, W_{m1h111}, W_{m1h112}, W_{m1h121}, W_{m1h122}] \qquad (7)$$

$$NSCT(W_{m2}) = [W_{m2l1}, W_{m2l2}, W_{m2h111}, W_{m2h112}, W_{m2h121}, W_{m2h122}] \qquad (8)$$

Step 7: RDWT is performed over NSCT manipulated components of both watermarks -

$$RDWT(W_{m1}) = [\, W_{m1a1}, W1_{m1h1}, W_{m1v1}, W_{m1d1}] \qquad (9)$$

$$RDWT(W_{m2}) = [\, W_{m2a1}, W_{m2h1}, W_{m2v2}, W_{m2d1}] \qquad (10)$$

Step 8: SVD of $W1_{A1}$ and $W2_{H1}$ sub bands is computed as follows-

$$SVD(W_{m1a1}) = [U_{m1w1a1} S_{m1w1a1} V_{m1w1a1}] \qquad (11)$$

$$SVD(W_{m2h1}) = [U_{m2w2h1} S_{m2w2h1} V_{m2w2h1}] \qquad (12)$$

Step 9: implanting the dual watermarks through the altered SVD vectors given below-

$$S_{m1} = S_{m1ea1} + g \times S_{m1w1a1} \qquad (13)$$

$$S_{m2} = S_{m2eh1} + g \times S_{m2w2h1} \qquad (14)$$

Where g= gain factor.

Step 10: Sequentially performing inverse of the applied techniques which generates the watermarked imageW_{m12}.

Step 11: Finally Applying lightweight (low complexity) encryption L_e on the watermarked image W_{m12} using 64 –bit secret key (K) in order to achieve an encoded watermarked imageE_{wm12}.

$$L_e(W_{m12}) = [E_{wm12}] \qquad (15)$$

4.2.3 Watermark extraction

Step 1: The encrypted watermarked image E_{wm12} is converted to decrypted watermarked image D_{wm12} after applying the decryption processD_e.

$$D_e(E_{wm12}) = [D_{wm12}] \qquad (16)$$

Step 2: Read decrypted watermarked imageD_{wm12} as input and performing sub – sampling of it as done in equation (2).

Step 3: Calculating maximum entropy values of the sub sampled components and selecting the maximum value (D_w).

Step 4: Applying first level NSCT upon (D_w) which results into two low frequency and four high frequency sub-bands generated after forward transformation of (D_w) . Further, applying first level RDWT decomposition upon (D_{wd121})as follows-

$$RDWT(D_{wd121}) = [D_{wA1}, D_{wH1}, D_{wV1}, D_{wD1}] \qquad (17)$$

Step 5: Calculating the SVD of obtained decomposed components E_{wA1} andE_{wH1} as follows-

$$SVD(D_{wA1}) = [U_{wA1}S_{wA1}V_{wA1}] \qquad (18)$$

$$SVD(D_{wH1}) = [U_{wH1}S_{wH1}V_{wH1}] \quad (19)$$

Step 6: Finally, both watermarks are recovered by using the modified SVD coefficients in the equation as follows-

$$S_{rec1} = (S_{wA1} - S_{W1A1})/\alpha \qquad (20)$$

$$S_{rec2} = (S_{wH1} - S_{W2H1})/\alpha \quad (21)$$

Step 7: Applying inverse SVD on the components S_{rec1}andS_{rec2} followed by inverse RDWT and NSCT to obtain recovered watermark images separately.

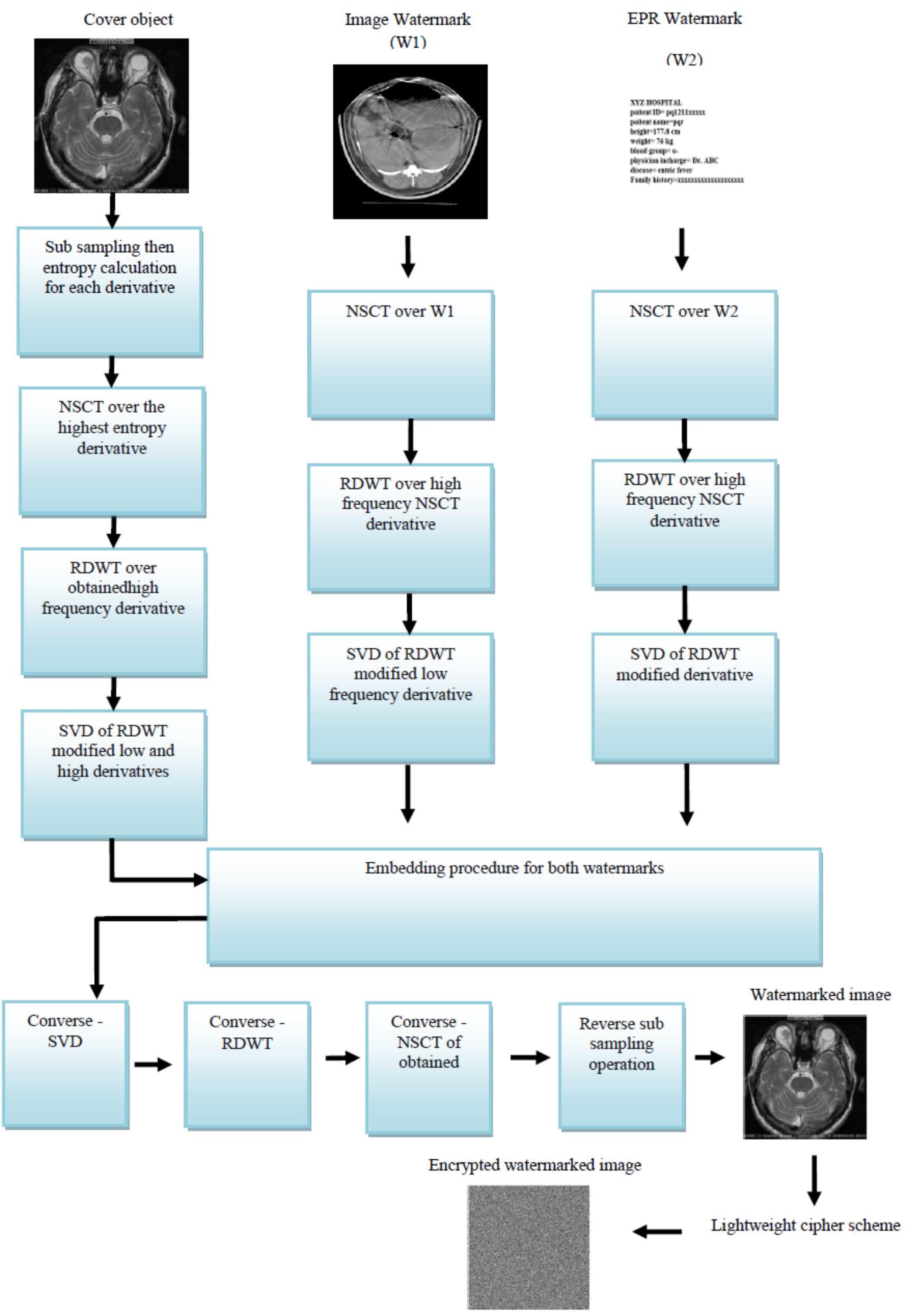

Cover object
Image Watermark
(W1)
EPR Watermark
(W2)
XYZ HOSPITAL
paitent ID= pq1211xxxxx
paitent name=pqr
height=177.8 cm
weight= 76 kg
blood group= o-
physician incharge= Dr. ABC
disease= entric fever
Family history=xxxxxxxxxxxxxxxxxx
Sub sampling then entropy calculation for each derivative
NSCT over W1
NSCT over W2
NSCT over the highest entropy derivative
RDWT over high frequency NSCT derivative
RDWT over high frequency NSCT derivative
RDWT over obtainedhigh frequency derivative
SVD of RDWT modified low frequency derivative
SVD of RDWT modified derivative
SVD of RDWT modified low and high derivatives
Embedding procedure for both watermarks
Converse - SVD
Converse - RDWT
Converse - NSCT of obtained
Reverse sub sampling operation
Watermarked image
Encrypted watermarked image
Lightweight cipher scheme

Figure 4.1: (a) flow diagram of embedding

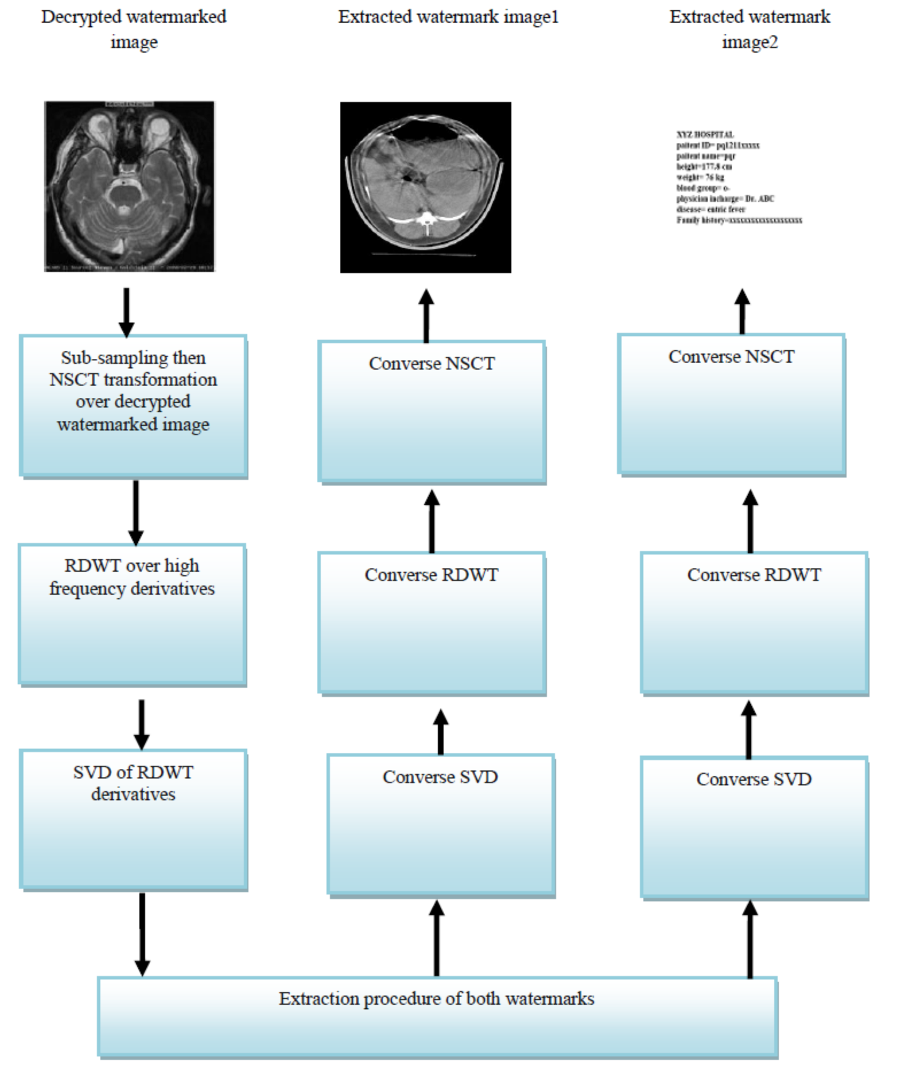

Decrypted watermarked image
Extracted watermark image1
Extracted watermark image2
XYZ HOSPITAL
paitent ID= pq1211xxxxx
paitent name=pqr
height=177.8 cm
weight= 76 kg
blood group= o-
physician incharge= Dr. ABC
disease= entric fever
Family history=xxxxxxxxxxxxxxxxxxx
Sub-sampling then NSCT transformation over decrypted watermarked image
Converse NSCT
Converse NSCT
RDWT over high frequency derivatives
Converse RDWT
Converse RDWT
SVD of RDWT derivatives
Converse SVD
Converse SVD
Extraction procedure of both watermarks

Figure 4.1: (b) Flow diagram of extraction

4.3. Simulation results and analysis

All the experiments were implemented using MATLAB R2013a. In order to conduct the experiments cover image of size 512×512 and two watermark images of size 256×256 and 128×128 are used. According to the robustness requirement the thorax and EPR watermarks are embedded into alternate RDWT sub- levels. Our method has been evaluated thoroughly for different gain values, ten medical [116] and five non-medical cover images [118] with different sized watermarks, six wavelet filters and various attacks. Further, the performance our method is compared with two existing techniques [117] and [95].

The fundamental metrics such as PSNR [110], NC [110], UACI and NPCR [115] are used to evaluate the performance of our technique. Detailed explanation of these metrics is given in chapter 1. The normalized correlation between original and recovered watermark is represented by the notation ‘NC1’ and normalized correlation between original and recovered EPR watermark is represented by ‘NC2’. The performance of our method using fundamental metrics is presented in table 4.1-table 4.7. Some of the significant results are depicted in fig. 4.2- fig.4.7. The fig 4.2 and fig. 4.3 illustrate the NPCR and UACI scores of proposed method for different medical images used as cover. Fig. 4.3 and fig. 4.5 illustrate ‘NC1’ and ‘NC2’ values of the scheme when subjected to unrelated attacks respectively. Fig. 4.6 and fig. 4.7 show the comparative evaluation of NC values with [117] and [95] respectively.

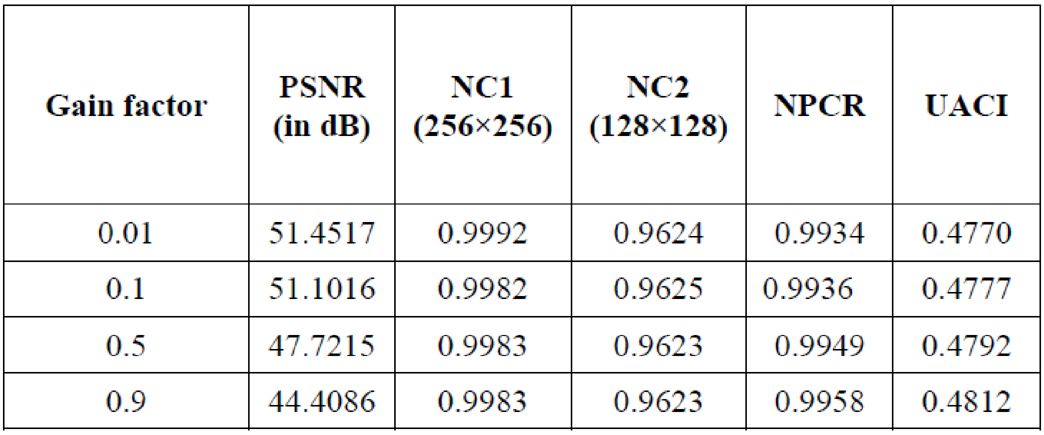
The metric PSNR, ‘NC1, ‘NC2’, NPCR and UACI of our technique at various gain values for different size watermarks is presented in table 4.1. From this table, it is seen that the best value of PSNR, ‘NC1’ and ‘NC2’ is 51.45 dB, 0.9992 and 0.9625 respectively. It is observed that the performance depends majorly on the gain value. In addition to this, the value of NPCR and UACI are approximately reaching the permissible range [115].

These metrics are also estimated and presented in table 4.2 and table 4.3 for ten medical and five non- medical images at a gain value of 0.1 respectively. From table 4.2, the obtained PSNR, ‘NC1’and 'NC2’ values are greater than 24 dB, 0.99 and 0.95, respectively. From table 4.3, the obtained PSNR, ‘NC1’and 'NC2’ values are greater than 36 dB, 0.99 and 0.96, respectively.

The NPCR and UACI values obtained for table 4.2 and table 4.3 are more or less reaching the acceptable limits [115] respectively.

The depicted metrics are also estimated and shown in table 4.4 for six different wavelet filters at a gain value of 0.1. From table 4.4 the obtained PSNR, ‘NC1’and 'NC2’ values are greater than 48 dB, 0.99 and 0.95, respectively. However, the NPCR and UACI values for table 4.4 are almost attaining the acceptable values [115]. The metrics ‘NC1’ and ‘NC2’ which are used to establish the robustness of our technique against variety of attacks are depicted in table 4.5. From table 4.5, it is noticed that the values obtained for ‘NC1’ and ‘NC2’ are greater than 0.95 and 0.95 respectively. Hence, it can be stated that our technique is able to survive different attacks. Comparative evaluation of our method to similar methods [117, 95] is depicted in table 4.6 and table 4.7 respectively. From these tables it is clearly observed that the ability our method to resist attacks is better than the compared methods [117] and [95].

Table 4.1: Performance metrics at specific gain



Gain factor	**PSNR (in dB)**	**NC1 (256×256)**	**NC2 (128×128)**	**NPCR**	**UACI**
0.01	51.4517	0.9992	0.9624	0.9934	0.4770
0.1	51.1016	0.9982	0.9625	0.9936	0.4777
0.5	47.7215	0.9983	0.9623	0.9949	0.4792
0.9	44.4086	0.9983	0.9623	0.9958	0.4812

Table 4.2: Performance metrics for ten cover medical cover media

Cover media	**PSNR (in dB)**	**NC1 (256×256)**	**NC2 (128×128)**	**NPCR**	**UACI**
Kidney stones	32.7698	0.9994	0.9629	0.9963	0.3495
PET-scan	29.4585	0.9992	0.9632	0.9974	0.4306
SPECT	32.4592	0.9992	0.9633	0.9973	0.4194
Ultrasound	26.9343	0.9991	0.9551	0.9962	0.4063
Chest CT	24.0722	0.9979	0.9505	0.9963	0.4496
Hand X-ray	38.6482	0.9988	0.9630	0.9971	0.3960
PET-CT	51.1016	0.9982	0.9625	0.9936	0.4777
MRI transversal	38.7159	0.9989	0.9626	09962	0.3417
Breast MRI	36.6514	0.9989	0.9632	0.9960	0.3500
Brain MRI	37.7986	0.9989	0.9632	0.9962	0.3471

Table 4.3: Performance metrics for general images

Cover media	**PSNR (in dB)**	**NC1 (256×256)**	**NC2 (128×128)**	**NPCR**	**UACI**
Cameraman	36.1472	0.9993	0.9631	0.9959	0.3104
Barbara	38.4987	0.9987	0.9631	0.9960	0.4198
Cell	54.4978	0.9983	0.9626	0.9960	0.2554
Zelda	42.0123	0.9988	0.9632	0.9962	0.2968
Coins	41.7215	0.9988	0.9632	0.9962	0.3078

Table 4.4: Performance metrics for different wavelet filters

Wavelet filter	**PSNR (in dB)**	**NC1 (256×256)**	**NC2 (128×128)**	**NPCR**	**UACI**
db5	50.9645	0.9979	0.9609	0.9940	0.4780
Sym4	50.6375	0.9979	0.9618	0.9935	0.4785
Dmey	51.2455	0.9978	0.9612	0.9940	0.4789
Coif5	50.8908	0.9978	0.9609	0.9945	0.4786
Bior3.5	48.8840	0.9983	0.9561	0.9944	0.4778
Rbior6.8	51.4411	0.9979	0.9577	0.9935	0.4776

Table 4.5: Robustness analysis for various attacks

Attack	**Noise density**	**NC 1**	**NC 2**
Salt and pepper noise	0.01	0.9990	0.9630
	0.08	0.9937	0.9558
Gaussian noise	0.01	0.9981	0.9626
	0.5	0.9830	0.9329
Rotation	10°	0.9989	0.9632
JPEG Compression	Q=90	0.9988	0.9632
Speckle noise	0.005	0.9987	0.9632
	0.01	0.9988	0.9632
Image scaling	×1.1	0.9986	0.9632
Cropping	[5 5 ,10 10]	0.9989	0.9632
Gaussian low- pass filter	Var=0.6	0.9989	0.9624
Median filter	[2 2]	0.9988	0.9632
Poisson noise		0.9988	0.9632
Histogram equalization		0.9988	0.9632

Table 4.6: Comparison of NC values with [117]

Attack	Noise density	[117]	NC by proposed scheme
Gaussian noise	mean= 0,Var-0.01 and 0.5	0.9604 and 0.6569	0.9626 and 0.9329
Salt & pepper noise	0.08	0.8859	0.9558
Histogram equalization		0.931	0.9632

Table 4.7: Comparison of robustness with [95]

Attack	Noise density	[95]	NC by proposed scheme
Gaussian noise	mean= 0,Var-0.01	0.9965	0.9981
Speckle noise	0.05	0.9948	0.9988
JPEG Compression	Quality factor =90	0.9951	0.9988
Salt & pepper noise	0.08	0.9905	0.9937
Median filter [2 2]		0.9950	0.9988
Histogram equalization		0.9902	0.9988

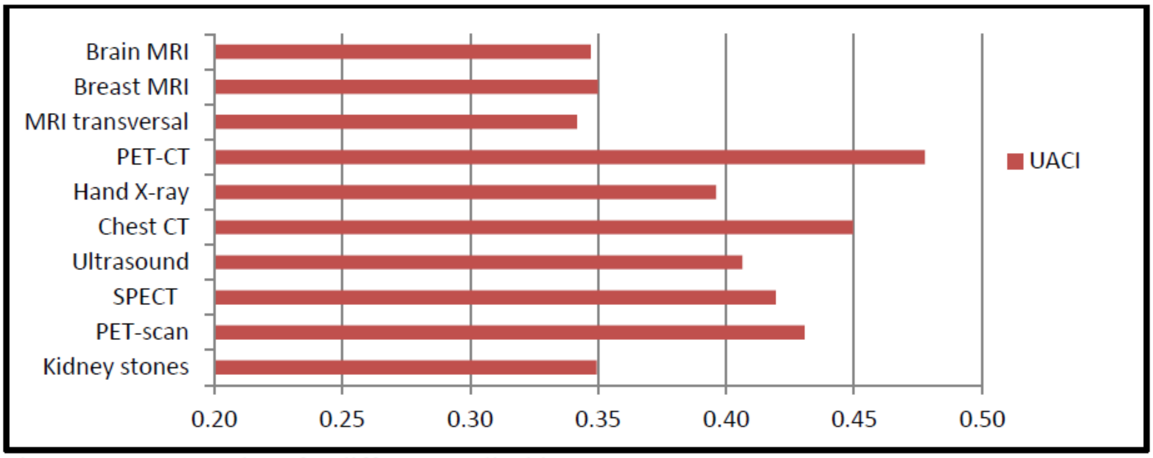


Figure 4.2: UACI values for different medical images

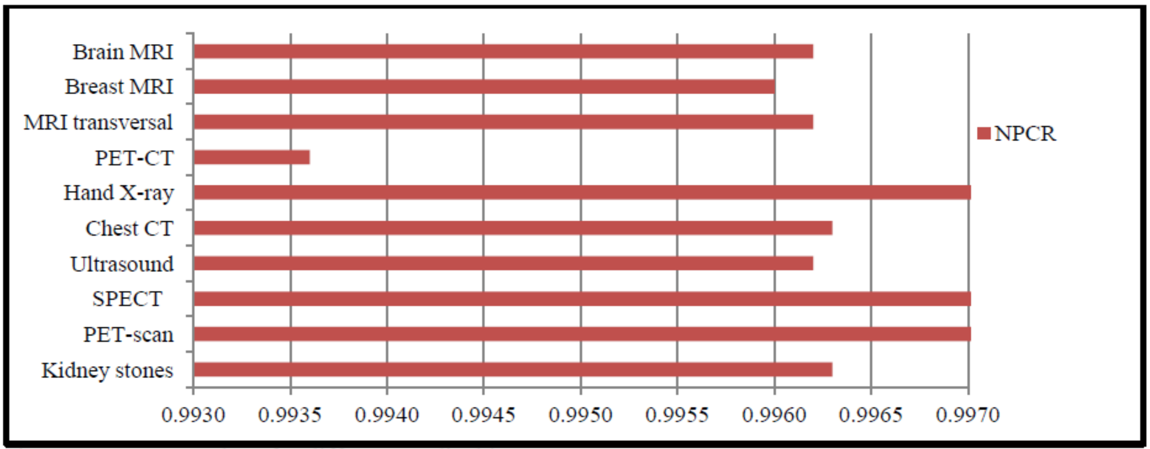


Figure 4.3: NPCR values for different medical images

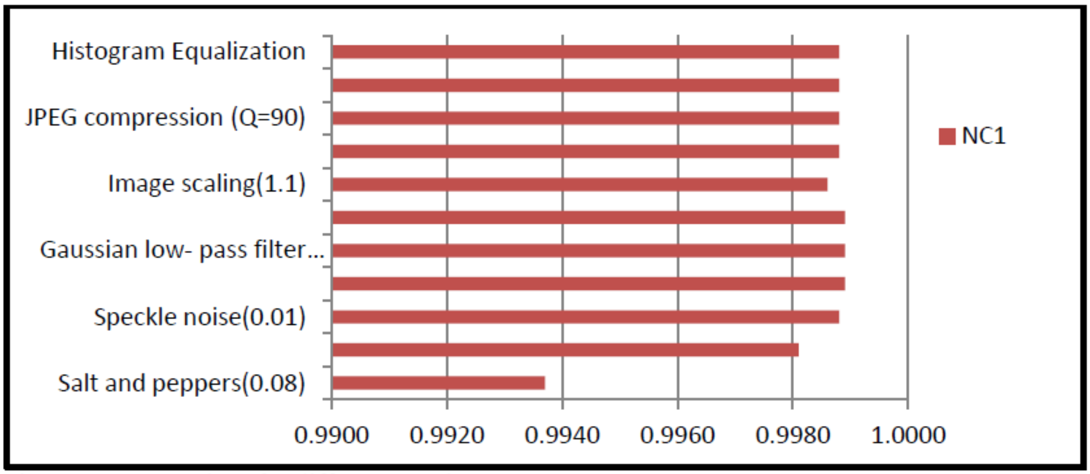


Figure 4.4:NC1 values for different attacks

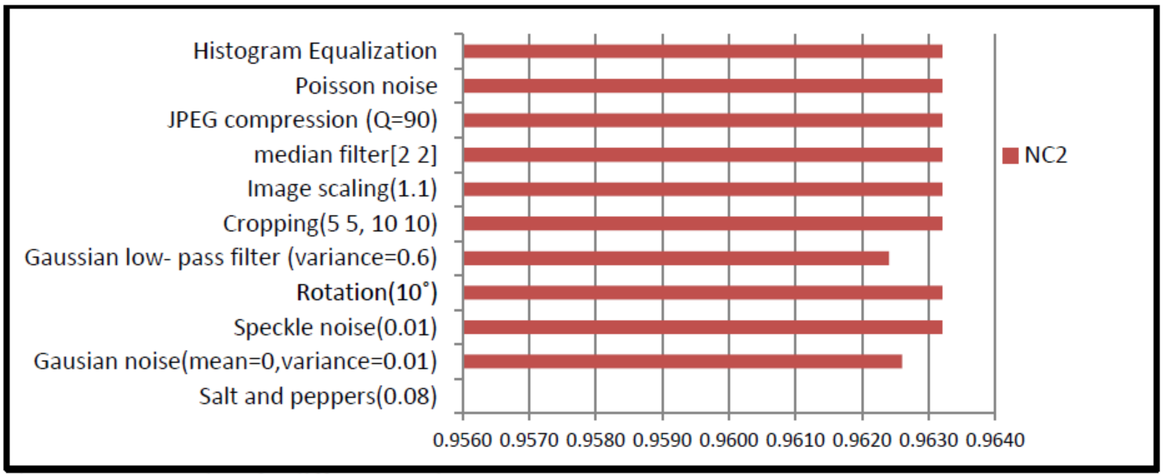


Figure 4.5: NC2 values for different attacks

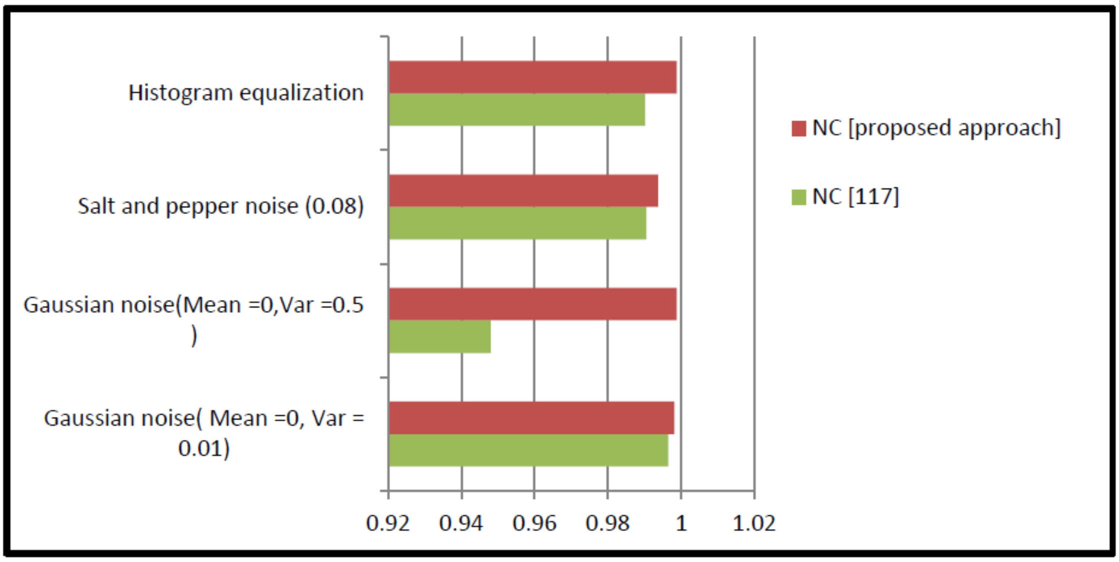


Figure 4.6: Comparative estimation through NC with [117]

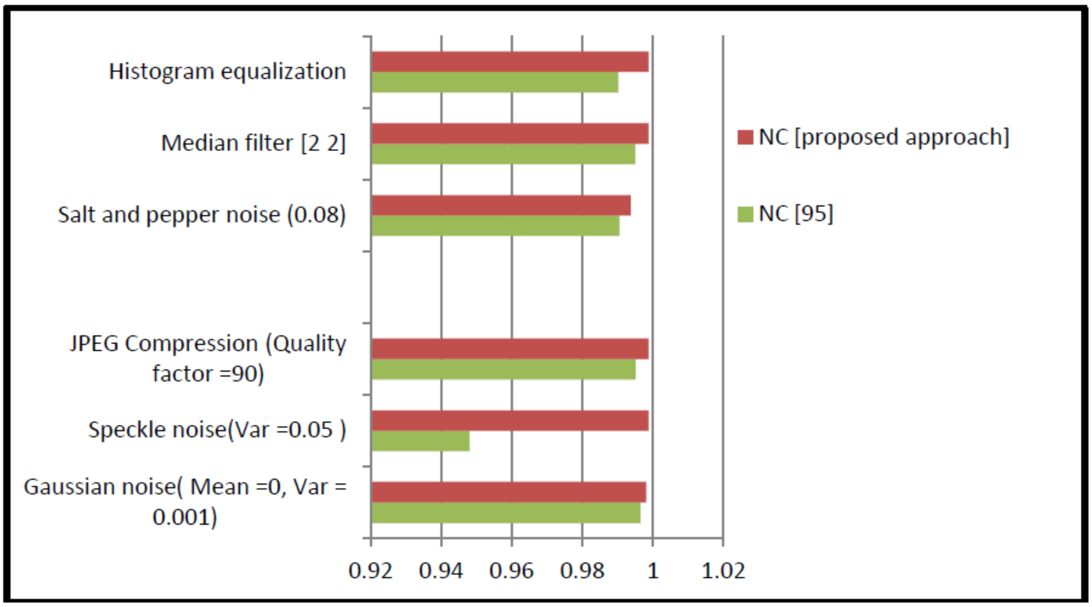


Figure 4.7: Comparative estimation through NC with [95]

This chapter provided a secure and robust watermarking at low cost. A robust and secure medical image watermarking is developed for embedding multi-watermarks (dual) in NSCT-RDWT and SVD domain. By applying low cost encryption scheme on watermarked image, the confidentiality of the technique is enhanced. The developed technique offer better robustness when compared to the other approaches. Our examination and results confirm that the technique is appropriate for data security using medical applications.

The work presented in this chapter has been published in Concurrency and Computation: Practice and Experience, pp. 1-10, doi: 10.1002/cpe.5108, Wiley indicated in list of publications at the end of the Chapter 6

CHAPTER 5

IMPROVED DWT- SVD BASED MEDICAL IMAGE WATERMARKING THROUGH HAMMING CODE, CHAOTIC ENCRYPTION AND SUBSTITUTION CIPHER

In this chapter, an improved DWT-SVD based approach for medical applications is developed. The method jointly uses hamming error correction code and chaotic encryption to provide robustness and security of the technique, respectively. Based on health data management policy, we have imperceptibly embedded more robust data at high DWT level and less robust data into the lower DWT level of the cover image. The result outcomes establish the merits of the suggested technique with respect to robustness, security and imperceptivity. The performance comparisons also confirmed that our technique is superior to existing techniques for various attacks. Further, the proposed technique is tested with rotation-13 encryption algorithm on encoded text watermark. We observed that the rotation-13 encryption based watermarking is performed better in terms of robustness than other technique.

5.1 Introduction

In tele-health services, various forms of medical images and patient report are transmitted between health centres or healthcare professionals [108]. Due to remarkable progress of ICT tools, this information is easily transmitted over the network. Initially, channel may contain noise and the transmitted information can be altered, deleted or modified by any professional hacker. Therefore, these tools are unreliable for information communication. Watermarking in medical domain is used to defend the patient related data [121-122]. In addition to providing security medical image watermarking also focuses on achieving the basic security requirements. Reliability, confidentiality and availability are the key security requirements [108]. How accurate and correct is the information received is determined by reliability. The privacy or secrecy of exchanged information is determined by confidentiality in which leakage to unintended users is prevented [109-110]. The uninterrupted and timely access of information is determined by availability.

Consequently, need of watermarking algorithms arises which take care of the basic security requirements effectively [109, 112]. Therefore to address these issues, watermarking algorithms incorporating cryptographic procedures are being developed by the researches. They not only enhance the security but also check the key security requirements.

Joint encryption- watermarking methods often employ complex cryptographic measures to provide all round security which increases the cost in terms of complexity [110, 121-122]. Researchers are creating encryption algorithms which not only provide significant security but also save computational time [121]. The related techniques are discussed in detail in Chapter 1 [32, 60, 43, 57, 26, 29, 37, 54, and 65].

A watermarking method using DWT and SVD is reported by the authors in [32]. The reported method placed ROI information into RONI section of cover. Comparison with related methods [33-36] show better performance in case of reported method. In the scenario of telemedicine DWT-SVD based watermarking approach is reported by the authors in [43]. The ROI section of host image is processed using DWT and SVD for embedding. The medical data is inserted into RONI after being encoded through ECC. The reported approach is extensively evaluated and performs better than similar schemes [44-45]. The authors in [60] reported a watermarking approach in the domain of DWT-SVD using two watermarks. Different kinds of error correcting codes are applied over the text watermark to test for robustness. The experimental assessment of the reported approach showed better results with respect to imperceptibility and robustness.

In this chapter, an error correcting code and encryption based multi-watermarking watermarking technique in frequency domain is developed. Key impact of the suggested technique is recognized as follows.

- It is evident that combination of DWT-SVD based watermarking technique performed better than the technique based on DWT or SVD individually [109-110].
- Multi-watermarks are placed inside the cover image which increases the security of the medical data. The sub-part of the image watermark is placed inside the cover which improves the imperceptibility performance as well.
- Hamming code is used to decrease the channel noise and improve the robustness of the text data.
- Cryptographic procedure governed by the principles of chaos [113] is used to further improve the overall security of our technique.
- Further, the method is tested with rotation-13 encryption algorithm [123] on encoded text watermark. It reduces the overall computational time of our technique.

The remaining chapter is structured as follows: introduction to this chapter is given in section 5.1. The suggested method is presented in section 5.2. The results outcomes are discussed in section 5.3.

5.2 Proposed procedure

The main aim is to propose a robust and secure watermarking at satisfactory quality of the marked image. In the process embedding, the method uses DWT to decompose the cover image. The selected component of DWT is transformed by SVD. The less robust watermark (image form) is divided into equal parts and each part is embedded into the two different components of the SVD cover image. However, more robust watermark is encoded by Hamming code and it is placed inside the second level DWT cover image. Finally, cryptographic procedure governed by the principles of chaos is used to encrypt the marked image prior to transmission over the network. This encryption process of the marked image further increases the validity of our technique. The second level DWT decomposition on image is shown in Fig 5.1. The complete process of the suggested technique is shown in Fig. 5.2 a-b.

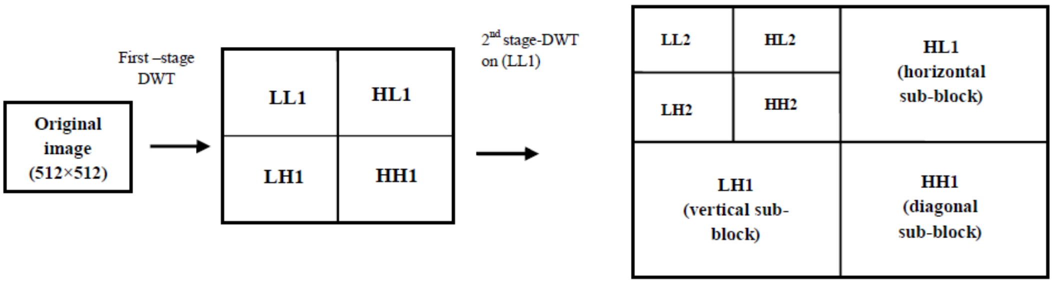


Figure 5.1: Second level DWT decomposition of an image

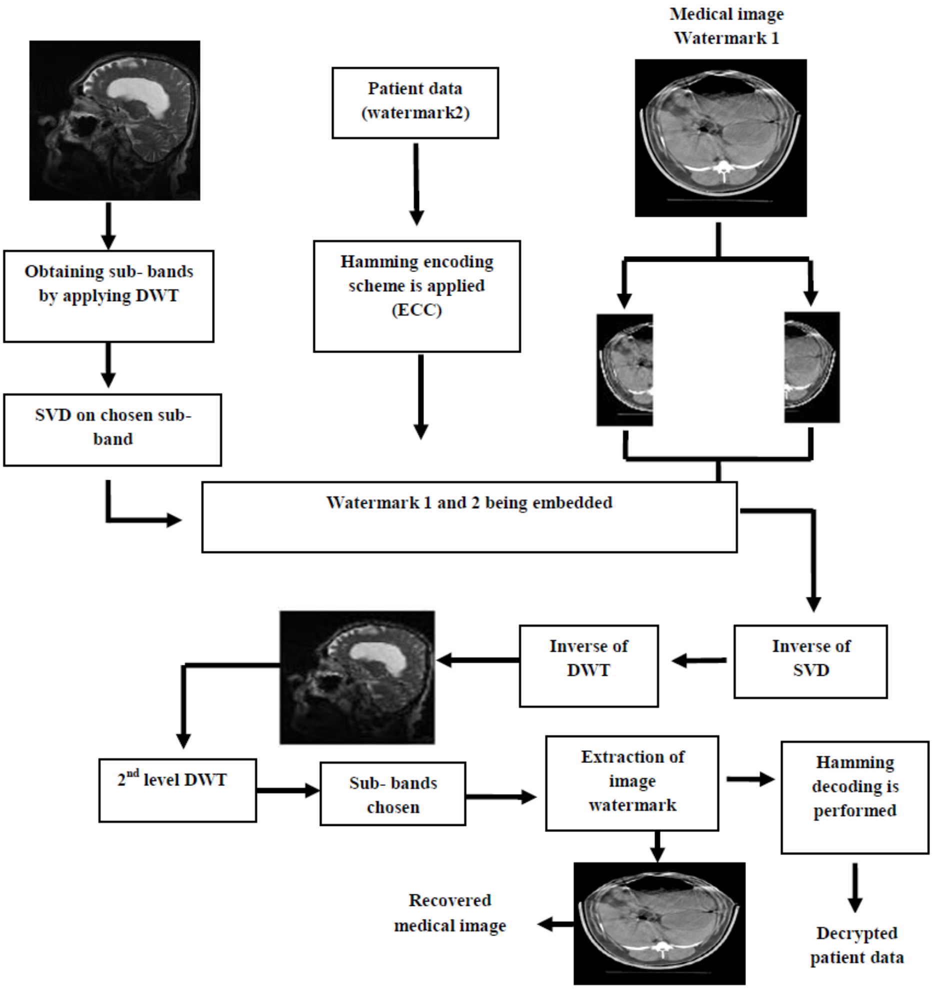

Medical image Watermark 1
Patient data (watermark2)
Obtaining sub- bands by applying DWT
Hamming encoding scheme is applied (ECC)
SVD on chosen sub-band
Watermark 1 and 2 being embedded
Inverse of DWT
Inverse of SVD
2nd level DWT
Sub- bands chosen
Extraction of image watermark
Hamming decoding is performed
Recovered medical image
Decrypted patient data

Figure 5.2: Schematic diagram for the proposed procedure

5.3 Experimental results and analysis

This section presents the outcome of the combined DWT-SVD-ECC with chaotic encryption. Subsequently, the performance of DWT-SVD-ECC with rotation-13 algorithm is introduced in separate sub-section. The experimental verification is performed using a 512 × 512 sized cover image, secret image of size 256 × 256 and a text watermark of 12 characters. Extensive assessment of our method has been done for chosen gain value, six medical [116] and four non-medical images [118] and different types of standard image processing attacks. Further, we have made a comparative analysis of our methods using chaotic encryption and Caesar cipher with the method proposed in [60] respectively.

The second method uses simple substitution cipher to encrypt the 12 character watermark only. The watermarked image is not encrypted in this version of our technique. After encoding the text watermark with hamming error correcting code, it further encrypted using rotation -13 algorithms [123]. Since in the second method the watermarked image is not encrypted, using a simple encryption scheme over the text information reduced the overall computational time of our technique. The major difference between the first and the second method lies in the encryption algorithm used to enhance the security. The first method use two dimensional logistic map based chaotic encryption [113] to encrypt the watermarked image. In the second method however, a simple substitution encryption technique [123] is used. This technique is performed over the EPR watermark and worked by replacing each alphabet of the text watermark with the thirteenth letter of its corresponding alphabet. Since it is applied over the text watermark it reduced time of the entire method.

5.3.1 Performance evaluation of chaotic encryption based technique

All the experiments were conducted using MATLAB (R2013a). The performance of the suggested chaotic encryption based technique is evaluated in terms of PSNR, NC, BER, NPCR and UACI [7, 9, and 23]. For the performance evaluation of our technique, six medical [116] and one non medical image [118] of size 512×512 has been used. Further the image watermark of size 256×5256 and EPR watermark of 96 bits has been used to evaluate the performance of our technique. The watermarks have been embedded according to health data management policy in which the less and more robust data is placed inside the lower and higher sub-bands respectively. Moreover, the performance comparison of the suggested technique with former technique [60] is also presented (see Table 5.4).

The standard metrics defined as PSNR [106], NC [106], BER [108], UACI and NPCR [115] are utilized to assess the performance of our technique. These metrics are extensively discussed in chapter 1.

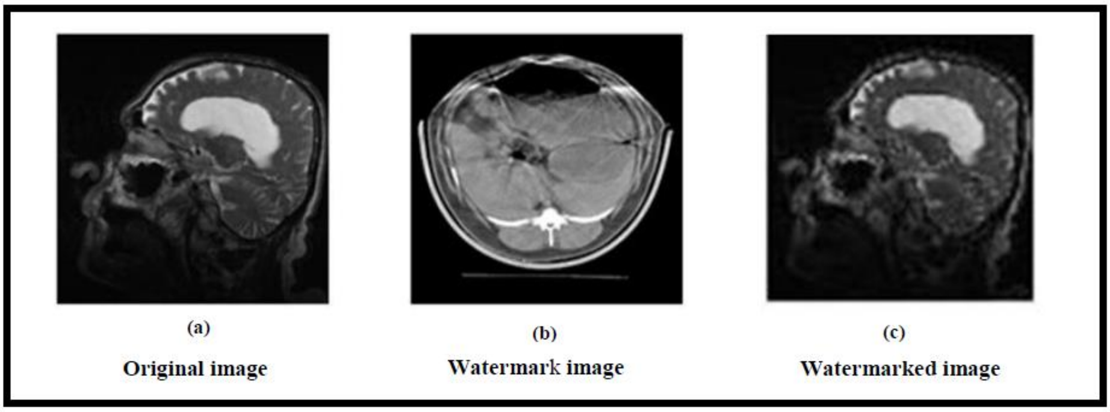
The performance evaluation of our method on the basis of standard metrics is depicted in table 5.1-table 5.4. Fig. 5.5 shows the performance comparison using NC values with [60].

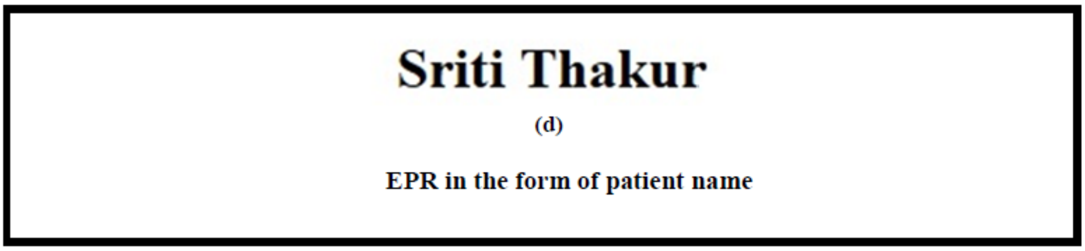
The metrics PSNR, NC, BER, NPCR and UACI of our technique at selected gain values for both the watermarks is presented in table 5.1. From this table, the best value of PSNR and NC is 38.35 dB and 0.9986 respectively. The BER value obtained for all gain values is 0. The PSNR and NC values are depends on the gain value. Further, NPCR and UACI values are just about reaching the permissible values [115].

These metrics are also realised for six medical and one non medical image at a gain value of 0.05 depicted in table 5.2. From table 5.2, the obtained PSNR and NC values are greater than 21 dB and 0.88 respectively. The BER value obtained in case of table 5.2 is 0. The NPCR and UACI values obtained for table 5.2 roughly reaching the acceptable limits [115] respectively.

The robustness of our technique is estimated using the metric NC and BER which is depicted in table 5.3. From table 5.3, it is clearly seen that the values obtained for NC is greater than 0.80 and the BER value is 0 for most attacks except for rotation attack.

Comparative evaluation of our method to related method [60] is depicted in table 5.4. From this table it is clearly observed that the NC and BER performance is better when compared with the method [60].





Sriti Thakur

(d)

EPR in the form of patient name

Figure 5.3: (a) cover object, (b) watermark image, (c) watermarked image and (d) patient name

Table 5.1: Performance outcomes for differing gain values

Gain factor	PSNR (dB)	NC (image)	BER (text)	NPCR	UACI
0.005	38.3571	0.9154	0	0.9961	0.4010
0.01	38.3538	0.9676	0	0.9960	0.4012
0.03	38.0954	0.9916	0	0.9960	0.4010
0.05	36.9234	0.9154	0	0.9961	0.4010
0.07	35.2507	0.9977	0	0.9961	0.4011
0.09	33.5399	0.9985	0	0.9960	0.4014
0.1	32.7280	0.9986	0	0.9958	0.4012

Table 5.2: Performance estimation for several cover objects

Cover media	PSNR (dB)	NC (image)	BER	NPCR	UACI
CT-scan	21.4548	0.8865	0	0.9961	0.4546
PET-CT	38.4215	0.9648	0	0.9960	0.4811
Ultrasound	24.5103	0.9327	0	0.9961	0.4132
PET-scan	28.0304	0.9488	0	0.99612	0.4480
Brain MRI	36.9234	0.9154	0	0.9961	0.4010
Hand X-ray	38.0842	0.9869	0	0.9961	0.4906
Barbara	36.4312	0.9793	0	0.9960	0.4206

Table 5.3: Robustness observations for both (image and text watermark) for attacks

Attack	Noise density	NC (image)	BER (text)
Salt and pepper noise	0.0001	0.9975	0
	0.0005	0.9630	0
	0.001	0.8761	0
Gaussian noise	0.0001	0.9785	0
	0.0005	0.8311	0
Rotation	1°	0.9308	55.95
	5°	0.8908	55.95
	10°	0.8913	0.55
JPEG Compression	QF = 10 and 50	0.8994 and 0.9626	0
Sharpening mask	0.1	0.8042	0
	0.5	0.8320	0
	0.9	0.8445	0
Speckle noise	0.001	0.9947	0
	0.01	0.8277	0
Image scaling	×1	0.9973	0
	×2	0.8242	0
Cropping	[5 5 ,10 10]	0.9800	7.1428
	[10 10 ,200 200]	0.9009	7.1428
Gaussian low- pass filter	Mean=1, Var=0.6	0.9973	0
	Mean=3, Var=0.6	0.9124	0
Median filter	[1 1]	0.9973	0
	[2 2]	0.9099	0
	[3 3]	0.9290	0
Poisson noise		0.8026	0
Histogram equalization		0.6624	2.38

Table 5.4: Comparative analysis of our method with [60]

Attack	Noise density	NC and BER by [60]		NC and BER [proposed scheme]	
		NC	BER	NC	BER
JPEG compression	QF = 100	0.9950	0	0.9974	0
Sharpening mask	0.1, 0.5 &0.9	0.5986, 0.6293 & 0.6457	0	0.80422, 0.8320 & 0.8445	0
Gaussian noise	0.05	0.3150	8.5714	0.4157	1.190
Image scaling	2 & 2.5				
Salt & pepper noise	0.001	0.7553	0	0.8765	0
Median filter	[3 3]	0.8885	0	0.9290	0
Gaussian low-pass filter	0.6	0.8780	0	0.9124	0
Cropping		0.7451	4.5714	0.9800	7.1428
Histogram equalization		0.5880	1.4286	0.6624	2.3809

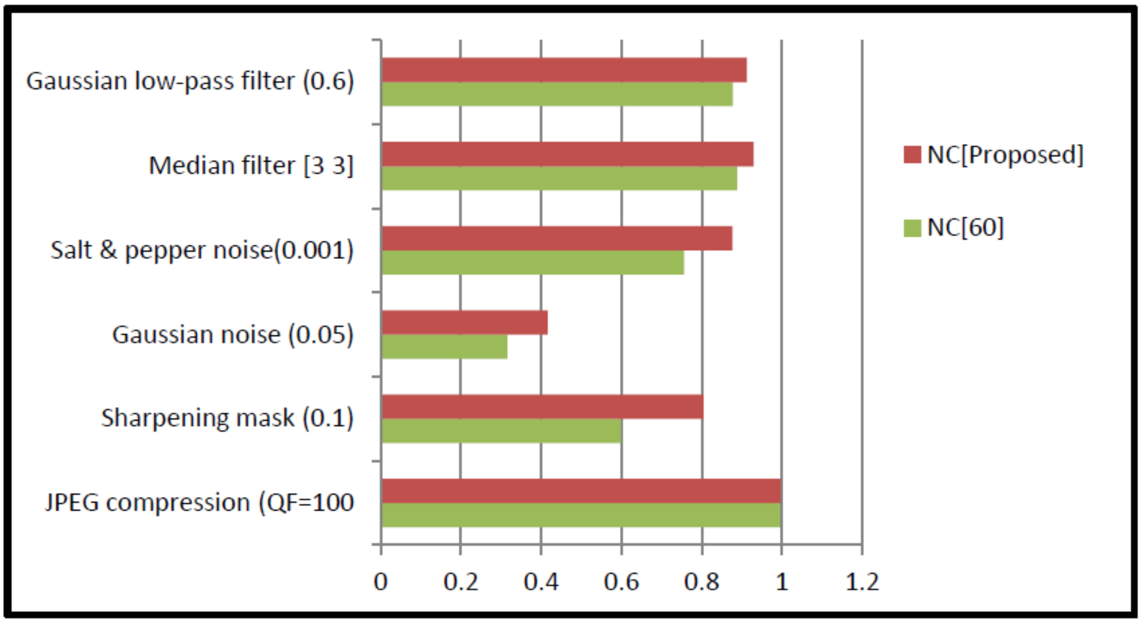


Figure 5.5: comparative estimation through NC with [60]

5.3.2 Proposed technique based on rotation-13 encryption

This technique is similar to the approach given in section 5.2 with a slight difference in the way of encryption is performed. The second method uses a simple Caesar cipher / substitution scheme [123] known as the rotation -13 technique to encrypt the text watermark. Instead of encrypting the entire watermarked information, the EPR watermark is only encrypted. This facilitates in faster implementation of proposed technique since chaotic encryption is heavier computationally.

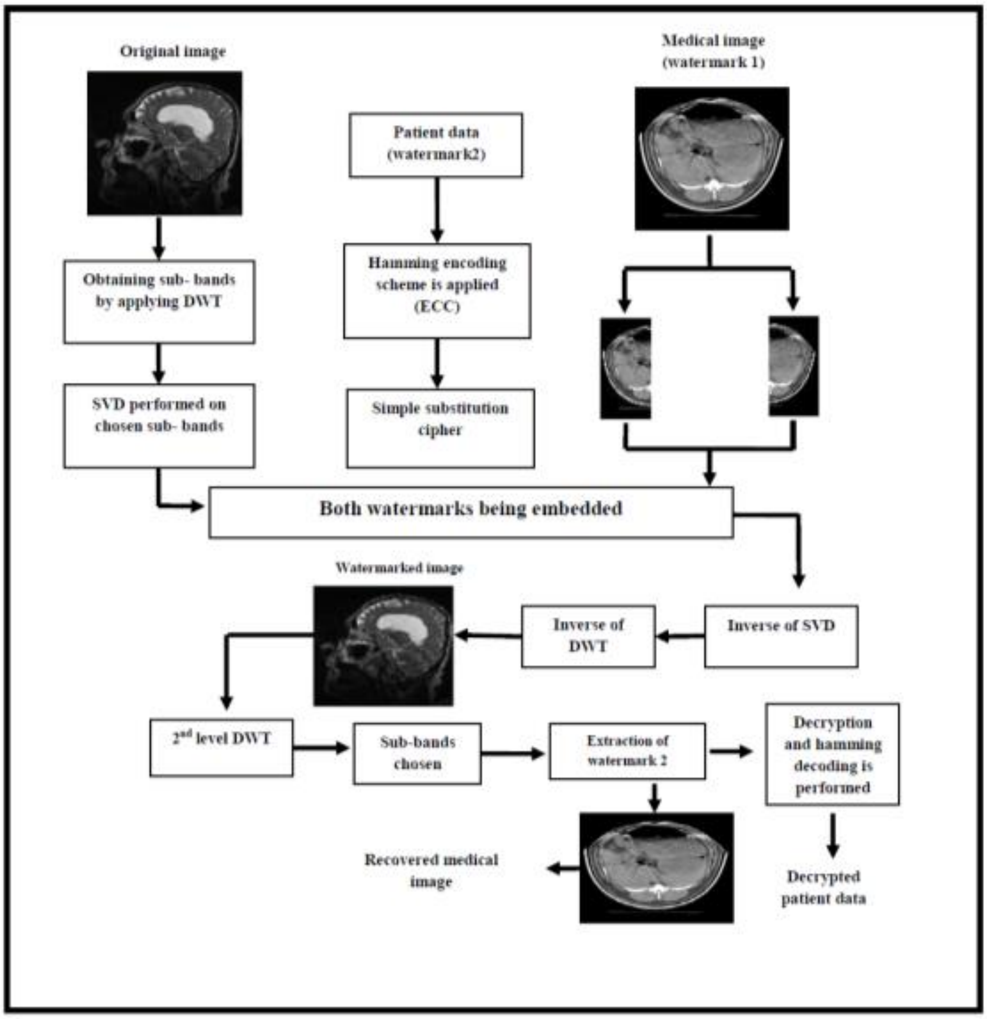

Original image
Medical image (watermark 1)
Patient data (watermark2)
Obtaining sub- bands by applying DWT
Hamming encoding scheme is applied (ECC)
SVD performed on chosen sub- bands
Simple substitution cipher
Both watermarks being embedded
Watermarked image
Inverse of DWT
Inverse of SVD
2nd level DWT
Sub-bands chosen
Extraction of watermark 2
Decryption and hamming decoding is performed
Recovered medical image
Decrypted patient data

Figure 5.4: flow diagram when Caesar cipher to text watermark is applied

The host image is altered using two-level DWT and sub bands are determined for the embedding process. SVD is applied to selected sub bands to obtain singular vectors. The patient image watermark is divided into two equal portions and inserted into DWT- SVD decomposed image. The EPR data is encoded and encrypted using hamming code and rotation-13 scheme respectively. The encrypted data is embedded into (High-High (HH2)) singular sub components. At the receiver side, decryption, hamming decoding and extraction procedure is performed to recover the 'patient medical image' and EPR data respectively. The proposed technique using the substitution cipher for EPR watermark is depicted in fig.5.4.

5.3.2 Performance evaluation of substitution encryption based technique

All experiments were implemented on MATLAB (R2013a). The performance of the proposed Caesar/ substitution encryption based technique is estimated using PSNR, NC, BER, NPCR and UACI [7, 9, and 23]. In order to estimate the performance of our technique, six medical [116] and four non medical images [118] of size 512×512 is used. Further the 'patient data' image watermark of size 256×256 and EPR watermark of 96 bits has been used to evaluate the performance of our technique. In addition to this, performance comparison is also determined of our method with similar technique [60].

The general metrics such as PSNR [106], NC [108], BER [108], UACI and NPCR [115] are used to analyze the performance of our technique. These metrics are extensively discussed in chapter 1.

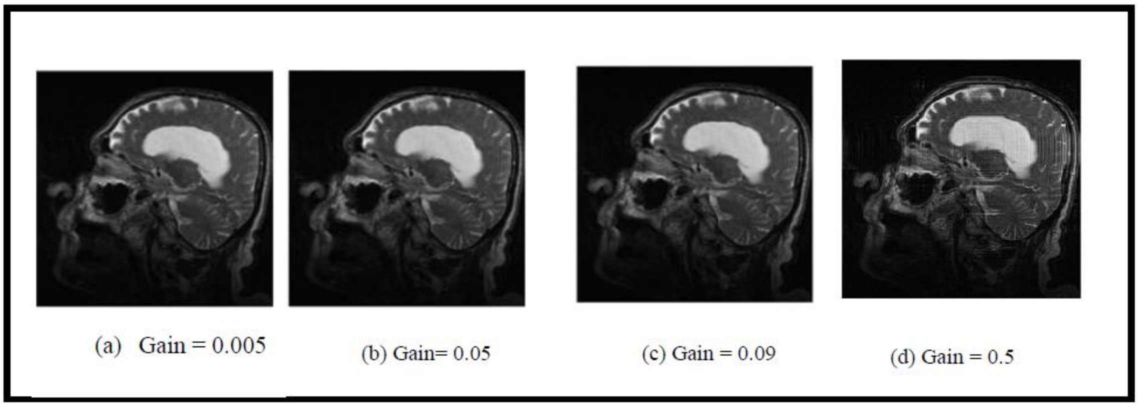
The performance estimation of our method utilizing the standard metrics is depicted in table 5.7-table 5.9. Fig. 5.7 shows the performance comparison using NC values with [60].

The metrics PSNR, NC, BER, NPCR and UACI of our technique at specific gain values for the two watermarks is shown in table 5.7. From this table, it is seen that the best value of PSNR and NC is 38.57 dB and 0.9963 respectively. The BER value is 0 for all gain values. It is noticed that the PSNR and NC performance depends majorly on the gain value. Further, NPCR and UACI values are reaching the permissible values [115] approximately.

These metrics are also realised for six medical and of our non medical image at a fixed gain value of 0.05 shown in table 5.2. From table 5.8, the achieved PSNR and NC values are greater than 20 dB and 0.85 respectively. The BER value for table 5.8 achieved is 0. The NPCR and UACI values for table 5.8 are reaching the acceptable limits roughly [115] respectively.

The metrics NC and BER are used determine the robustness of our technique depicted in table 5.9. From table 5.9, it noticed that the NC value for most attacks is greater than 0.80 except for histogram equalization. The BER value is zero for most attacks except for few attacks.

Comparative assessment of our method to similar method [60] is shown in table 5.10. From this table it is noticed that the NC and BER performance is better when compared with the method [60].



(a) Gain = 0.005 (b) Gain= 0.05 (c) Gain = 0.09 (d) Gain = 0.5

Figure.5.6: watermarked images at different gain factor values

Table 5.7: Performance assessment at selected gain

Gain factor	PSNR (in dB)	NC (image)	BER (text)
0.005	38.3572	0.8300	0
0.01	38.3538	0.9228	0
0.03	38.0954	0.9781	0
0.05	36.9234	0.9911	0
0.07	35.2507	0.9935	0
0.09	33.5400	0.9959	0
0.1	34.6957	0.9963	0

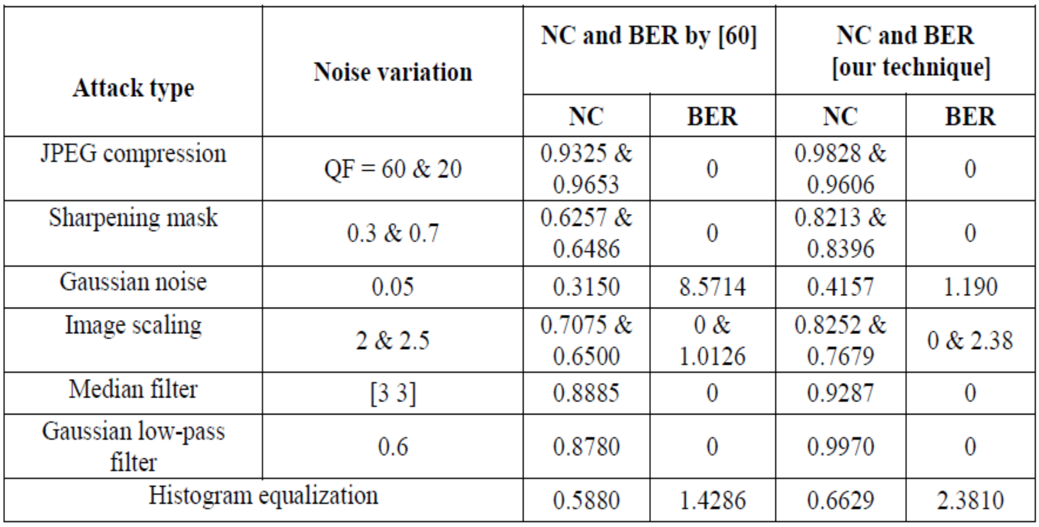
Table 5.8: Performance assessment for a range of cover images

Cover media	**PSNR (in dB)**	**NC (image)**	**BER (text)**
CT-scan	21.4548	0.8960	0
PET-CT	38.4216	0.9610	13.09
Ultrasound	24.5104	0.9318	0
PET-scan	28.0304	0.9479	0
Brain MRI	36.9234	0.9911	0
Hand X-ray	38.0842	0.9869	0
Barbara	29.1970	0.9952	0
Boat	32.0078	0.9887	0
Lena	36.4533	0.9724	0
Cameraman	20.2734	0.8585	0

Table 5.9: Robustness assessment for image and text watermark(s) under attacks

Attack	Noise variation	NC (image)	BER (text)
Salt and pepper noise	0.0001	0.9974	0
	0.0005	0.9657	0
	0.001	0.8942	0
Gaussian noise	0.0001	0.9788	0
	0.0005	0.8337	0
Rotation	1°	0.9326	53.57
	5°	0.8933	55.95
	10°	0.8908	57.14
JPEG Compression	QF = 10 and 50	0.8950 and 0.9640	0
Sharpening mask	0.1	0.8056	0
	0.5	0.8323	0
	0.9	0.8446	0
Speckle noise	0.001	0.9946	0
	0.01	0.8343	0
Image scaling	×1	0.9970	0
	×1.5	0.9094	0
	×2	0.8252	0
Cropping	[5 5 ,10 10]	0.8994	10.71
	[20 20 ,50 50]	0.8994	10.71
Gaussian low- pass filter	Mean=1, Var=0.6	0.9970	0
	Mean=4, Var=0.2	0.8950	0
Median filter	[1 1]	0.9970	0
	[2 2]	0.9114	0
	[3 3]	0.9287	0
Poisson noise		0.8056	0
Histogram equalization		0.6629	2.38

Table 5.10: comparative study of second method with [60]



Attack type	Noise variation	NC and BER by [60]		NC and BER [our technique]	
		NC	BER	NC	BER
JPEG compression	QF = 60 & 20	0.9325 & 0.9653	0	0.9828 & 0.9606	0
Sharpening mask	0.3 & 0.7	0.6257 & 0.6486	0	0.8213 & 0.8396	0
Gaussian noise	0.05	0.3150	8.5714	0.4157	1.190
Image scaling	2 & 2.5	0.7075 & 0.6500	0 & 1.0126	0.8252 & 0.7679	0 & 2.38
Median filter	[3 3]	0.8885	0	0.9287	0
Gaussian low-pass filter	0.6	0.8780	0	0.9970	0
Histogram equalization		0.5880	1.4286	0.6629	2.3810

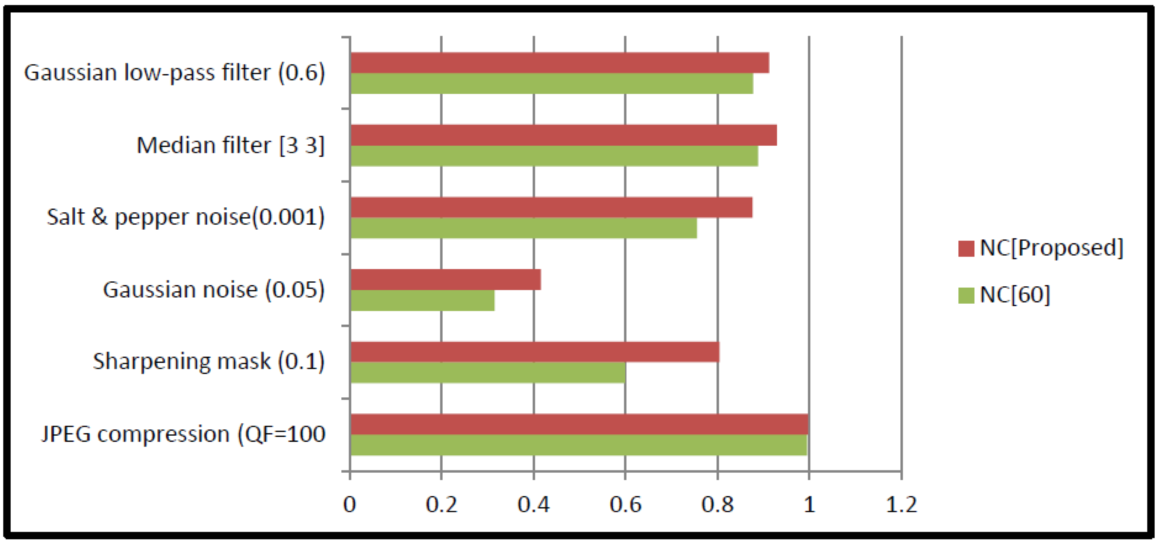
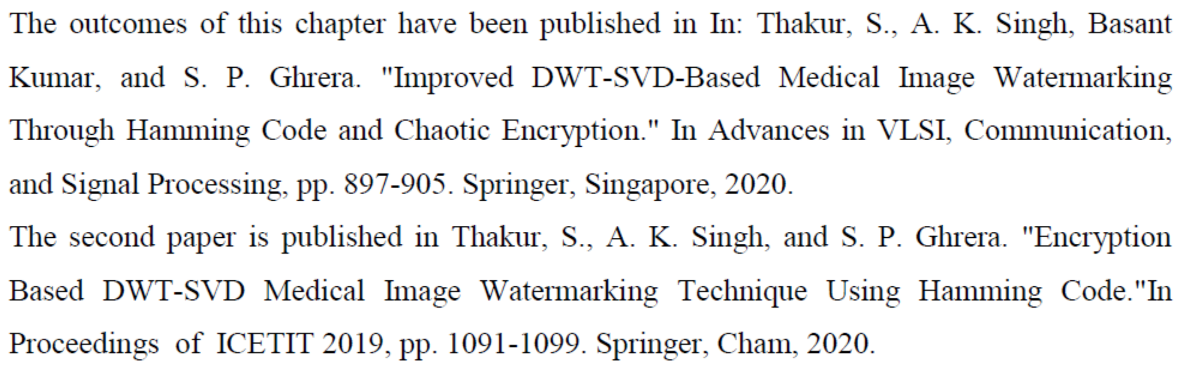


Figure 5.7: comparative estimation through NC with [60]

Due to significant importance of dual watermarking along with encryption and error correction code in medical domain, an improved DWT-SVD based watermarking using hamming code and chaotic encryption is developed.The result outcomes establish the merits of the proposed technique in terms of robustness, security and imperceptivity. The robustness comparisons also confirmed that our technique is superior to existing techniques for various attacks. Further, the proposed technique is tested with rotation-13 encryption algorithm on encoded text watermark. We observed that the rotation-13 encryption based is performed better than former technique.



The outcomes of this chapter have been published in In: Thakur, S., A. K. Singh, Basant Kumar, and S. P. Ghrera. "Improved DWT-SVD-Based Medical Image Watermarking Through Hamming Code and Chaotic Encryption." In Advances in VLSI, Communication, and Signal Processing, pp. 897-905. Springer, Singapore, 2020.

The second paper is published in Thakur, S., A. K. Singh, and S. P. Ghrera. "Encryption Based DWT-SVD Medical Image Watermarking Technique Using Hamming Code."In Proceedings of ICETIT 2019, pp. 1091-1099. Springer, Cham, 2020.

This is indicated under the list of publication at the end of the Chapter 6.

CHAPTER 6

CONCLUSION AND FUTURE DIRECTIONS

Motivated by medical information security issues in the area of e-healthcare, the aim of this research work was to develop improved robust and secure image watermarking technique that offer optimum trade-off between robustness, imperceptibility, capacity and security at low cost.

In this research, we have developed some improved secure and robust medical image watermarking technique in wavelet domain. Chapter 1 presents the basic concept of digital watermarking, novel characteristics of digital watermark, potential applications, important spatial and transform domain techniques, vital performance metrics, and major watermarking attacks. This is followed by literature review of various reported medical image watermarking techniques along with performance comparison in tabular format. The transform domain and chaotic encryption based secure watermarking for e-healthcare is proposed in Chapter 2. The method uses fusion of DWT, DCT and SVD to imperceptibly embed patient report/identity in to host medical image. Further, chaos based encryption technique is used to provide confidentiality of the patient medical data. Effectiveness and importance of the method is validated through both subjective and objective methods. The method is extensively evaluated for varying gain factor, several medical and non-medical cover images, encryption–decryption time and popular image processing attacks. It is important to see that the suggested scheme is robust and secure for different attacks and found improved performance in terms of NC value than other approaches [45] and [107]. Further, the maximum PSNR, NC and SSIM values are obtained as 74.6099 dB, 0.9991and1.0000, respectively. Moreover, it is determined that NPCR and UACI values mostly satisfy the permissible range. However the percentage improvement in terms of NC for JPEG compression (25) is 0.27%.

In chapter 3, a robust and secure technique is developed for embedding multi-watermarks (dual) in NSCT- RDWT and SVD domain. By applying chaos based encryption on watermarked image, the security of the proposed technique is improved.

We have extensively examined the performance at varying gain factor, nine medical and five non-medical image modalities, five wavelet filters and several image processing attacks. The maximum PSNR, ‘NC1’ and ‘NC2’ values are obtained as 54.4978dB, 0.9993 and 0.9637 respectively. Moreover, it is determined that NPCR and UACI values are mostly within the acceptable range. The developed technique offer better robustness when compared to the other approaches [95] and [102].

Our examination and results confirm that the technique is appropriate data security for medical application. However the percentage improvement in terms of NC for salt and pepper noise (0.08) is 7.31%.

A secure medical image watermarking approach using low-complexity cryptographic mechanism is developed in Chapter 4. The idea is same as our previous technique (dual watermarking approach in NSCT domain as discussed in Chapter 3); however, this cryptographic mechanism uses Fiestel network and substitution-permutation network to provide security at low cost. We have extensively evaluated our method for different gain value, ten medical and five non-medical cover images with different size of watermarks, six wavelet filters and different signal processing attacks. The maximum PSNR, 'NC1' and 'NC2' values are obtained as 54.4978dB, 0.9994 and 0.9633 respectively. Further, the NPCR and UACI values are well within the acceptable range. It is important to see that the suggested technique is robust and secure for different attacks and found improved performance in terms of NC value than other approaches [117] and [95]. However the percentage improvement in terms of NC for histogram equalisation is 3.34%.

In chapter 5, an improved DWT-SVD based approach for medical applications is developed. The method jointly uses hamming error correction code and chaotic encryption to provide robustness and security of the technique, respectively. Based on health data management policy, we have imperceptibly embedded more robust data at high DWT level and less robust data into the low DWT level of the cover image. It is important to see that maximum PSNR and NC values are obtained as 38.3572 dB and 0.9986 respectively. Further, the BER is 0 at all gain values and the NPCR and UACI values are well within the acceptable range. The robustness comparisons also confirmed that our technique is superior to existing techniques [60] for various attacks. However the percentage improvement in terms of NC for median filter [3, 3] is 4.35%.

Further, the proposed technique is tested with rotation-13 encryption algorithm on encoded text watermark. Extensive assessment of our method has been done for chosen gain value, six medical and four general images and different types of standard image processing attacks. We observed that the rotation-13 encryption based offered superior performance to former approach [60].

Therefore, our methods are suitable for medical applications and providing a valued result for the avoidance of medical related identity theft. In future, we will try 1) to develop more secure algorithm for medical as well as other emerging applications, 2) to develop efficient watermarking approaches with recent technologies, and 3) to test our methods for other multimedia applications.

REFERENCES

[1] Singh, Amit Kumar, Basant Kumar, Ghanshyam Singh, and Anand Mohan, eds. Medical image watermarking: techniques and applications. Springer, 2017.

[2] Chauhan, Digvijay Singh, Amit Kumar Singh, Basant Kumar, and J. P. Saini. "Quantization based multiple medical information watermarking for secure e-health." Multimedia tools and applications 78, no. 4 (2019): 3911-3923.

[3] Giakoumaki, Aggeliki, KonstantinosPerakis, AnastassiosTagaris, and DimitrisKoutsouris. "Digital watermarking in telemedicine applications-towards enhanced data security and accessibility." In 2006 International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 6328-6331. IEEE, 2006.

[4] Chao, Hui-Mei, Chin-Ming Hsu, and Shaou-Gang Miaou. "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records." IEEE Transactions on Information Technology in Biomedicine 6, no. 1 (2002): 46-53.

[5] Giakoumaki, Aggeliki, Sotiris Pavlopoulos, and DimitrisKoutsouris. "Multiple image watermarking applied to health information management." IEEE Transactions on Information Technology in Biomedicine 10, no. 4 (2006): 722-732.

[6] Mohanty, Saraju P., AnirbanSengupta, ParthasarathyGuturu, and Elias Kougianos. "Everything You Want to Know About Watermarking: From Paper Marks to Hardware Protection: From paper marks to hardware protection." IEEE Consumer Electronics Magazine 6, no. 3 (2017): 83-91.

[7] Singh, Amit Kumar, Basant Kumar, Sanjay Kumar Singh, S. P. Ghrera, and Anand Mohan. "Multiple watermarking technique for securing online social network contents using back propagation neural network." Future Generation Computer Systems 86 (2018): 926-939.

[8] Singh, Amit Kumar, Basant Kumar, Mayank Dave, Satya Prakash Ghrera, and Anand Mohan. "Digital image watermarking: techniques and emerging applications." In Handbook of research on modern cryptographic solutions for computer and cyber security, pp. 246-272. IGI Global, 2016.

[9] Singh, Amit Kumar, Mayank Dave, and Anand Mohan. "Wavelet based image watermarking: futuristic concepts in information security." Proceedings of the National Academy of Sciences, India Section A: Physical Sciences 84, no. 3 (2014): 345-359.

[10] Mohanty, Saraju P. Nanoelectronic mixed-signal system design. No. 0071825711. New York: McGraw-Hill Education, 2015.

[11] Petitcolas, Fabien AP, and Stefan Katzenbeisser. Information Hiding Techniques for Steganography and Digital Watermarking (Artech House Computer Security Series). Artech House, 2000.

[12] Boato, Giulia, Valentina Conotter, and Francesco GB De Natale. "GA-based robustness evaluation method for digital image watermarking." In International Workshop on Digital Watermarking, pp. 294-307. Springer, Berlin, Heidelberg, 2007.

[13] Singh, Amit Kumar, ZhihanLv, Huimin Lu, and Xiaojun Chang. "Guest editorial: Recent trends in multimedia data-hiding: a reliable mean for secure communications." (2019): 1-3.

[14] Hore, Alain, and DjemelZiou. "Image quality metrics: PSNR vs. SSIM." In 2010 20th International Conference on Pattern Recognition, pp. 2366-2369. IEEE, 2010.

[15] Nyeem, Hussain, Wageeh Boles, and Colin Boyd. "Digital image watermarking: its formal model, fundamental properties and possible attacks." EURASIP Journal on Advances in Signal Processing 2014, no. 1 (2014): 135.

[16] Voloshynovskiy, Sviatolsav, Shelby Pereira, Thierry Pun, Joachim J. Eggers, and Jonathan K. Su. "Attacks on digital watermarks: classification, estimation based attacks, and benchmarks." IEEE communications Magazine 39, no. 8 (2001): 118-126.

[17] Mohanty, Saraju P. "Digital watermarking: A tutorial review." URL: http://www. csee. usf. edu/~ smohanty/research/Reports/WMSurvey1999Mohanty. pdf (1999).

[18] Ustubioglu, Arda, and GuzinUlutas. "A new medical image watermarking technique with finer tamper localization." Journal of digital imaging 30, no. 6 (2017): 665-680.

[19] Kulkarni, Madhuri B., and Ramesh T. Patil. "Tamper Detection & Recovery in medical image with secure data hiding using reversible watermarking." International Journal of Emerging Technology and Advanced Engineering 2, no. 3 (2012): 370-373.

[20] Das, Sudeb, and Malay Kumar Kundu. "Effective management of medical information through ROI-lossless fragile image watermarking technique." Computer methods and programs in biomedicine 111, no. 3 (2013): 662-675.

[21] Liew, Siau-Chuin, Siau-Way Liew, and JasniMohd Zain. "Tamper localization and lossless recovery watermarking scheme with ROI segmentation and multilevel authentication." Journal of digital imaging 26, no. 2 (2013): 316-325.

[22] Woo, Chaw-Seng, Jiang Du, and Binh L. Pham. "Multiple watermark method for privacy control and tamper detection in medical images." (2005): 59-64.

[23] Thabit, Rasha, and Bee EeKhoo. "Medical image authentication using SLT and IWT schemes." Multimedia Tools and Applications 1, no. 76 (2015): 309-332.

[24] Eswaraiah, Rayachoti, and EdaraSreenivasa Reddy. "Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest." IET image Processing 9, no. 8 (2015): 615-625.

[25] Parah, Shabir A., FarhanaAhad, Javaid A. Sheikh, and GhulamMohiuddinBhat. "Hiding clinical information in medical images: a new high capacity and reversible data hiding technique." Journal of biomedical informatics 66 (2017): 214-230.

[26] Sharifara, Ali, and Amir Ghaderi. "Medical Image Watermarking using 2D-DWT with Enhanced security and capacity." arXiv preprint arXiv: 1703.05778 (2017).

[27] Shih, Frank Y., XinZhong, I-Cheng Chang, and Shin'ichi Satoh. "An adjustable-purpose image watermarking technique by particle swarm optimization." Multimedia Tools and Applications 77, no. 2 (2018): 1623-1642.

[28] Gao, Guangyong, Xiangdong Wan, Shimao Yao, Zongmin Cui, Caixue Zhou, and Xingming Sun. "Reversible data hiding with contrast enhancement and tamper localization for medical images." Information Sciences 385 (2017): 250-265.

[29] Trivedy, Saswati, and Arup Kumar Pal. "A logistic map-based fragile watermarking scheme of digital images with tamper detection." Iranian Journal of Science and Technology, Transactions of Electrical Engineering 41, no. 2 (2017): 103-113.

[30] Chang, Chin-Chen, Kuo-Nan Chen, Chin-Feng Lee, and Li-Jen Liu. "A secure fragile watermarking scheme based on chaos-and-hamming code." Journal of Systems and Software 84, no. 9 (2011): 1462-1470.

[31] Hsu, Ching-Sheng, and Shu-Fen Tu. "Probability-based tampering detection scheme for digital images." Optics Communications 283, no. 9 (2010): 1737-1743.

[32] Bakthula, Rajitha, ShivendraShivani, and Suneeta Agarwal. "Self authenticating medical X-ray images for telemedicine applications." Multimedia Tools and Applications 77, no. 7 (2018): 8375-8392.

[33] Tan, Chun Kiat, Jason Changwei Ng, XiaotianXu, Chueh Loo Poh, Yong Liang Guan, and Kenneth Sheah. "Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability." Journal of Digital Imaging 24, no. 3 (2011): 528-540.

[34] Eswaraiah, Rayachoti, and E. Sreenivasa Reddy. "Medical image watermarking technique for accurate tamper detection in ROI and exact recovery of ROI." International journal of telemedicine and applications 2014 (2014): 13.

[35] Memon, Nisar Ahmed, Asmatullah Chaudhry, Mushtaq Ahmad, and Zulfiqar Ali Keerio. "Hybrid watermarking of medical images for ROI authentication and recovery." International Journal of Computer Mathematics 88, no. 10 (2011): 2057-2071.

[36] Wu, Jeffery HK, Ruey-Feng Chang, Chii-Jen Chen, Ching-Lin Wang, Ta-HsunKuo, Woo Kyung Moon, and Dar-Ren Chen. "Tamper detection and recovery for medical images using near-lossless information hiding technique." Journal of Digital Imaging 21, no. 1 (2008): 59-76.

[37] Khor, Hui Liang, Siau-ChuinLiew, and JasniMohd Zain. "Region of interest-based tamper detection and lossless recovery watermarking scheme (ROI-DR) on ultrasound medical images." Journal of digital imaging 30, no. 3 (2017): 328-349.

[38] Liew, SiewChuin. "Tamper Localization and recovery watermarking schemes for medical images in PACS." PhD diss., UMP, 2011.

[39] Lei, Baiying, Xin Zhao, Haijun Lei, Dong Ni, Siping Chen, Feng Zhou, and Tianfu Wang. "Multipurpose watermarking scheme via intelligent method and chaotic map." Multimedia Tools and Applications 78, no. 19 (2019): 27085-27107.

[40] Seo, Hyeon-Uk, Qun Wei, Seong-Geun Kwon, and Kyu-IkSohng. "Medical image watermarking using bit threshold map based on just noticeable distortion in discrete cosine transform." Technology and Health Care 25, no. S1 (2017): 367-375.

[41] Chou, Chun-Hsien, and Yun-Chin Li. "A perceptually tuned subband image coder based on the measure of just-noticeable-distortion profile." IEEE Transactions on circuits and systems for video technology 5, no. 6 (1995): 467-476.

[42] Liu, Jiang-Lung, Der-Chyuan Lou, Ming-Chang Chang, and Hao-Kuan Tso. "A robust watermarking scheme using self-reference image." Computer Standards & Interfaces 28, no. 3 (2006): 356-367.

[43] Thakkar, Falgun N., and Vinay Kumar Srivastava. "A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications." Multimedia Tools and Applications 76, no. 3 (2017): 3669-3697.

[44] Parah, Shabir A., Javaid A. Sheikh, FarhanaAhad, Nazir A. Loan, and GhulamMohiuddinBhat. "Information hiding in medical images: a robust medical image watermarking system for E-healthcare." Multimedia Tools and Applications 76, no. 8 (2017): 10599-10633.

[45] Singh, Amit Kumar, Basant Kumar, Mayank Dave, and Anand Mohan. "Multiple watermarking on medical images using selective discrete wavelet transform

coefficients." Journal of Medical Imaging and Health Informatics 5, no. 3 (2015): 607-614.

[46] Pandey, Richa, Amit Kumar Singh, Basant Kumar, and Anand Mohan. "Iris based secure NROI multiple eye image watermarking for teleophthalmology." Multimedia Tools and Applications 75, no. 22 (2016): 14381-14397.

[47] Arsalan, Muhammad, Aqsa Saeed Qureshi, Asifullah Khan, and MuttukrishnanRajarajan. "Protection of medical images and patient related information in healthcare: Using an intelligent and reversible watermarking technique." Applied Soft Computing 51 (2017): 168-179.

[48] Xuan, Guorong, Chengyun Yang, Yizhan Zhen, Yun Q. Shi, and Zhicheng Ni. "Reversible data hiding using integer wavelet transform and companding technique." In International Workshop on Digital Watermarking, pp. 115-124. Springer, Berlin, Heidelberg, 2004.

[49] Liu, Yuling, XinxinQu, and GuojiangXin. "A ROI-based reversible data hiding scheme in encrypted medical images." Journal of Visual Communication and Image Representation 39 (2016): 51-57.

[50] Zhang, Xinpeng. "Reversible data hiding in encrypted image." IEEE signal processing letters 18, no. 4 (2011): 255-258.

[51] Hong, Wien, Tung-Shou Chen, and Han-Yan Wu. "An improved reversible data hiding in encrypted images using side match." IEEE Signal Processing Letters 19, no. 4 (2012): 199-202.

[52] Zhang, Xinpeng. "Separable reversible data hiding in encrypted image." IEEE transactions on information forensics and security 7, no. 2 (2011): 826-832.

[53] Lavanya, A., and V. Natarajan. "Watermarking patient data in encrypted medical images." Sadhana 37, no. 6 (2012): 723-729.

[54] Mantos, Petros LK, and IliasMaglogiannis. "Sensitive patient data hiding using a ROI reversible steganography scheme for DICOM images." Journal of medical systems 40, no. 6 (2016): 156.

[55] Anusudha, K., N. Venkateswaran, and J. Valarmathi. "Secured medical image watermarking with DNA codec." Multimedia Tools and Applications 76, no. 2 (2017): 2911-2932.

[56] Al-Haj, Ali, and Ahmad Mohammad. "Crypto-watermarking of transmitted medical images." Journal of digital imaging 30, no. 1 (2017): 26-38.

[57] Amri, Hedi, Ali Khalfallah, MalekGargouri, NaïmaNebhani, Jean-Christophe Lapayre, and Mohamed-SalimBouhlel. "Medical image compression approach based on image resizing, digital watermarking and lossless compression." Journal of Signal Processing Systems 87, no. 2 (2017): 203-214.

[58] Mousavi, SeyedMojtaba, Alireza Naghsh, Azizah A. Manaf, and S. A. R. Abu-Bakar. "A robust medical image watermarking against salt and pepper noise for brain MRI images." Multimedia Tools and Applications 76, no. 7 (2017): 10313-10342.

[59] Parah, Shabir A., Javaid A. Sheikh, FarhanaAhad, Nazir A. Loan, and GhulamMohiuddinBhat. "Information hiding in medical images: a robust medical image watermarking system for E-healthcare." Multimedia Tools and Applications 76, no. 8 (2017): 10599-10633

[60] Singh, Amit Kumar, Basant Kumar, Mayank Dave, and Anand Mohan. "Robust and imperceptible dual watermarking for telemedicine applications." Wireless Personal Communications 80, no. 4 (2015): 1415-1433.

[61] Singh, Amit Kumar, Basant Kumar, Mayank Dave, and Anand Mohan. "Multiple watermarking on medical images using selective discrete wavelet transform coefficients." Journal of Medical Imaging and Health Informatics 5, no. 3 (2015): 607-614.

[62] Kumar, Basant, Harsh Vikram Singh, Surya Pal Singh, and Anand Mohan. "Secure spread-spectrum watermarking for telemedicine applications." Journal of Information Security 2, no. 02 (2011): 91.

[63] Kumar, Basant, AnimeshAnand, S. P. Singh, and Anand Mohan. "High capacity spread-spectrum watermarking for telemedicine applications." World Academy of Science, Engineering and Technology 79 (2011): 2011.

[64] Mousavi, SeyedMojtaba, Alireza Naghsh, and S. A. R. Abu-Bakar. "A heuristic automatic and robust ROI detection method for medical image watermarking." Journal of digital imaging 28, no. 4 (2015): 417-427.

[65] Lu, J., M. Wang, J. Dai, Q. Huang, L. Li, and C. C. Chang. "Multiple watermark scheme based on DWT-DCT quantization for medical images." Journal of Information Hiding and Multimedia Signal Processing 6, no. 3 (2015): 458-472.

[66] Qi, Xiaojun, and Xing Xin. "A quantization-based semi-fragile watermarking scheme for image content authentication." Journal of visual communication and image representation 22, no. 2 (2011): 187-200.

[67] Liu, Yuling, XinxinQu, GuojiangXin, and Peng Liu. "ROI-based reversible data hiding scheme for medical images with tamper detection." IEICE TRANSACTIONS on Information and Systems 98, no. 4 (2015): 769-774.

[68] Al-Qershi, Osamah M., and Bee EeKhoo. "Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images." Journal of digital imaging 24, no. 1 (2011): 114-125.

[69] Al-Qershi, Osamah M., and B. E. Khoo. "Authentication and data hiding using a reversible ROI-based watermarking scheme for DICOM images." In Proceedings of international conference on medical systems engineering (ICMSE), pp. 829-834. 2009.

[70] Lei, Baiying, Ee-Leng Tan, Siping Chen, Dong Ni, Tianfu Wang, and Haijun Lei. "Reversible watermarking scheme for medical image based on differential evolution." Expert Systems with Applications 41, no. 7 (2014): 3178-3188.

[71] Kumsawat, Prayoth, KittiAttakitmongcol, and ArthitSrikaew. "A new approach for optimization in image watermarking by using genetic algorithms." IEEE Transactions on Signal Processing 53, no. 12 (2005): 4707-4719.

[72] Coatrieux, Gouenou, Wei Pan, Nora Cuppens-Boulahia, FrédéricCuppens, and Christian Roux. "Reversible watermarking based on invariant image classification and dynamic histogram shifting." IEEE Transactions on information forensics and security 8, no. 1 (2012): 111-120.

[73] Hwang, HeeJoon, Hyoung-Joong Kim, VasiliySachnev, and Sang-Hyun Joo. "Reversible Watermarking Method Using Optimal Histogram Pair Shifting Based on Prediction and Sorting." TIIS 4, no. 4 (2010): 655-670.

[74] Kamstra, Lute, and Henk JAM Heijmans. "Reversible data embedding into images using wavelet techniques and sorting." IEEE transactions on image processing 14, no. 12 (2005): 2082-2090.

[75] Pan, Wei, GouenouCoatrieux, N. Cuppens, FrédéricCuppens, and Ch Roux. "An additive and lossless watermarking method based on invariant image approximation and Haar wavelet transform." In 2010 Annual International Conference of the IEEE Engineering in Medicine and Biology, pp. 4740-4743. IEEE, 2010.

[76] Sachnev, Vasiliy, HyoungJoong Kim, Jeho Nam, Sundaram Suresh, and Yun Qing Shi. "Reversible watermarking algorithm using sorting and prediction." IEEE Transactions on Circuits and Systems for Video Technology 19, no. 7 (2009): 989-999.

[77] Al-Haj, Ali. "Secured telemedicine using region-based watermarking with tamper localization." Journal of digital imaging 27, no. 6 (2014): 737-750.

[78] Tareef, Afaf, Ahmad Al-Ani, Hung Nguyen, and Yuk Ying Chung. "A novel tamper detection-recovery and watermarking system for medical image authentication and EPR hiding." In 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 5554-5557. IEEE, 2014.

[79] Hajjaji, Mohamed Ali, El-Bay Bourennane, Abdessalem Ben Abdelali, and AbdellatifMtibaa. "Combining Haar wavelet and KarhunenLoeve transforms for medical images watermarking." BioMed research international 2014 (2014).

[80] Eswaraiah, Rayachoti, and E. Sreenivasa Reddy. "Medical image watermarking technique for accurate tamper detection in ROI and exact recovery of ROI." International journal of telemedicine and applications 2014 (2014): 13.

[81] Priya, R. Lakshmi, T. Belji, and V. Sadasivam. "Security of health imagery via reversible watermarking based on differential evolution." In 2014 International Conference on Medical Imaging, m-Health and Emerging Communication Systems (MedCom), pp. 30-34. IEEE, 2014.

[82] Naheed, Talat, Imran Usman, Tariq M. Khan, Amir H. Dar, and Muhammad FarhanShafique. "Intelligent reversible watermarking technique in medical images using GA and PSO." Optik-International Journal for Light and Electron Optics 125, no. 11 (2014): 2515-2525

[83] Luo, Lixin, Zhenyong Chen, Ming Chen, Xiao Zeng, and Zhang Xiong. "Reversible image watermarking using interpolation technique." IEEE Transactions on information forensics and security 5, no. 1 (2009): 187-193.

[84] Xuan, Guorong, Yun Q. Shi, Chengyun Yang, YizhanZheng, DekunZou, and Peiqi Chai. "Lossless data hiding using integer wavelet transform and threshold embedding technique." In 2005 IEEE International Conference on Multimedia and Expo, pp. 1520-1523. IEEE, 2005.

[85] Tian, Jun. "Reversible data embedding using a difference expansion." IEEE transactions on circuits and systems for video technology 13, no. 8 (2003): 890-896.

[86] Lee, Sunil, Chang D. Yoo, and Ton Kalker. "Reversible image watermarking based on integer-to-integer wavelet transform." IEEE Transactions on information forensics and security 2, no. 3 (2007): 321-330.

[87] Lai, Chih-Chin, and Cheng-Chih Tsai. "Digital image watermarking using discrete wavelet transform and singular value decomposition." IEEE Transactions on instrumentation and measurement 59, no. 11 (2010): 3060-3063.

[88] Dhavale, Sunita V., and L. M. Patnaik. "High capacity, robust lossless EPR data hiding using CDCS with ROI tamper detection." In 2010 International Conference on Computer and Communication Technology (ICCCT), pp. 108-112. IEEE, 2010.

[89] Shehab, Abdulaziz, Mohamed Elhoseny, Khan Muhammad, Arun Kumar Sangaiah, Po Yang, Haojun Huang, and GuolinHou. "Secure and robust fragile watermarking scheme for medical images." IEEE Access 6 (2018): 10269-10278.

[90] Muhammad, Khan, Muhammad Sajjad, IrfanMehmood, Seungmin Rho, and Sung WookBaik. "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image." Multimedia Tools and Applications 75, no. 22 (2016): 14867-14893.

[91] Dhole, Vinayak S., and Nitin N. Patil. "Self embedding fragile watermarking for image tampering detection and image recovery using self recovery blocks." In 2015 International Conference on Computing Communication Control and Automation, pp. 752-757. IEEE, 2015.

[92] Patra, Banani, and Jagdish C. Patra. "Crt-based fragile self-recovery watermarking scheme for image authentication and recovery." In 2012 international symposium on intelligent signal processing and communications systems, pp. 430-435. IEEE, 2012.

[93] Preda, RaduOvidiu. "Self-recovery of unauthentic images using a new digital watermarking approach in the wavelet domain." In 2014 10th international conference on communications (COMM), pp. 1-4. IEEE, 2014.

[94] Kannammal, A., and S. Subha Rani. "Two level security for medical images using watermarking/encryption algorithms." International Journal of Imaging Systems and Technology 24, no. 1 (2014): 111-120.

[95] Singh, Amit Kumar. "Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images." Multimedia Tools and Applications 76, no. 6 (2017): 8881-8900.

[96] Rosiyadi, Didi, Shi-Jinn Horng, Pingzhi Fan, Xian Wang, Muhammad Khurram Khan, and Yi Pan. "Copyright protection for e-government document images." IEEE MultiMedia 19, no. 3 (2011): 62-73.

[97] Singh, Amit Kumar, Mayank Dave, and Anand Mohan. "Hybrid technique for robust and imperceptible multiple watermarking using medical images." Multimedia Tools and Applications 75, no. 14 (2016): 8381-8401.

[98] Singh, Anjul, and AkashTayal. "Choice of wavelet from wavelet families for DWT-DCT-SVD image watermarking." (2012).

[99] Srivastava, Arpita, and PrafulSaxena. "DWT-DCT-SVD based semiblind image watermarking using middle frequency band." IOSR J ComputEng 12, no. 2 (2013): 63-66.

[100] S Singh, VS Rathore, R Singh and MK Singh, “Hybrid semi-blind image watermarking in redundant wavelet domain”, Multimedia Tools and Applications, Vol. 76, No. 18, pp. 19113-37, 2017.

[101] Singh, Siddharth, Vivek Singh Rathore, and Rajiv Singh. "Hybrid NSCT domain multiple watermarking for medical images." Multimedia Tools and Applications 76, no. 3 (2017): 3557-3575.

[102] Zear, Aditi, Amit Kumar Singh, and Pardeep Kumar. "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine." Multimedia tools and applications 77, no. 4 (2018): 4863-4882.

[103] Singh, Amit Kumar, Mayank Dave, and Anand Mohan. "Hybrid technique for robust and imperceptible multiple watermarking using medical images." Multimedia Tools and Applications 75, no. 14 (2016): 8381-8401.

[104] Elhoseny, Mohamed, Gustavo Ramírez-González, Osama M. Abu-Elnasr, Shihab A. Shawkat, N. Arunkumar, and Ahmed Farouk. "Secure medical data transmission model for IoT-based healthcare systems." IEEE Access 6 (2018): 20596-20608.

[105] Anwar, AsmaaSabet, Kareem Kamal A. Ghany, and Hesham El Mahdy. "Improving the security of images transmission." International Journal 3, no. 4 (2015): 7-13.

[106] Thakur, Sriti, Amit Kumar Singh, Satya Prakash Ghrera, and Mohamed Elhoseny. "Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications." Multimedia tools and Applications 78, no. 3 (2019): 3457-3470.

[107] Khan, Mohammad Ibrahim, Md Rahman, MdSarker, and Iqbal Hasan. "Digital Watermarking for Image AuthenticationBased on Combined DCT, DWT and SVD Transformation." arXiv preprint arXiv:1307.6328 (2013).

[108] Singh, Amit Kumar, Basant Kumar, Sanjay Kumar Singh, S. P. Ghrera, and Anand Mohan. "Multiple watermarking technique for securing online social network contents using back propagation neural network." Future Generation Computer Systems 86 (2018): 926-939.

[109] Singh, Amit Kumar, Basant Kumar, Ghanshyam Singh, and Anand Mohan, eds. Medical image watermarking: techniques and applications. Springer, 2017.

[110] Singh, Amit Kumar, Basant Kumar, Sanjay Kumar Singh, Mayank Dave, Vivek Kumar Singh, Pardeep Kumar, S. P. Ghrera, Pradeep Kumar Gupta, and Anand Mohan. "Guest

editorial: robust and secure data hiding techniques for telemedicine applications." Multimedia Tools and Applications 76, no. 5 (2017): 7563-7573.

[111] https://www.forbes.com/sites/forbestechcouncil/2017/12/15/the-real-threat-of-identity-theft-is-in-your-medical-records-not-credit-cards/#3221cf1a1b59

[112] Bhatnagar, Gaurav, and Balasubramanian Raman. "A new robust reference watermarking scheme based on DWT-SVD." Computer Standards & Interfaces 31, no. 5 (2009): 1002-1013.

[113] Wu, Yue, Joseph P. Noonan, Gelan Yang, and Huixia Jin. "Image encryption using the two-dimensional logistic chaotic map." Journal of Electronic Imaging 21, no. 1 (2012): 013014.

[114] El-Samie, Fathi E. Abd, HossamEldin H. Ahmed, Ibrahim F. Elashry, Mai H. Shahieen, Osama S. Faragallah, El-Sayed M. El-Rabaie, and Saleh A. Alshebeili. Image encryption: a communication perspective. CRC Press, 2013.

[115] Wu, Yue, Joseph P. Noonan, and SosAgaian. "NPCR and UACI randomness tests for image encryption." Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT) 1, no. 2 (2011): 31-38.

[116] MedPix searchable online database- https://medpix.nlm.nih.gov/.

[117] S Singh, VS Rathore, R Singh and MK Singh, "Hybrid semi-blind image watermarking in redundant wavelet domain", Multimedia Tools and Applications, Vol. 76, No. 18, pp. 19113-37, 2017.

[118] Public-Domain Test Images for Homeworks and Projects https://homepages.cae.wisc.edu/~ece533/images/

[119] AljosaPavelin, I Klapan, M Kovac, M Katic, R Stevanovic, M Rakic and N Klapan, ‘‘A Functional Telemedicine Environment in the Framework of the Croatian’’, In Remote Cardiology Consultations Using Advanced Medical Technology, IOS Press, Inc. Vol. 372, pp.79–93, 2006.

[120] Usman, Muhammad, Irfan Ahmed, M. Imran Aslam, Shujaat Khan, and Usman Ali Shah. "SIT: a lightweight encryption algorithm for secure internet of things." arXiv preprint arXiv:1704.08688 (2017).

[121] Priya, S., R. Varatharajan, GunasekaranManogaran, RevathiSundarasekar, and PriyanMalarvizhi Kumar. "Paillierhomomorphic cryptosystem with poker shuffling transformation based water marking method for the secured transmission of digital medical images." Personal and ubiquitous computing 22, no. 5-6 (2018): 1141-1151.

[122] C Lakshmi, K Thenmozhi, JB Rayappan and R Amirtharajan "Encryption and watermark-treated medical image against hacking disease—An immune convention in spatial and frequency domains" Computer methods and programs in biomedicine, vol. 159, pp. 11-21, 2018.

[123] W Stallings, "Cryptography and Network Security: Principles and Practice", 5thed, Pearson Education India, 2010.

LIST OF PUBLICATIONS

Book Chapter(s)

[1] S Thakur, AK Singh, SP Ghrera and M Dave (2017) Watermarking Techniques and its Applications in Tele-Health: A Technical Survey, In: S. Ramakrishnan (ed.) Cryptographic and Information Security Approaches for Images and Videos, CRC pp. 467- 508.

Journal(s)

[1] S Thakur , AK Singh , SP Ghrera and Mohamed Elhoseny (2019) Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications, Multimedia Tools and Applications, Vol. 78, Issue 3, pp. 3457-3470, doi: 10.1007/s11042-018-6263-3,Springer. **(SCI Indexed, IF = 2.101**)

[2] S Thakur, AK Singh, SP Ghrera and A Mohan (2018) Chaotic based secure watermarking approach for medical images, Multimedia Tools and Applications, pp. 1-14, doi: 10.1007/s11042-018-6691-0, Springer.**(SCI Indexed, IF = 2.101**)

[3] S Thakur, A K Singh and SP Ghrera (2018) NSCT domain based secure multiple watermarking technique through lightweight encryption for medical images, Concurrency and Computation: Practice and Experience, pp. 1-10, doi: 10.1002/cpe.5108, Wiley **(SCI Indexed, IF = 1.114**).

Conference(s)

[1] S Thakur, AK Singh, Basant Kumar, and SP Ghrera (2020) Improved DWT-SVD-Based Medical Image Watermarking Through Hamming Code and Chaotic Encryption. In: Dutta D., Kar H., Kumar C., Bhadauria V. (eds) Advances in VLSI, Communication, and Signal Processing. Lecture Notes in Electrical Engineering, vol 587, pp. 897-905, Springer, Singapore

[2] S Thakur, AK Singh, and SP Ghrera (2020) Encryption Based DWT-SVD Medical Image Watermarking Technique Using Hamming Code. In: Singh P., Panigrahi B., Suryadevara N., Sharma S., Singh A. (eds) Proceedings of ICETIT 2019. Lecture Notes in Electrical Engineering, vol 605, pp. 1091-1099, Springer, Cham