Securing the Digital Documents for Application in E-Governance

A Thesis Report submitted in fulfillment of the requirement for the award of the degree of

Master of Technology

In

Computer Science & Engineering

Under the Supervision of

Dr. AMIT KUMAR SINGH
(Supervisor)

By

Akankasha Sharma (152217)

Jaypee University of Information Technology Waknaghat, Solan, Himachal Pradesh- India 173234

JAYPEE UNIVERSITY OF INFORMATIO TECHNOLOGY
(Established by H.P. State Legislative 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
Fax: +91-01792-245362

CERTIFICATE

This is to certify that thesis report entitled **"Securing the Digital Documents for Application in E-Governance "**, submitted by Akankasha Sharma in partial fulfillment for the award of degree of Master of Technology in Computer Science & Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been made under my supervision.

This synopsis has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

Date: June 2017

Signature

Supervisor's Name: Dr. Amit Kumar Singh

Designation:

Assistant Professor (Senior Grade)

Computer science & Engineering

JUIT, Solan

Acknowledgement

The great desire to acquire higher qualifications and purse research drove me to promise my parents, brother a useful research work. My promise was to live up to their expectations and never let them down.

I express my heartfelt gratitude to all those who have contributed directly or indirectly towards obtaining my master's degree and at the same time I cherish the years spent in the department of Computer Science and Engineering Department. I am extremely indebted to my esteemed supervisor Dr. Amit Kumar, who has guided me through thick and thins. The project would not have been possible without his guidance and active support. I am indebted to Dr. S.P. Ghrera (H.O.D of Computer Science and Engineering) for providing all kinds of the facilities to carry out the research.

I would like to thank my parents Mr. Shashi Sharma and Mrs. Anjna Sharma, and my brother Abhishek Sharma who have supported and encouraged me at every stage of my life. Without them, I would never have had neither the confidence nor the tenacity to do the research. They had been a constant source of inspiration to me.

Date:

Akankasha Sharma

Table of Content

S. No.		Topic	Page No.
1.		Introduction	1
	1.1	Concept of data hiding	2
	1.2	Objective of digital watermarking	4
	1.3	Watermark image characteristics	6
	1.4	Application of watermarking	7
2.		Recent trends in Watermarking	10
3.		Wavelet and Karhunen - Loeve Transform based Robust and Imperceptible Data Hiding Technique using digital images	19
	3.1	Introduction	19
	3.2	Proposed Technique	20
	3.3	Experimental Result and Analysis	28
4.		Study of Techniques and Simulation Tool Used for the Proposed Technique	34
	4.1	DWT	34
	4.2	Distribution and Attacks	34
	4.3	About Matlab	35
5.		Conclusion and future directions	37

List of Figures

S.No.	Title	Page No.
1.	Stegnography process	3
2.	Cryptography process	3
3.	Watermarking process	4
4.	Characteristics of watermarked image	6
5.	Applications of watermarking	7
6.	Implementation of the proposed solution (Embedding)	20
7.	Implementation of the proposed solution (Extraction)	21
8.	Original Image(Lena.jpg)	22
9.	Watermark Image(Peppers.jpg)	22
10.	1 level DWT on cover image (lena.jpg)	23
11.	1 level DWT on watermark image	23
12.	Transformed Image (KL transform)	24
13.	Possibly Distorted image	25
14.	Image denoising using DCT dictionary	25
15.	Image denoising using the Global trained dictionary	26
16.	Image denoising using KSVD	26
17.	Denoised image	27
18.	Inverse KL transformed image	27
19.	Extracted watermark (Ewatermark.jpg)	28
20.	Watermark Image (256 *256)	29
21.	Watermark Image (128 *128)	29
22.	Watermark Image (64 *64)	29

S.No.	Title	Page No.
23.	Watermark Image (v= 0.01)	31
24.	Watermark Image (v= 0.02)	31
25.	Watermark Image (v= 0.03)	31
26.	Watermark Image (v= 0.04)	31
27.	Watermark Image (v= 0.01) for watermark (256* 256)	32
28.	Watermark Image (v= 0.02) for watermark (256* 256)	32
29.	Watermark Image (v= 0.03) for watermark (256* 256)	32
30.	Watermark Image (v= 0.04) for watermark (256* 256)	32
31.	Watermark Image (d= 0.01)	33
32.	Watermark Image (d= 0.02)	33
33.	Watermark Image (d= 0.03)	33
34.	Watermark Image (d= 0.04)	33
35.	Gaussian noise on watermarked image (Mean =0, Variance=0.01)	33
36.	Gaussian noise on watermarked image (Mean =0, Variance=0.02)	33

List of Tables

S.No.	Title	Page No.
1.	Difference between Cryptography Stegnography, Watermarking	4
2.	Summary of various state of arts techniques	14
3.	Fixed gain (0.04), variable watermark size	29
4.	Fixed gain(0.04), variable bands	30
5.	Variable gain	30
6.	NC performance against attacks at gain = 0.1	31
7.	Speckle noise on Watermark image (with fixed gain 0.04) when applied on watermark (256 * 256)	32
8.	Commands for managing Variable	36

Abstract

Information security is essential to an effective and safe e-government. The objective of e-governments is to provide services accessible to an entire region at a reasonable cost and in a reasonable amount of time. Government offices can use information technology and the Internet to provide better services to people and businesses and to facilitate cooperation among government institutions. However, e-governments must ensure efficient information authentication. Watermarking, or data hiding, can help e-governments meet these goals. In this work, we will propose a robust and secure watermark technology and try to make the optimal balance between the major benchmark imperceptibility, robustness and capacity. When digital watermarks are used for intellectual property protection, many e-governance and e-commerce applications are beneficial and they include the online and offline distribution of multimedia content, broadcast services, document verification, and ownership identification and so on. The result of present study also confirmed that there are numerous emerging tools that rectify the drawback of one and another. The objective of the study of various experimentalists remains the same that is to prevent the digital media from being comprised. One level DWT is applied on both the cover image and the watermark image. The KL transform is applied on the LH band of the cover image. The watermarked image is denoised using the KSVD process with improved PSNR. The possible solution to optimize the major benchmark performance parameters are hybrid approach, watermarking with encryption, watermarking with ECCs, watermarking with genetic algorithm. The watermarked image is checked on the attack of poisson noise but the PSNR drop is expectable in positive range. Chapter wise description of the thesis report is describe as follows:

Chapter 1 presents the basic concepts of watermarking and their importance in recent applications and characteristics of watermarking system. Watermarking techniques are divided into spatial and transform domain techniques. Various spatial, transform domain techniques are described briefly in this chapter.

Chapter 2 presents the state-of-the-art watermarking methods and compares the performance of some recent techniques in tabular form.

In chapter 3, we have proposed a watermarking algorithm based on Wavelet and KL transform for robust watermarking scheme. The performance of the method is tested in terms of PSNR and NC. The method is also robust for different attacks.

The introduction of techniques and simulation tool (MATLAB) and its important functions are presented in Chapter 4.

Conclusion and future directions of the work is presented in Chapter 5.

CHAPTER 1
Digital Image Watermarking: An Introduction

In the 21st century the information is exposed to the unprotected network. For protecting the vital information over the communication media, multiple ways like watermarking, cryptography and steganography are been strengthened. E-governance organization handles the various major function over the society. Electronic governance or e-governance is the application of information and communication technology (ICT) for distributing regime accommodations, exchange of information, communication transactions, integration of sundry stand-alone systems and accommodations between regime-to-customer, regime-to-business, regime-to-regime as well as back office processes and interactions within the entire regime framework. Through e-governance, regime accommodations will be made available to denizens in a convenient, efficient and transparent manner. The three main target groups that can be distinguished in governance concepts are regime, denizens and businesses/interest groups. Information security need to be maintained to verify that data are not breached, e.g. ascertaining that data is not disoriented when critical issues arise. These issues include, but are not constrained to: natural disasters, computer/server malfunction or physical larceny. A prevalent method of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arise. Information security is essential to an efficient and safe e-government. The objective of e-governments is to make services accessible to an entire region at a reasonable cost and in a reasonable amount of time. Government offices can use information technology methods and the Internet to provide better services to mankind and businesses, to facilitate cooperation among government and private institutions. However, e-governments must ensure effective information authentication that means the information shouldn't be shared with any unauthenticated third party resources. Watermarking, or data hiding, can help e- government to meet the mentioned goal. Watermarking technology can be explained using the following procedure. First, the watermark is the copyright data that can be later inferred from the cover image for showing the authenticity of the multimedia. The watermarked information in addition to other data is added in the multimedia cover using different embedding techniques. Then, the cover image is transmitted over the exposed network. The multimedia host is manipulated to ensure watermark presence. In contradiction to encryption, watermarking allows data accessibility. If ciphered data is deciphered, then data intellectual property rights are vanished. The

watermark is planned to be inserted inside the multimedia host. If the data owner is questioned, the reply data is reproduced to describe the data owner and its distribution path. Multimedia is the most effective tool for the transfer of the information over the network, for the quick understandable document we need as much as media as possible and that to be integrated in the meaningful way take the example of a webpage in the internet comprises of various media images or text that impart with a meaningful information. In the era of information technology, we are enjoying the benefits of internet that allows free flow of information with no barriers over user and area. The development in the digital media has drastically changed the information flow throughout the globe. With the ease of data creation and retrieval, lead to the threat of data manipulation and theft. To enhance the security issues in terms of confidentiality, data integrity, authentication and authorization various methods such as Cryptography, Steganography, digital watermarking are enforced. Nowadays, growth in technology such as computers and computer network offers widespread use of multimedia contents such as digital image, audio, and video [1-8]. This growth has also made easy duplication and distribution of these multimedia data. Therefore, protection of multimedia content has become an essential and difficult job. Cryptography, Steganography, digital watermarking are the important methods for protection multimedia contents [2]. The important differences between these three methods are illustrated in Table 1 [2]. As discussed in Table 1, watermarking is better than Cryptography and Steganography. The popular application of digital watermarking is depicted in Figure 5 [1]. Depending on the type of multimedia data to be watermarked, the watermarking methods is defined as text, image, audio, and video watermarking [1, 7]. Out of four multimedia data types, data embedding capacity of the image is better than other media. In this context, the present work considered image as cover media. Image watermarking is divided in to spatial and transforms domain techniques. However, the transform domain techniques are more robust than the spatial domain techniques, as reported by various surveys [2-8].

1.1 Concept of Data Hiding

The data hiding means hiding the information for confidentiality or integrity purposes. Different types of data hiding techniques are given as follows:

- **Steganography:** Steganography is derived from the geek word which means to write on a covered surface [1]. In Steganography, the information is hidden in the cover object (any multimedia component such as image, text etc.) to

hide it from the plain side for security purposes. Figure 1 show the basic Steganography process.

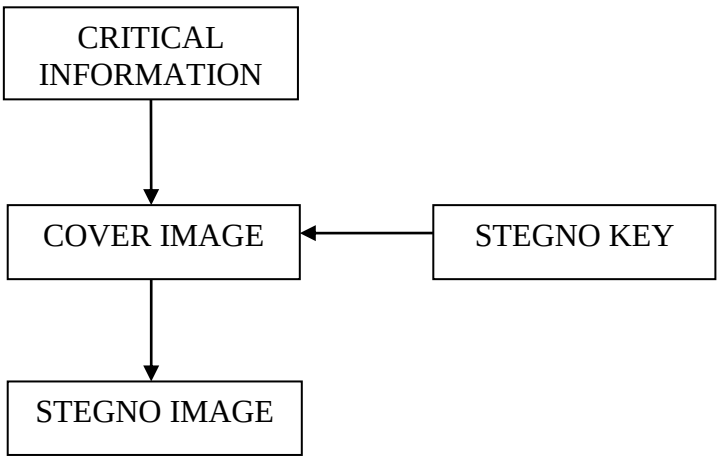

Fig 1: Steganography process

As shown in the Figure 1, the vital information that is more susceptible for an intruder to intrude is hidden inside the cover image using the stegno key , the critical information is hidden in such a way that it is difficult to say just by seeing the cover image that it contain any additional information in it. The resultant image after converting the cover image with stegno key is termed as Stegno image.

- **Cryptography:** Cryptography is a technique where the plain text is converted to encrypted text using the encryption key. Fig 2 describes the general process of the cryptography

Fig 2: Cryptography process

The encrypted text is more susceptible to attacker's attention than stegno image because scrambled text is more attractive to the hacker as it shows some important information is being scrambled up, unlike the stegno image where the data is hidden in the cover image.

- **Watermarking:** Digital watermarking is a technique that offers the confidentiality of the multimedia. Watermarking is a multimedia component

(such as image, text, video etc) that is used for authentication purposes. The watermark is embedded in such a way that quality, robustness and originality are being maintained of the original image. In watermarking, the original image is interleaved with the watermarked code for the copyright protection purposes. There should be no difference between the watermarked image and the cover image. In Fig 3 we shows the general process of watermarking.

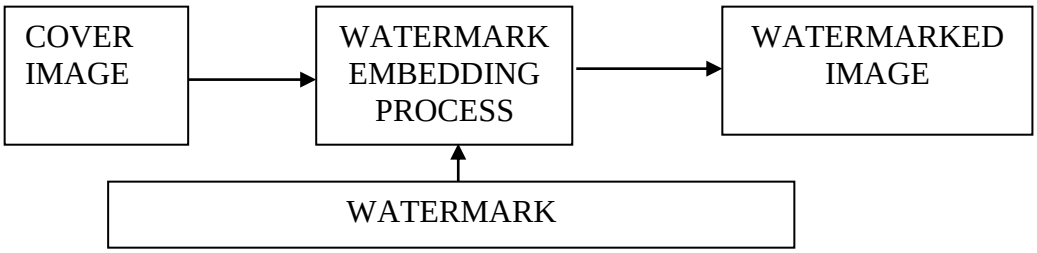

Fig 3: Watermarking process

1.2 Objective of digital watermarking:

The objective of digital watermarking is to embed owner's authentication to user (Visible or invisible) for copyright protection on the digital media. Watermarking is done in such a way that original meaning of the image is not changed. Any attack on the watermarked image shouldn't render the watermark quality. So, watermarking is done to ensure the digital media authenticity which unlike the continuous media can be stored, reproduced and vulnerable to loss of the information. Table 1 shows the difference between amongst the three secure measures to protect the credentialed of the authenticated user.

Table 1: Difference between Cryptography, Steganography, Watermarking

Factors	**Cryptography**	**Steganography**	**Watermarking**
Definition	Cryptography is a technique where the plain text is converted to encrypted text using the encryption key.	Steganography is derived from the geek word which means to write on a covered surface.	Digital watermarking is a technique that offers the confidentiality of the multimedia
Process	The encrypted text is more susceptible to attacker's attention than stegno image because scrambled text is more attractive to the hacker as it shows some important	In Steganography, the information is hidden in the cover object (any multimedia component such as image, text etc.) to hide it from the plain side for security	The watermark is embedded in such a way that quality, robustness and originality are being maintained of the original image.

	information is being scrambled up, unlike the stegno image where the data is hidden in the cover image.	purposes.	
Goal	The main goal of cryptography is to encrypt a message, in such a way that an intruder cannot decrypt or find out what the message was using the set of keys (private or public).	The main goal of Steganography is to hide a message in cover media such as the cover remains unaffected and draws no attention of the intruder.	The main goal of watermarking is to prevent the authenticity and authorization of multimedia and achieve it by embedding a piece of authentic code in the original media.

1.3 Watermarked Image Characteristics:

The watermark should possess certain kind of the benchmarks for effective preservation of authenticity of the media and user. Fig 4 describes certain kind of benchmarks.

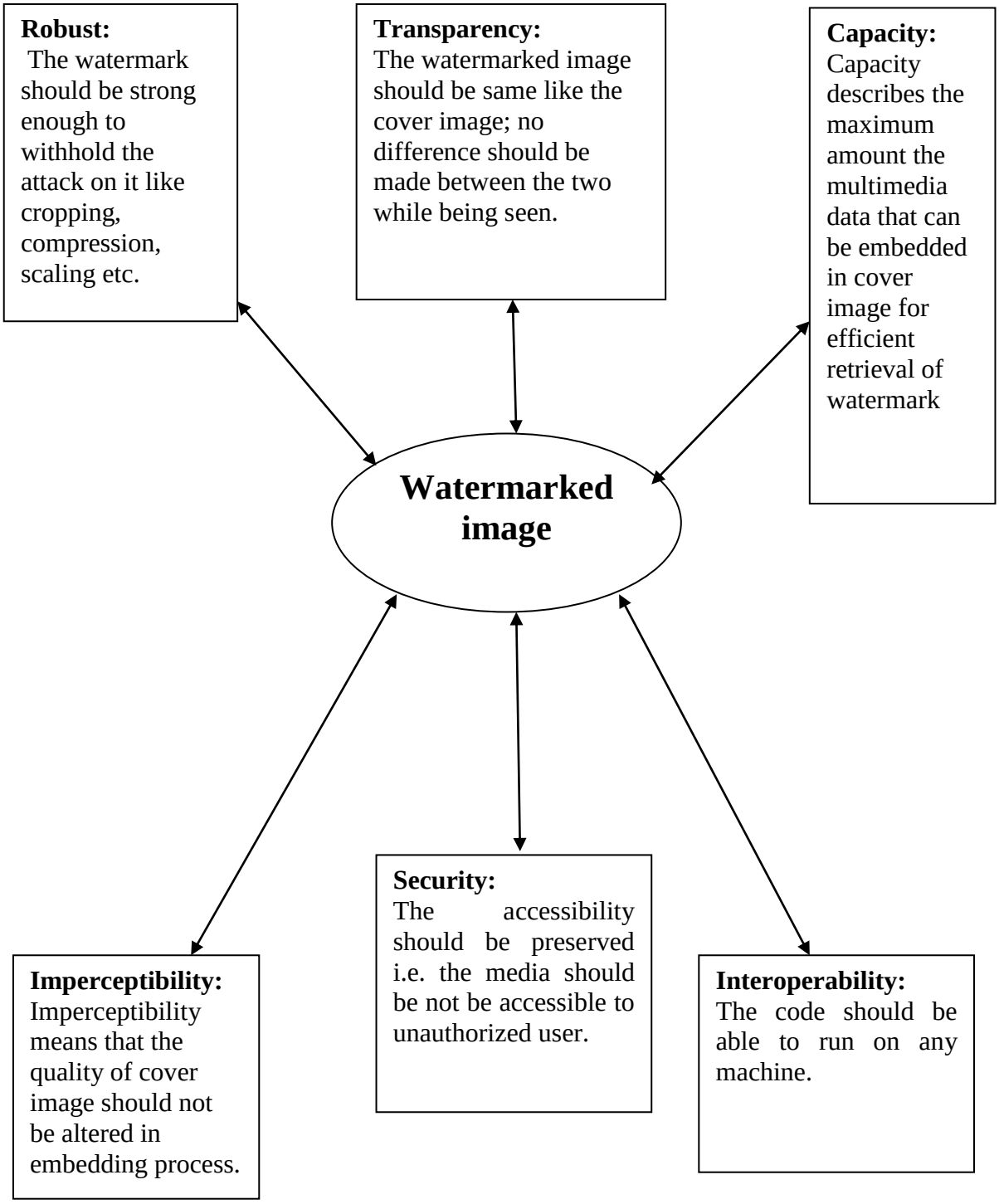

Fig 4: Characteristics of watermarked image

1.4 Application of watermarking

Watermarking have touched various fields and changed the idea of security to great extent. Various application of the watermarking technique is given as following [2, 3]:

- **Copyright protection:** In copyright protection, user's data protection is to be maintained. Copy control should be enforced, to prevent the attacker to copy the media.
- **User's Authenticity preservation**: Watermarking technique can be used to preserve the user authenticity i.e. the media belong to the authorized user such authenticity should be maintained.
- **Telemedicine Application:** In medical applications**,** watermarking can be used to ensure the authenticity of the medical images.
- **Fingerprinting:** finger printing is used to check if there is in a tampering to the multimedia and to find the intruder's information.
- **Broadcast monitoring:** In broadcast monitoring the media is monitored that it is only shared with authentic user.

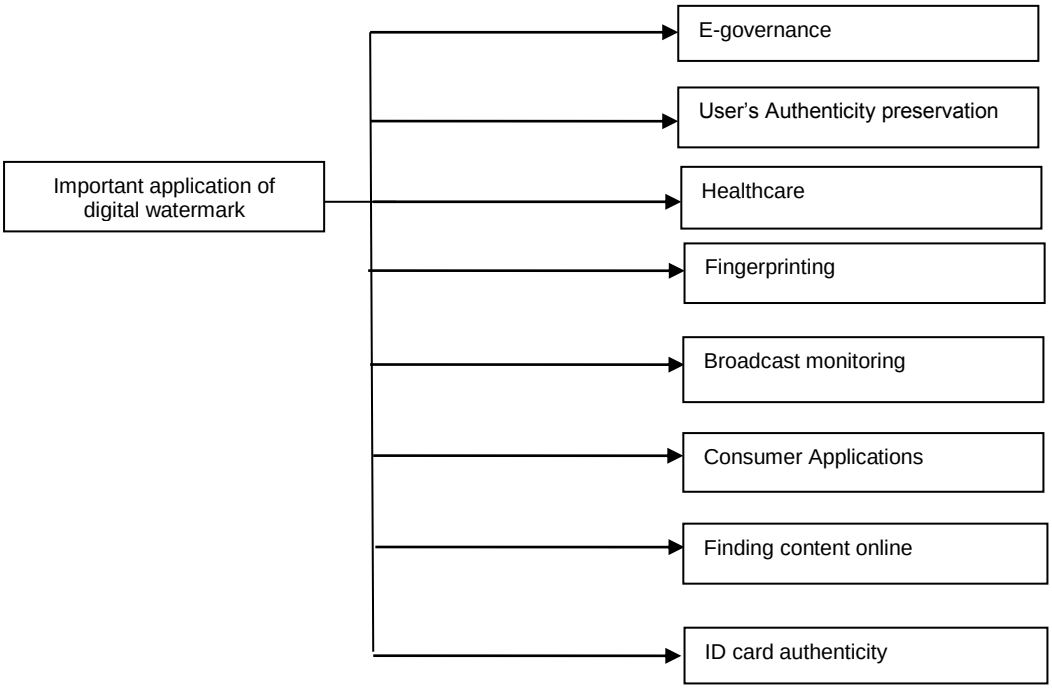

Fig 5 Application of the Watermarking

Watermark embedding can be done in the following ways [4]:

- **On the basis of the domain:**

  The watermark can be embedded in any of the two domain **spatial domain or the transformation domain.**

  In spatial domain, we work directly on image pixels i.e. for watermark embedding we directly manipulated the pixels value of the original image. Example of such techniques are logarithmic transforms, power law transforms, histogram equalization.

  In transformation domain also called as frequency domain don't directly deal with the original image but rather works on the orthogonal transform of the image.

- **On the basis of the visibility:**

  On the basis of the visibility the watermark can be divided into two categories **Visible or the invisible watermark.**

  In invisible watermark technique, the watermark is camouflaged fully in the cover image. That means the viewer won't figure out by seeing the cover image that the original image has any vital information embed in it.

  In the visible watermark technique, the watermark is made visible to viewer. Such Watermark is used in broadcast monitoring.

- **On the basis of media used:**

  The watermark can be text watermark (If sequences of text are embedded in the cover image), Image watermark (If image is used as watermark), Video watermark (If video is used as a watermark), Audio watermark (If audio is used as a watermark).

  Digital watermark may be categorized into spatial and transformation domains watermarking methods. Spatial domain watermarking works through changing spatial/temporal data samples. Transformation domain watermarking works by modifying transform coefficients. Watermarking embeds data into a multimedia file (may be text, image, video etc.) that can later be extracted for authenticity purposed. Applying the security in the digital media can be performed in two ways. One way is that the authentic digital data is not shared with the public. That means, the data is secretly delivered from source to the destination without the involvement of any third party resources. And the other way is to make the digital data made visible to the outside world that makes it less susceptible to the attacker's attention. In the second case, digital watermarking must use robust embedding methodologies to prevent the

data compromise and immune to different attacks. Thus, the digital documents can be transfer over the unsafe media but the benchmarks such as robustness, capacity and imperceptibility of the watermarked image shouldn't be compromised.

"Watermarking" is the process of obnubilating digital information in a carrier signal; the obnubilated information should, but does not require to, contain a cognation to the carrier signal. Digital watermarks may be acclimated to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently utilized for tracing copyright infringements and for banknote authentication. A signal may carry several different watermarks concurrently. Unlike metadata that is integrated to the carrier signal, a digital watermark does not transmute the size of the carrier signal. Both steganography and digital watermarking employ stenographic techniques to embed data covertly in strepitous signals. But whereas steganography aims for imperceptibility to human senses, digital watermarking endeavors to control the robustness as top priority. Since a digital replica of data is identically tantamount to the pristine, digital watermarking is a passive aegis implement. It just marks data, but does not degrade it or control access to the data.

CHAPTER 2

Recent Trends in Image Watermarking: A Brief Survey

The recent and related literatures are discussed below:

Ali Al-Haj [5] proposed a combined robust and imperceptible image watermarking method using combination of DWT and DCT. The PN sequence is generated for the gray scale watermark information before embedding into the cover image. Further, the sequence number is embedding into the DCT transformed of the cover image. The visual quality and robustness performance of the method is evaluated and found to be robust for different known attacks The authors in [6] present a robust and secure watermarking method through DWT, Arnold transform and CDMA. Initially, the Y component of the YIQ color model is decomposed by DWT and the scrambled binary watermark information is encrypted by using the CDMA to generate random number sequence. This sequence is now embedding into the selected sub-band of the DWT cover. The robustness of the method is evaluated for different attacks. Simultaneous embedding of robust and fragile watermark the cove image using pseudo-random sequence based bit substitution is proposed by Shen and Chen [7]. Initially, the method decomposes the cover image up to third level DWT where the fragile and robust watermark is embedding in to the significant and non-significant coefficient of the DWT respectively. The method is extensively evaluated for various attacks. Further, the PSNR performance better than the other reported technique [7] however, the method keep the same robustness as single watermarking method.

A robust and secure logo watermarking technique through SVD and fractional wavelet packet transform (FRWPT) is presented by Bhatnagar et al.[8]. Initially, the considered host image is decomposed into the different sub-band by FRWPT and SVD is applied on the FRWPT transformed coefficients. The singular value of the transformed FRWPT coefficients is modified with the singular value of the watermark image. The performance of the method is extensively evaluated in terms of PSNR, NC, computational and time complexity. Further, the method offers better performance than other exiting work [8].Arsalan et al. [9] developed a blind medical image watermarking method using GA and IWT. In the block (size =16) based embedding process of the watermark, compression function is applied on IWT coefficients and the watermark bit is embedding into the compressed coefficient. The compression function is only applied on those IWT coefficients which are greater than or equal to a chosen threshold value. The experimental results demonstrated that the PSNR and

SSIM performance is better than other existing techniques [9].Bouslimi et al. [10] proposed a combined encryption and watermarking technique for verifying the reliability of the echographic image through RC4, QIM and spatial domain LSB technique. The experimental results demonstrated that the performance of the method is evaluated in terms of entropy and PSNR. Lei et al. [11] proposed a watermarking techniques for binary image through Haar wavelet. Initially the cover binary image is divided into different blocks whereas each block is also divided into the embedding and level area. Further, the method determined the number of black pixel for every block. For embedding the watermark into the cover image, the method first determined the flippable pixels through Haar wavelet and embedding into the selected area of the cover. Didi Rosiyadi et al. [12] describe a robust and non-blind image watermarking method for copyright protection of e-government documents through DCT, SVD and genetic algorithm. In the embedding process of the logo watermark, DCT is applied on cover e-government document image and using the space-filling curve (SFC) for the DCT coefficients of the cover. Further, SVD is applied on each area of the DCT coefficients having different frequencies in a rectangular shape. The SVD coefficient of the cover document is modified by the control parameters consisting of the left singular vectors and singular values of the DCT-transformed logo watermark to avoid the false-positive problem as suffered by the SVD based watermarking techniques. In addition to that the scaling factor is optimised by using the GA. The experimental results demonstrated that the performance of the method is extensively evaluated for all four areas of the DCT coefficients and found to be robust for the nineteen different attacks.

Bhatnagar et al. [13] proposed a robust DWT based watermarking method where the logo watermark of size 32*32 is embedding into the significant wavelet coefficient of the cover image using ZIG-ZIG sequence. The experimental result is demonstrated that the performance of the method is evaluated in terms of PSNR, NC and time efficiency (embedding and extraction) for different images. Further, the method is also tested for different known attacks and offer superior performance than other reported technique [13].For the copyright protection through image watermarking method is proposed by Lang and Sun[14] using FRFT and hyper chaos. The middle coefficients of the FRFT transformed cover image are considered to embed binary watermark. The experimental results established that the method is robust for different attacks. Shi-Jinn Horng et al. [15] presents a robust and secure blind watermarking technique for the protection of e-governance document using DCT, SVD and genetic algorithm. In the embedding process of the watermark logo image, DCT is applied on the gray scale cover image. All the DCT coefficients of the cover image

are scan into the four different blocks (from lower to higher) in zigzag way. Further, SVD is applied on each block of the DCT transformed image where the singular value of each block of the DCT coefficient is modified with quantizing value using genetic algorithm. The motivation behind using the GA to improved the PSNR and NC performance of the watermarked the extract binary watermark image respectively. The method is also evaluated for various attacks and found to be robust than other reported techniques [15].Rahmati et al. [16] proposed watermarking method to protecting verification documents for E-commerce application. In this method, a person identification number considered as watermark is embedding into the cover digital card image using block based watermarking algorithm. The performance (PSNR and average error ratio) of the method is evaluated for Print Scan (PS) attack and found to be better than other reported technique [16].Region based multiple watermarking method is presented in [17] for securing the medical information through DWT, SVD and LSB technique. The patient information considered as robust watermark is embedding in the region-of-noninterest (RONI) of the image through the transform domain techniques which provide the confidentiality and authenticity of the image. However, the logo watermark is considered as fragile watermark is embedding into the region-of interest (ROI) part of the cover image through LSB technique to provide the image integrity. Experimental results established that the performance of the method is extensively evaluated for various attacks.

Dual level security for the medical applications is also provided through combined encryption and watermarking technique is proposed by Kannammal et al. [18]. In the embedding process of the medical image watermark, the watermark is embedding into the selected sub-band of the natural cover image. Further, the security of the watermarked is enhanced by using three different encryption techniques is applied on the watermarked image. The performance of these three encryption techniques is compared in terms of time for encrypt and decrypt the massage. The experimental results established that the method is robust for different kind of attacks and the RC4 encryption technique perform better than the other two encryption techniques. Singh et al. [19] proposed a robust medical image watermarking method through DWT and SVD. The method is embedding image and text watermark simultaneously into the DWT cover image for patient recognition purpose. Further, the BER performance of the method is reduced by applying four different error correcting codes on the text watermark of size 20 characters before embedding into the medical cover image. The performance of the method is extensively evaluated for various attacks with and without using the ECCs. The experimental results demonstrated that the performance of hybrid ECCs consisting of BCH

and repetition code is better than other ECCs.Singh et al. [20] proposed a secure spread spectrum based text watermarking technique, where four different medical text watermark is embedding simultaneously at different DWT sub-bands of the medical cover image to solved the medical data management issues. Further, the security of the medical information is enhanced by using encryption technique before the information is embedded into the cover image. The method is robust for various signal processing attacks. The proposed method can embed 104 characters without degradation of the visual quality of the watermarked image. Chen et al.[21] developed a robust and blind watermarking technique for 3D images using contourlet transform and depth-image-based rendering (DIBR). The watermark generated through spread spectrum method and each watermark bits is embedding into the selected coefficients of the cover contourlet sub-bands through proper quantization. The PSNR, NC and BER performance of the method is extensively evaluated and found that the low BER performance at different views than other reported methods [21]. In [22] authors present a JND (Just noticeable distortion) DCT based visible watermarking technique, where JND is used to rectify the distortion made by the embedding process. For watermark embedding, grey scale cover image is divided into non overlapping blocks and DCT is applied on the different blocks. For achieving the embedding strength, the mapping is performed on the watermarking intensity range and the cover image's intensity range using JND technique. An improved spread transform dither modulation based robust and secure watermarking technique is proposed by Cao et al.[23]. The watermark is only embedding into the selected embedding subspace. The security and robustness performance of the method is extensively evaluated for estimation of projection vector and amplitude scaling attacks respectively.

Zolotavkin and Juhola [24] proposed a robust watermarking method using QIM. The performance of the method is measured by WNR AND Document to Watermark Ratio (DWR). The method is found to be robust It provides high robust for Additive White Gaussian Noise (AWGN) and Gain Attack (GA).Wang and Allebach[25] proposed a halftone image watermarking in which watermark is embedding into the halftone by using synchronization pattern. The performance of the method is evaluated in terms of PSNR, normalized HVS mean square error and watermark rate and found to be good visual quality and achieved high watermark capacity. ESSAIDANI et al.[26] presents a robust image watermarking method using Delaunay triangulation and the features points of the cover image. The sobel edge detector is used to determine the features points which are used to produce Delaunay Triangulation. A region based robust and secure watermarking method is presented by Sharma et al.[27] for medical applications. The method initially uses DWT and

DCT to embed multiple watermark information in to the cover medical image. Further, the security of the image and text watermark information is enhanced by message-digest (MD5) hash algorithm and Rivest–Shamir–Adleman (RSA) respectively before embedding into the medical cover image. In order to enhance the robustness of the text watermark hamming error correction code is also applied on the encrypted watermark. The experimental results have been shown that the method is robust for important signal processing attacks.In [28] authors address the image denoising problem, where zero-mean white and homogeneous Gaussian additive noise is to be removed from a given image. The approach is based on sparse and redundant representations over trained dictionaries. Using the K-SVD algorithm, they obtain a dictionary that describes the image content effectively.

Table 2 differentiate between the various research issues with the parameters of technology used, objective of study, results found and any other important issue.

Table 2: Summary of different state of art techniques

Reference Number	**Objective**	**Technique to achieve the objective**	**Results**	**Other important points/issues**
[5]	Robust and imperceptible watermarking method for copyright protection	DWT, DCT	Max NC for Gaussian attacks = 0.9738 Max PSNR(with HL2 sub-bands) = 97.072 dB	- Combined techniques compensate the drawback of each other. - Tested for different DWT sub-bands and three important attacks. -Grey-scales cover and watermark image of size 512´512 and 256´256 respectively.
[6]	Robust and secure watermarking method.	DWT2, Arnold Scramble, CDMA	For value k=0.5 PSNR (Lena): 78.01 dB Max Correlation (JPEG compression attack) : 0.9999	- Tested for small watermark sizes. (27*27). - Cover image size is 512 * 512. - Addition of more PN sequence alters the image transparency. - High complexity due to the scrambling
[7]	Using multiple watermarking to protect the information and integrity of media	Three level DWT, Pseudo random sequence based bit substitution	PSNR (Mean shift): 28.5274 Max NC for median filter attack :0.9999	-Fragile watermark technique. -Two watermark are used (Robust and fragile). -NC falls to 0.6062 when noise is increased 10%
[8]	Secure, imperceptible , user adjustable	SVD,FRWPT	PSNR: 41.0695dB Correlation coefficient:	- Tested on gray scale images. - High Complexity

	watermarking scheme.		0.7296 (Sharpen attack)	- Cropping attack lead to cropping of the watermarked image. - Quality of image is directly associated with the watermark.
[9]	Imperceptible and intelligent watermarking scheme for medical images.	Block based embedding , Genetic Algorithm, Integer wavelet Transform	PSNR: (X-ray) 56.6 SSIM (Lena): 0 .9982	- Gray Scale images are used, both cover and watermark. - If number of block size increased than threshold matrix increase for extraction.
[10]	Joint encryption and watermarking to ensure integrity and authenticity for medi cal images.	LSB substitution, QIM modulation , RC4	PSNR : 49.366 Entropy of encrypted image: 7.995	- Gray scale watermark is used. - Less robust to attack like lossy image compression. - Digital signatures are used to ensure the reliability of the image. - embedded messages are randomly generated.
[11]	Robust and blind watermarking schemes for binary cover images	Harr wavelet transform	Number of black flappable pixels: Text : 2770 Picture: 2502 Number of white flappable pixels: Text: 2620 Picture: 2567 ELDM /N = Text : 3.4673 Picture: 2.4063	- Increase Salt and pepper noise alters the detection of the watermark. - probability of error increases if the mean value of Gaussian noise increased.
[12]	robust and non-blind image watermarking method for copyright protection of e-government documents	DCT,SVD	Cropping on right half with replacement: PSNR : 36.6554 NC: 0.9882	- Low PSNR value for rotation attacks. - Low NC value for Gaussian noise. - Can be implemented adaptive watermarking scheme based on texture and edge masking.
[13]	Secure and robust watermarking technique based on image fusion.	DWT	PSNR (Lena) : 57.7460 TIME EFFICENCY (Extraction + Embedding) : 11.0994	- gray scale watermark is used. - watermark size is particularly smaller (32 * 32). Gray scale cover image (256 *256 is used)

				- Single watermark is used. -increase in noise; degrade the watermark (extracted watermark noisy).
[14]	Robust, Imperceptible, Secure watermarking scheme for copyright protection.	Hyperchaos system , FRFT	NC (Salt and pepper noise): 0.94596	- Gray level image is used.(cover) 512 * 512 and watermark size is 64 *64 pixels. - Binary image is used as the watermark. - If the standard deviation is increased the NC value drops for all attacks.
[15]	Robust and secure method for copyright protection of E-Documents	DCT,SVD,GA	Gaussian noise for variance value 1.5 PSNR: 22.2400 NC: 0.5891	- Increase in computational complexity after applying SVD to the DCT transformed image. -Single watermark is used. -Blind watermarking scheme. -NC value drops if variance increased.
[16]	watermarking method for protecting verification documents for E-commerce application	block based watermarking algorithm	PSNR: 44.3324 Average error ratio (Rotation 5°): 1.12%	- Identification number is taken as a watermark. - High average error ratio if cropping rate is increased 75 %.
[17]	Secure, blind region based watermarking scheme for medical images.	DWT,LSB,SVD	PSNR : 34.1107 (X-ray image) Gaussian noise NC : 0.979	- ROI is watermarked in the spatial domain and RONI is watermarked in frequency domain (fragile and robust watermarks) - Low robust to JPEG compression attack - Time for execution is high if smaller block is used for watermarking process.
[18]	Robust Dual level security for the medical applications	Discrete non-tensor product wavelet transform, RSA, AES, RC4	(Brightness Attack) PSNR : 91.70dB NC: 1 (RC 4 encrypted) CV: 0.09 SSIM:0.677	- Tested on radiological images. - Watermark is embed on the LH suband by LSB substitution. - Watermark processing Complexity is increased as the watermarked image is encrypted with encryption algorithm. - RC4 results in speed and performance are better than AES and RSA
[19]	Robust, secure medical image	DWT,SVD,	Highest PSNR obtained with ECC's	- Gray level image is made as a cover

	watermarking		(140 text bits) is 37.22dB NC: 1 BER: 0 (All gain factors)	image.(512 * 512) - Two watermarks (Text + image) were added. - Four different types of error correcting code were used. - Image watermark is embedded using DWT and SVD and text watermark using ECC's.
[20]	Secure, robust spread spectrum based text watermarking technique for medical image.	Harr wavelet transform	Gain Factor : 15 PSNR: 31.23dB with encryption of 104 BER(%) Median filtering characters. : 0.0480	- Tested for test watermarks. - Gray scale cover image is used. - High BER value with JPEG compression attack (0.4326) - High multi resolution, superior HVS quality. - Text watermarks are added to the third band HL3 and LH3 subands. - Patient records are added to the HL2 and LH2 subands. - Complexity is increased as the text watermark is encrypted.
[21]	robust and blind watermarking technique for 3D images	Contourlet transform, (DIBR).	For art image: PSNR: 42.71 SSIM: 0.995 MOS: 4.7	- Quality factor decreased if BER increased in the case of JPEG compression. - Gaussian noise variance increased if BER increased in case of Gaussian noise.
[22]	Robust visible watermarking technique.	JND,DCT	Obtrusiveness controlling factor : 60	- Gray scale watermark image is used. - Can be used with the JND estimation. - To avoid blocking artifiact $JND_{b=0}$ - Future scope involves finding the non-linearity between the watermark and texture.
[23]	Secure and robust (to amplitude scaling) technique for watermarking	STDM,ISTDM	WCR : 20dB Nv= 400	- ISTDM uses STDM to embed the watermark in embedding space. - Only tested with text watermark. - Comparative study is done and tested for Gaussian noise and amplitude scaling.
[24]	Robust	GA, brute force	DWR (Document to	- Tested for gray

	watermarking method using scalar quantization to achieve higher amount of extracted information	optimization, RDM,DCQIM	Watermark ratio): 28dB WNR: 12dB	scale images. - Not tested for the watermark tampering attacks. - Optimization of the embedding procedure is computationally difficult.
[25]	Robust, imperceptible halftone image watermarking technique	Halftoning, DBS	For host image (Lena) PSNR: 30.3 dB NMSE: 24.5 dB BER: 0.73 % WMR: 4.62 % PER: 0.79 %	- Complexity is increased due to the every step pixel by pixel scanning. - Cover image of size 512 * 512 is chosen. - Error decoding rate depends on the P&S recovery.
[26]	Robust ,Blind image watermarking method using Delaunay triangulation	Delaunay triangulation	NC (Rot crop_0.5) : 19.9123 PSNR: 42.62 dB	- High complexity. - Modified triangulation is immune to the geometric transformation. - Tested on gray scale (665 * 586) cover image. - Watermark size is particularly smaller (28 * 28)
[27]	Secure multiple watermarking techniques using various errors correcting code for medical images.	DWT,DCT,RSA Hamming code, MD5	PSNR (Without processing attacks): 51.833272 Max NC value for Gaussian LPF: 0.965043 BER for Gaussian LPF: 0.1233	- Medical image of size of 512 *512 and watermark of size 256 *256 is selected. - DWT is being applied to LL of ROI and LL band of NROI of cover image. - Low NC value against the rotation attack. - NC value drops if the value of noise is increased in Salt and pepper attack and speckle attack. - Robustness is increased using Hamming code. - PSNR value decreases if gain factor is increased.
[28]	Solving the image denoising problem, when an image is subjected to the white Gaussian noise.	DCT,KSVD,MAP estimation	PSNR (on average with DCT dictionary): 34.45 dB	- sparse decompositions of each image block under one fixed over-complete dictionary. - Worked on small image patches. - K-SVD cannot be directly deployed on larger blocks.

CHAPTER 3

Wavelet and Karhunen - Loeve Transform based Robust and Imperceptible Data Hiding Technique using digital images

Abstract

The technique followed uses DWT, KL transform and KSVD for image denoising. Wavelet [29] analysis has perfect local property, giving nice combination of classical temporal analysis and frequency analysis. Wavelet analysis is used in digital image and video compression and coding, computer vision, pattern reorganization, etc. KLT is used in many domains such as correlation analysis, principal component analysis, and rough sets. KL [30] transform makes the pristine correlative information become independent information. And they are presented in an orthogonal space so that it makes the information category and magnitude study quite possible. K-L transform presents the information distribution features at space and the efficacy of the information transmission. Because K-L transform is unique, the presented information structure is unique additionally. It makes the information quantification become possible. In [31] a accumulation of DWT and KLT designated DWT-predicated KLT and DWT block-predicated KLT was performed. Michael Elad et al. [28] proposed KSVD algorithm for image denoising when the image is quantified in the presence of an additive zero-mean white and homogeneous Gaussian noise. They have utilized sparse and redundant representations over trained dictionaries. Redundant representations were acclimated to have the shift invariance property. KSVD algorithm is simple and efficient for image denoising, but it can't be directly applied on the sizably voluminous images blocks

3.1 Introduction

The cover image is decomposed by DWT and KLT transform is applied on selected sub-band of the cover. The transformed watermark information by DWT is embedding into the KLT coefficients of the DWT cover image. In order to enhanced the visual quality of the watermarked image and reduce the bandwidth requirements, different de-noising dictionary based method is applied on the image. It is noticed that

adaptive based dictionary method is better than DCT and Global dictionary method. The method is also robust for different image processing attacks.

3.2 Proposed Technique

The implementation of the secure and effective data transfer is done using security techniques such as watermarking. Fig 6 depicts the plan for implementation of the plan of the proposed solution for effective transfer of digital documents over the unsafe media.

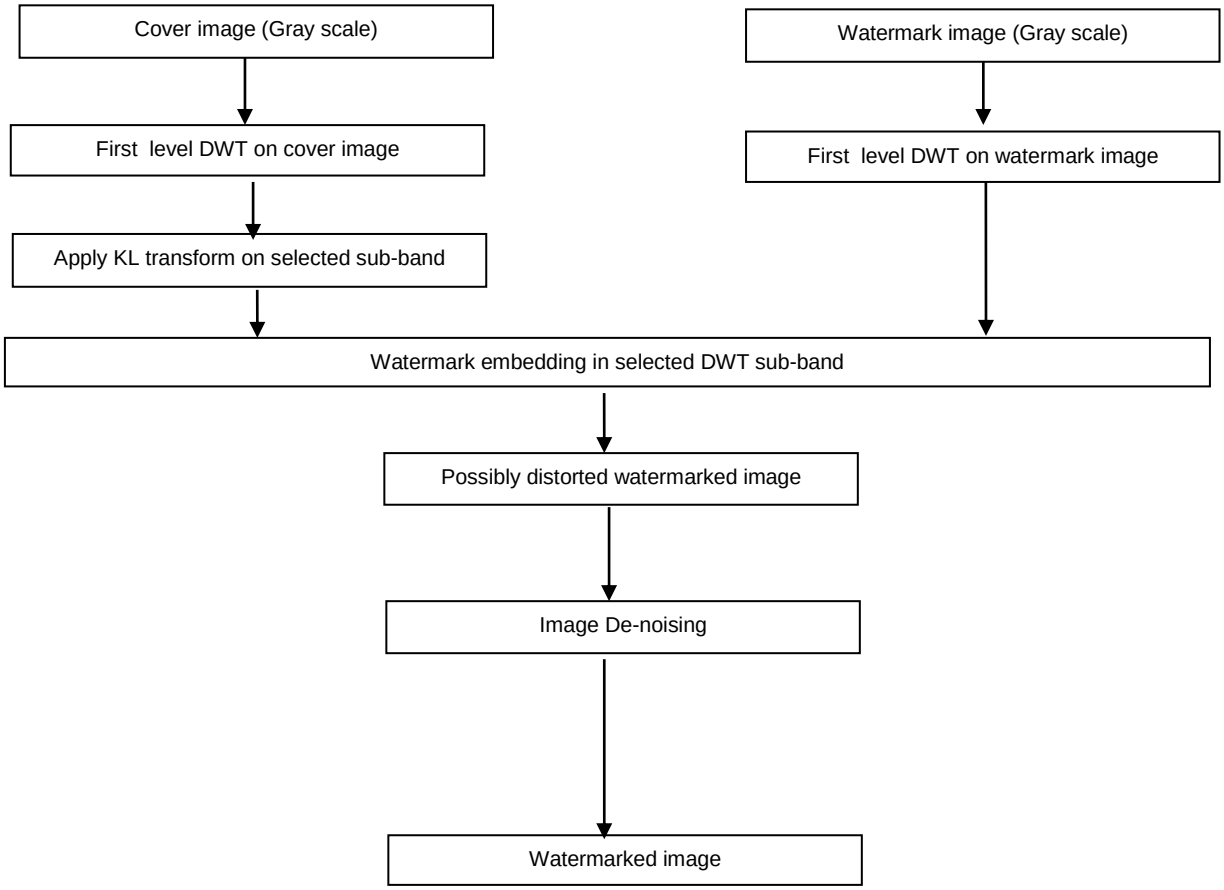

Fig 6: Implementation of the proposed solution (Embedding)

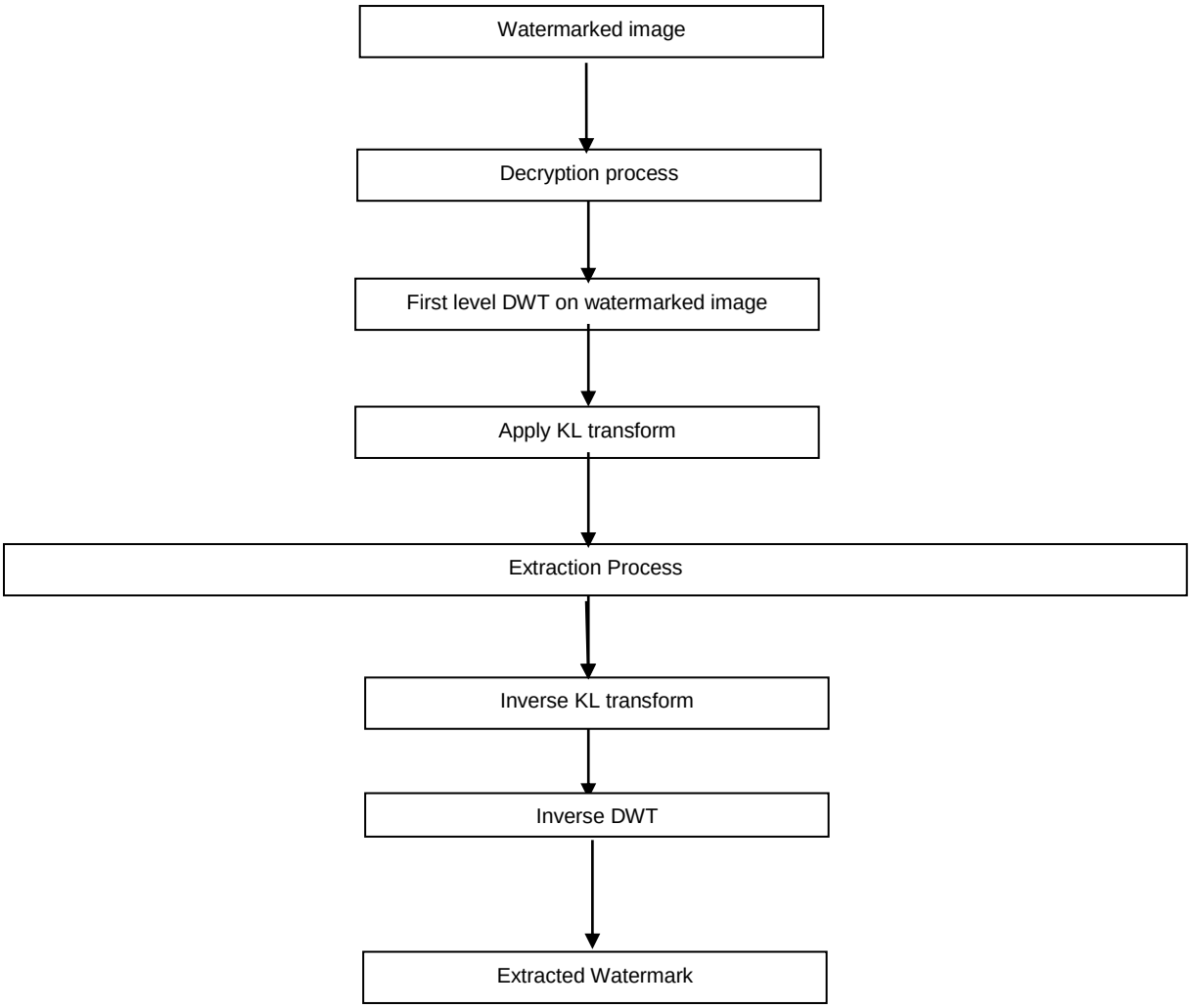

Fig 7: Implementation of the proposed solution (Extraction)

Fig 7 depicts the extraction process that is done at the receiver's end to get back the extracted watermark. As shown in the Fig 6, the embedding process involves the fusion of DWT, KL transform. After embedding process the image is possibly distorted, the distorted image is In order to enhanced the visual quality of the watermarked image and reduce the bandwidth requirements, different de-noising dictionary based method is applied on the image. It is noticed that adaptive based dictionary method is better than DCT and Global dictionary method.

Step 1: On the first step we have applied the one level DWT on the original and watermark image. Watermark image and the cover image are 512 * 512 gray scale images.

Fig 8 Original Image(Lena.jpg)

Fig 9 Watermark Image(Peppers.jpg)

Step2: One level DWT is applied to each image dividing the image into 4 segments LL, LH, HL, HH band. DWT can be considered as wavelet transform that symbolizes any signal as a set of approximation and detail coefficients.

Following code is being implemented for converting the images to one level DWT

```
% Applying DWT on cover image
i=imread('lena.jpg');
sX=size(i);
[LL,LH,HL,HH]=dwt2(i,'db1');
% Applying DWT on watermark
j=imread('peppers.jpg');
sX=size(j);
[WLL,WLH,WHL,WHH]=dwt2(j,'db1');
```

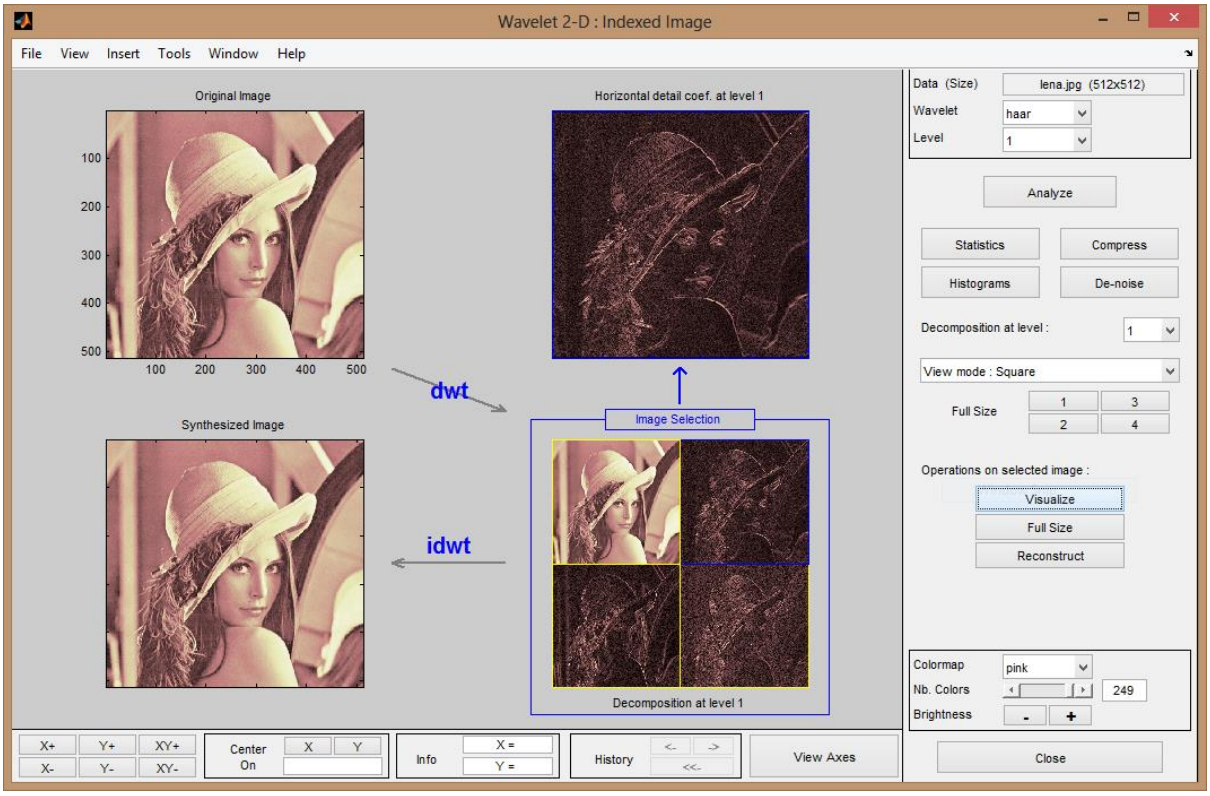

Fig 10: 1 level DWT on cover image (lena.jpg)

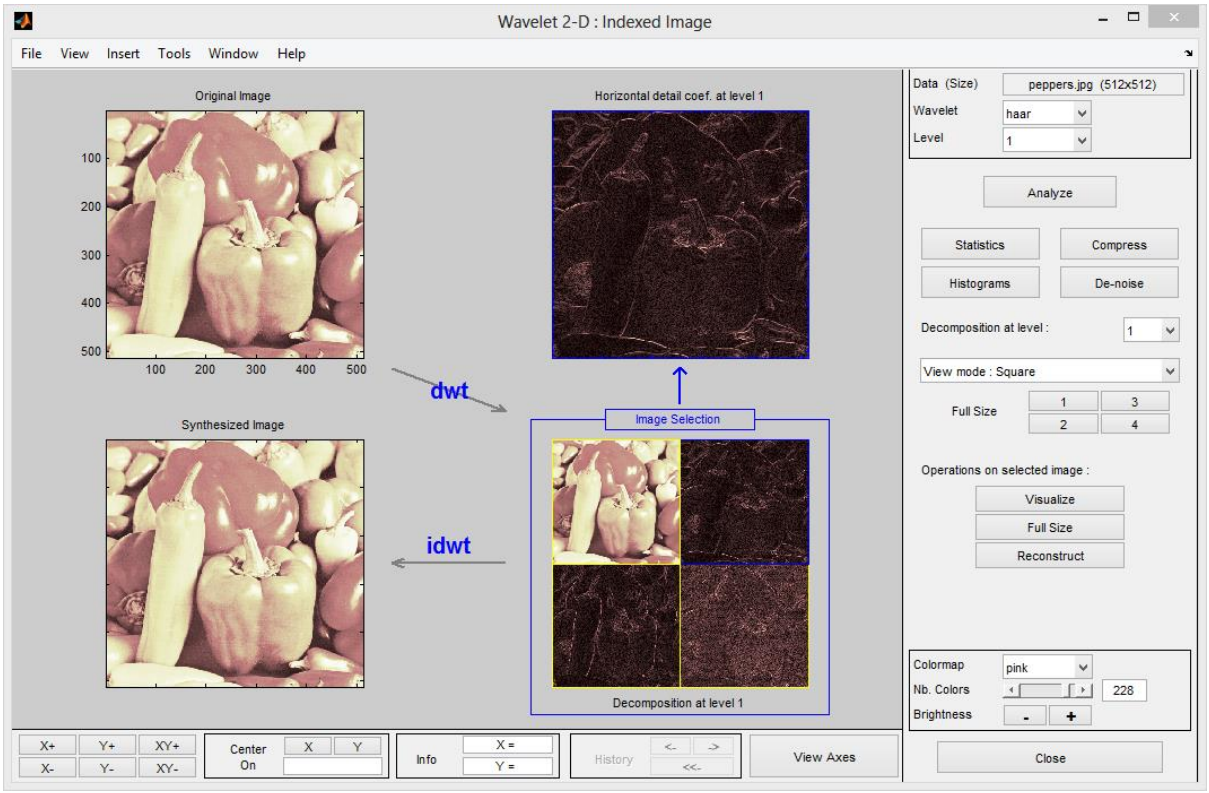

Fig 11: 1 level DWT on watermark image (peppers.jpg)

Step 3: KL transform is applied to the LH band of the cover image. A = imread(filename, fmt) reads a grayscale or color image from the file specified by the string filename. If the file is not in the current folder, or in a folder on the MATLAB path, specify the full pathname. The text string fmt specifies the format of the file by its standard file extension.

```
% applying KL transform on LH band
I=LH;
I=im2double(I);
m=1;
%finding eigen vectors
% making transformed image
          for x=0:7
                for  y=0:7
                    transformed_img(i+x,j+y)=trans_img1(x+1,y+1);
                end
            end
```

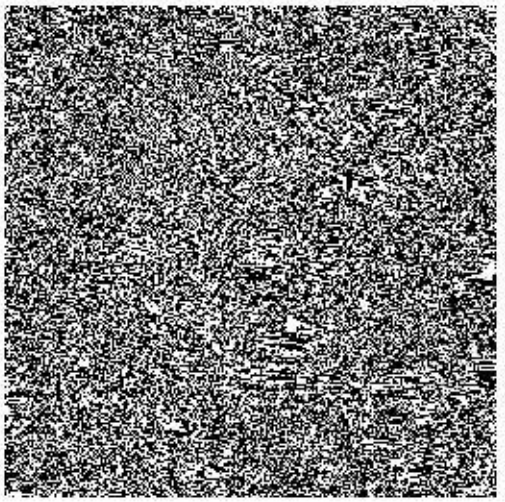

Fig 12: Transformed Image (KL transform)

Step 4: Watermark embedding is done at gain 0.4.

```
%watermarking
newhost_LL = LL + (0.04*WLL);

% new watermarked image
rgb2=idwt2(newhost_LL,transformed_img,HL,HH,'haar');
```

Fig 13: Possibly distorted image

Step 5: Image denoising is performed on the watermarked image. Various denoising techniques are used such as DCT dictionary, Global dictionary and KSVD. Afterwards, the PSNR values are checked.

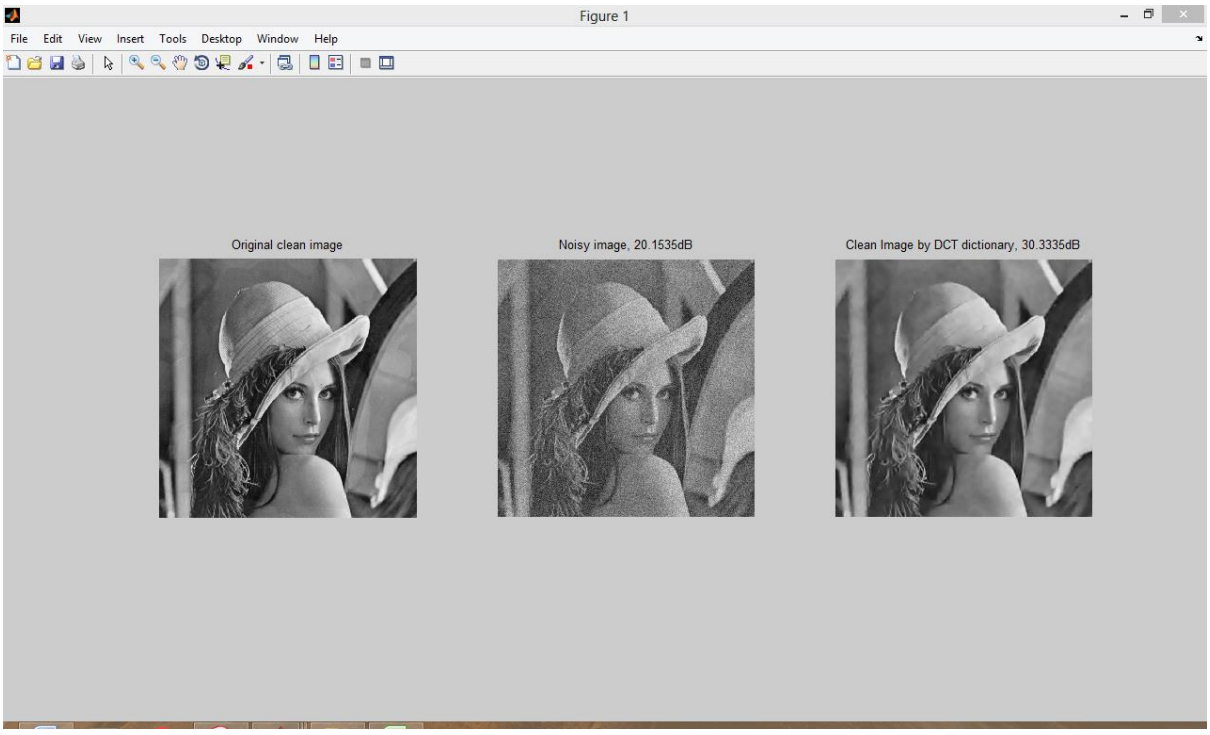

Fig 14: Image denoising using DCT dictionary

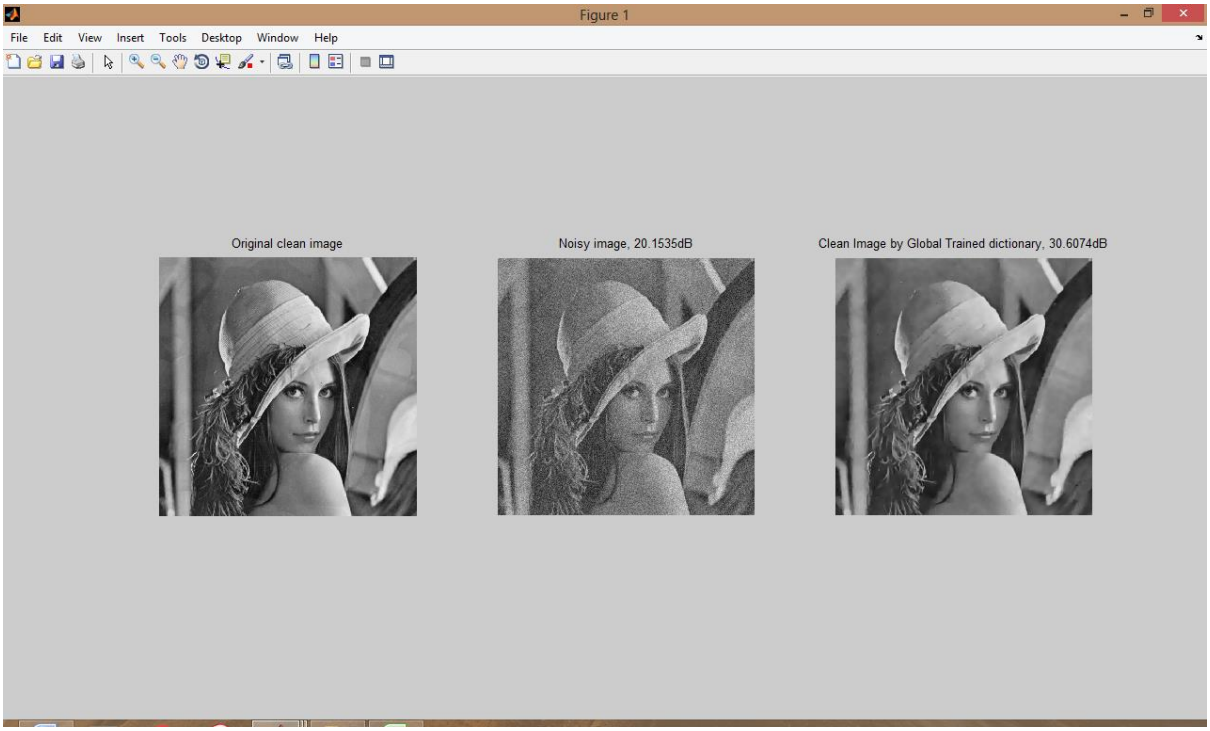

Fig 15: Image denoising using the Global trained dictionary

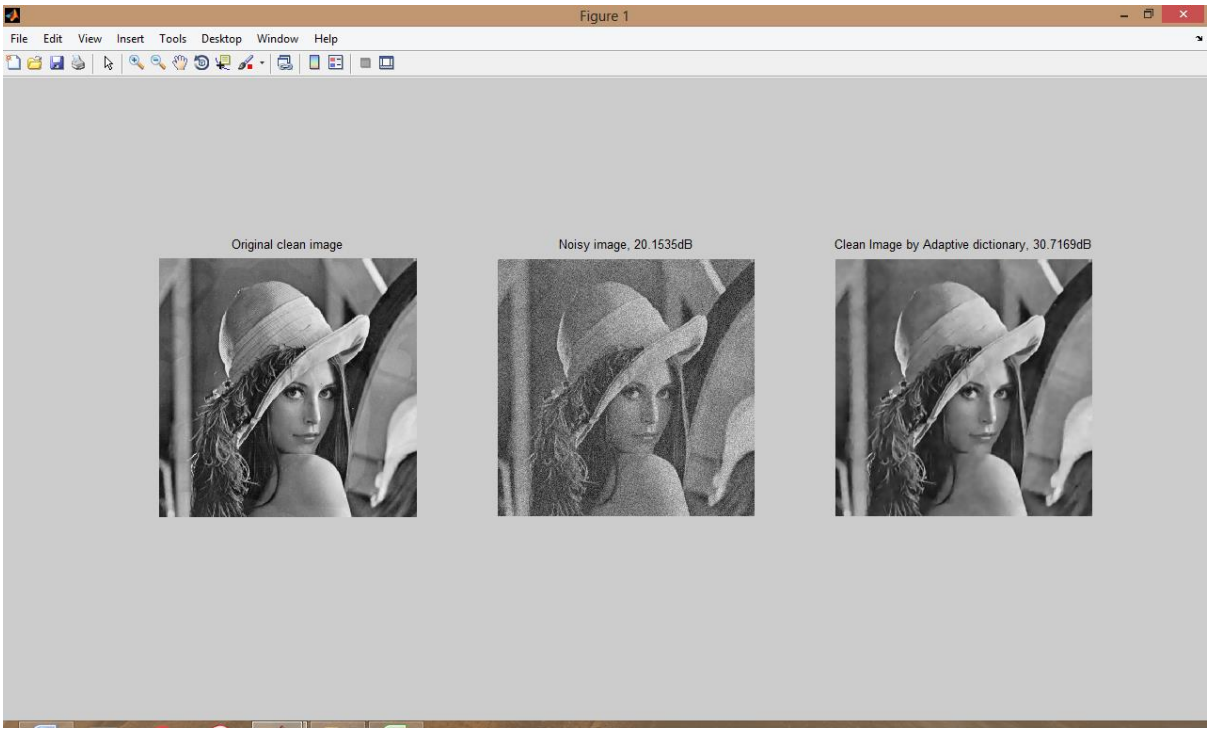

Fig 16: Image denoising using KSVD

Step 6: After performing the image denoising, the resultant image have improved PSNR value.

Fig 17: Denoised Image

Step 7: Inverse KL transform is being applied to the LH band of the cover image for the watermark extraction

```
for x=0:7
   for  y=0:7
      inv_transformed_img(i+x,j+y)=inv_trans_img(x+1,y+1);
   end
end
```

Fig 18: Inverse KL transformed image

Step 8: Inversing the encryption process performed on the watermarked image to prevent it from tempering from unauthenticated third party.

Step 9: Watermarking extraction is performed.

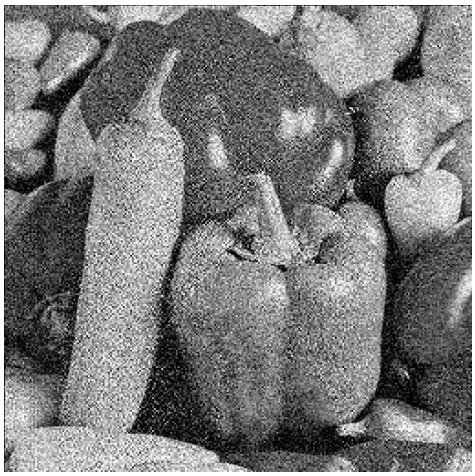

Fig 19: Extracted watermark (Ewatermark.jpg)

3.3 Experimental Results and analysis

a) Peak to Signal Ratio (PSNR)

It is utilized to quantify the intangibility of a watermarked picture, i.e. closeness between the first picture and watermarked picture. It can likewise be utilized to contrast unique watermark and the removed watermark. It is communicated as quality measure. Higher the PSNR esteem higher is the security. It itself utilizes Mean Square Blunder (MSE) for its calculation.Larger peak signal-to-noise ratio (PSNR) [20] between cover and watermarked image indicates that the watermarked image more closely resembles the cover image resulting into imperceptible watermarking. Generally, watermarked image with PSNR value>27 dB is acceptable. PSNR is defined as

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

where the mean square error (MSE) is defined as

$$MSE = \frac{1}{X * Y} \sum_{i=1}^{X} \sum_{j=1}^{Y} \left(I_{ij} - W_{ij}\right)^2$$

where I_{ij} a pixel of the original is image of size X *Y and W_{ij} is a pixel of the watermarked image of size X * Y.

b) Normalized Cross Correlation

The normalized cross correlation (NCC) is utilized to quantify the closeness between the cover picture and the watermarked picture and also unique watermark and recouped watermark. Higher the estimation of NCC will bring about better method.

The similarity and differences between original watermark and extracted watermark is measured by the normalized correlation (NC). Its value is generally 0 to 1. Ideally it should be 1 but the value 0.7 is acceptable [20].

$$NC = \frac{\sum_{i=1}^{X}\sum_{j=1}^{Y}(W_{originalij} * W_{recoveredij})}{\sum_{i=1}^{X}\sum_{j=1}^{Y}W_{originalij}^{2}}$$

where Worignalij is a pixel of the original watermark of size X × Y and Wrecoveredij is a pixel of the recovered watermark of size X ×Y.

The above procedure is implemented for the fixed cover 512 * 512 cover image but variable watermark size of gray scale, so the following table is inferred. Table 3 show the inferred PSNR, MSE and NC value.

Table 3: Fixed gain (0.04), variable watermark size

WATERMARK SIZE	**PSNR**	**MSE**	**NC**
256 * 256	28.98	82.8	0.9511
128 * 128	28.47	93.16	0.895
64 * 64	30.16	63.17	0.9834

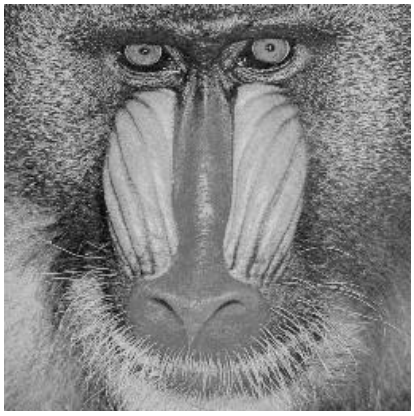

Fig: 20 Watermark image (256 * 256)

Fig: 21 Watermark image (128 * 128)

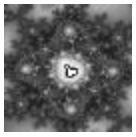

Fig: 22 Watermark image (64 * 64)

Table 4 shows when the KL transform is applied to the various bands LL, LH,HL and HH of cover image. The resultant PSNR, MSE, and NC value

Table 4: Fixed gain(0.04), variable bands

Bands	**PSNR**	**NC**
LL	9.46	0.23
LH	29.38	0.931
HL	27.7	0.952
HH	31.39	0.9411

.

Table 5 shows when the gain was varied, so what was the corresponding PSNR, MSE, NC value and when the image is Denoised using the DCT dictionary, global dictionary and adaptive dictionary.

Table 5: Variable gain

Gain	**PSNR**	**NC**	**MSE**	**PSNR WITH DCT DICITIONARY**	**PSNR WITH GLOBAL DICITIONARY**	**PSNR WITH KSVD**
0.1	24.75	1	219.74	30.32	30.59	30.72
0.09	25.44	0.991	187.19	30.34	30.59	30.73
0.08	26.18	0.993	157.82	30.38	30.64	30.77
0.07	26.96	0.979	132.01	30.37	30.64	30.76
0.06	27.75	0.956	109.09	30.383	30.63	30.77
0.05	28.57	0.953	91.01	30.328	30.58	30.7
0.04	29.38	0.931	75.58	30.33	30.61	30.71

Table 6 show the NC performance of the proposed technique for different attacks. Referring this table it is observed that the NC value always be greater than 0.9437.

Table 6: NC performance against attacks at gain = 0.1

Attack	**NC value**
Speckle noise at different intensity level:	
0.01	0.9868
0.02	0.9800
0.03	0.9761
0.04	0.9719
Salt and pepper noise at different intensity level:	
0.01	0.9888
0.02	0.9859
0.03	0.9827
0.04	0.9792
Poisson noise	0.9871
Gaussian noise with mean = 0 and different variance	
0.01	0.9594
0.02	0.9437
Gaussian noise with mean = 0.002 and different variance	
0.01	0.9582
0.02	0.9457

Speckle noise affects the edge and local details of the image. The default value of v in matlab is 0.04

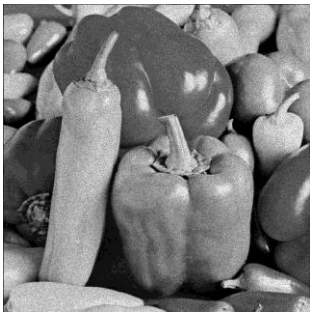

Fig 23: Watermark image (v =0.01)

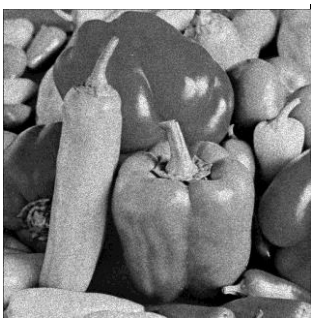

Fig 24: Watermark image (v= 0.02)

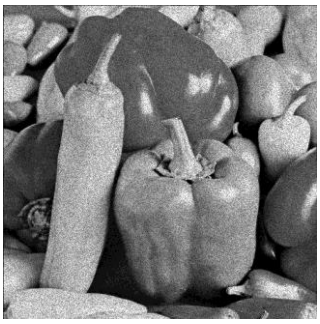

Fig 25: Watermark image (v=0.03)

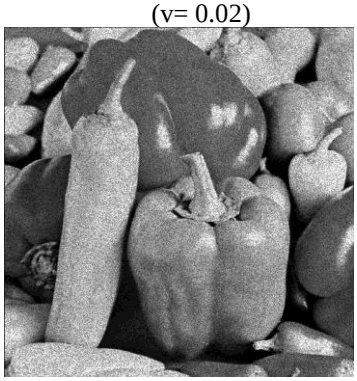

Fig 26: Watermark Image (v = 0.04)

In fig 27 the speckle noise is applied on the 256 * 256 gray scale watermark image. Table 7 shows the resultant PSNR and MSE values.

Table 7: Speckle noise on Watermark image (with fixed gain 0.04) when applied on watermark (256 * 256)

Value of v (Multiplicative Noise)	**NC**
0.01	0.993
0.02	0.988
0.03	0.983
0.04	0.981

Highest value of NC is found 0.993 at value of v 0.01

Fig 27: Watermark image (v =0.01)

Fig 28: Watermark image (v= 0.02)

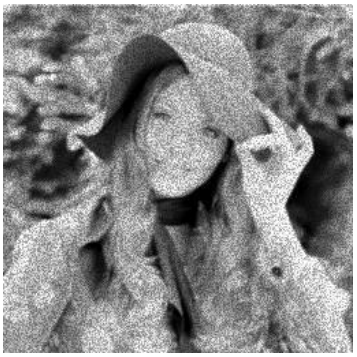

Fig 29: Watermark image (v=0.03)

Fig 30 : Watermark image (v=0.04)

In the salt and pepper noise black and white dots appear on the source image. The main cause of this type of noise is use of overheated faulty components at time of image acquisition. In Fig 31 the salt and pepper noise is applied to the watermark image with the noise intensity of 0.01.The experiment is performed on fixed gain of 0.04.

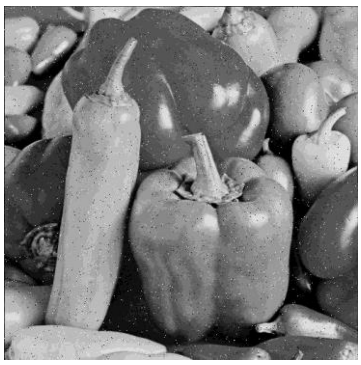

Fig 31: Watermark image
(d=0.01)

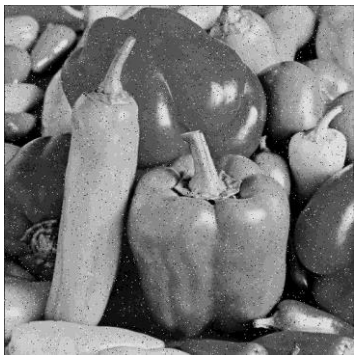

Fig 32: Watermark Image
(d=0.02)

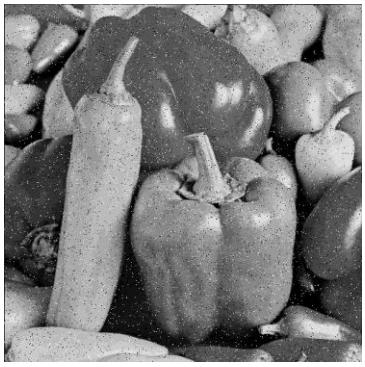

Fig 33: Watermark Image
(d=0.03)

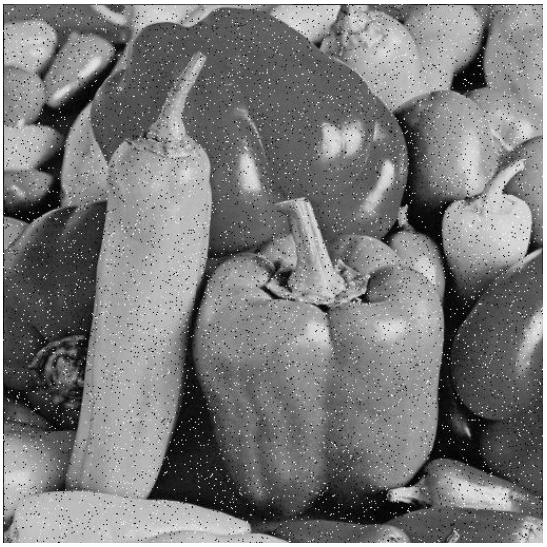

Fig 34: Watermarked Image
(d=0.04)

In fig 35, the Gaussian noise is applied in the image. This type of the noise is additive in nature and it follows the Gaussian distribution.

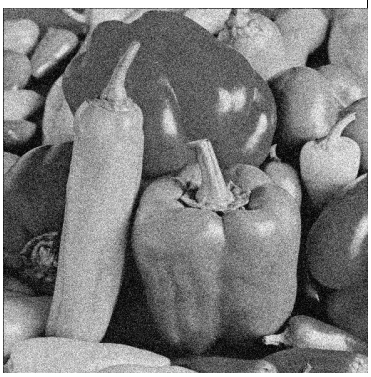

Fig 35: Gaussian noise on watermarked image
(Mean =0, Variance=0.01)

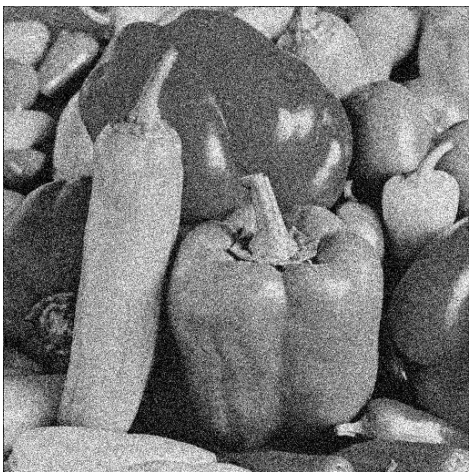

Fig 36 : Gaussian noise on watermarked image
(Mean =0, Variance=0.02)

CHAPTER 4

Study of Techniques and Simulation Tool Used for the Proposed Technique

4.1 DWT

The discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. It captures both location and frequency information unlike DFT which have only frequency information. In dwt we enter the code in the maximum information filed. Actually in entering the code we need a grey level image and we divide the code (image) into number of small frames by formula 4^n where n is number of frame, and the frame used is an i- frame, because details of i frame is not lost in case of any compression. One of the primary tasks in computer vision is to extract features (point, line, edges) from an image or a sequence of images. Fourier transform offer a shaped fine-tuned rectangle that only refers to the frequency domain. Conventional wavelets offer shape transmuting attributes but are fine-tuned windows. Wavelets offer poor directionality. Wavelets only do well at point singularities and ignore the geometric properties. Utilizing error rectifying codes, the watermarking algorithms are designed to be robust against intentional or unintentional attacks such as JPEG compression, additive white Gaussian noise, low pass filter and color attacks (hue, saturation and effulgence modifications)[32]. Media encryption obviates media content from leakage by encoding multimedia data into unintelligible form, which forfend media data's confidentiality during the process of transmission, storage, etc [33] The inhibition of multimedia encryption is that once the multimedia data is decrypted, there is no way for content owner to obviate illicit replication, reproduction, or distribution of multimedia content. Quantum watermarking is a technique which embeds the invisible quantum signal such as the owner’s identification into quantum multimedia data (such as audio, video and image) for copyright aegis [34].

4.2 **Distribution and Attacks:**

The transmission media can realize some incident in the banner recommending in a hurt substance. These ambushes may be consider or accidental. Ponder attacks use

each open resource for destroy or adjust the watermark making it hard to focus it, the techniques by and large used are: banner planning systems, cryptanalysis, steganalysis. On the other hand, coincidental strikes are unavoidable, in light of the way that each photo taking care of or transmission racket may exhibit twisting [10].

These assaults are named takes after:-

a) **Simple Attacks**: These attacks change the information of the cover picture without endeavoring to focus on the watermark area. Case: Noise expansion, trimming, change to simple and wavelet-based pressure.
b) **Disabling Attacks**: The objective of these attacks is to endeavor to break the connection between's the watermark and the cover picture, making extraction unimaginable. Case: Geometric bends, pivot, trimming and inclusion of pixels.
c) **Ambiguity Attacks**: These attacks confound the receptor installing a fake watermark, making it difficult to find which the first implanted stamp in the cover picture was.
d) **Removal Attacks**: In this type of an investigation of the watermark is done, assessing the watermark substance and endeavoring to separate it from the host picture. Case: Certain non-direct channel operations and assaults custom-made to a particular watermark calculation.

4.3 About MATLAB

Short for matrix laboratory" developing MATLAB in the late 1970s by Cleve Moler, the chairperson of the computer science department at the University of New Mexico. He give the entrance to the two understudies LINPACK and EISPACK without them learning FORTRAN. MATLAB soon spread to different colleges and found a solid gathering of people and individuals inside the connected arithmetic group. These revised libraries were known as JACKPAC. In 2000, MATLAB was changed to utilize a more current arrangement of libraries for framework control. MATLAB used in various fields of education, in particular associated with the linear algebra and various mathematical and as well as numerical operations of mathematics.

MATLAB code sometimes called M –code or simply M. The simple way is to execute MATLAB is to type at the prompt >>, in the command window, one of the elements in the desktop. In this way MATLAB can be used as an interactive mathematical or programming shell.

There are various windows in MATLAB

a) Editor window

b) Command window

c) Command history

d) Workspace

e) Command history

Editor window is used for coding command window to display output and Command window is used to display output.

Table 8.Commands for managing Variable

Command	**Description**
clear	Removes all variables from the memory.
clear x, y, z	Clears/removes only variables **x, y** and **z** from the memory.
Who	Lists the variables currently in the workspace

In matlab, Image Processing Toolbox provides a comprehensive set of reference-standard algorithms and graphical tools for image processing, analysis, visualization, and algorithm development. You can perform image enhancement, image deblurring, feature detection, noise reduction, image segmentation, spatial transformations, and image registration. Many toolbox functions are multithreaded to take advantage of multicore and multiprocessor computer. The basic data structure in MATLAB is the array, an ordered set of real or complex elements. This object is naturally suited to the representation of images, real-valued ordered sets of color or intensity data. MATLAB stores most images as two-dimensional arrays (i.e., matrices), in which each element of the matrix corresponds to a single pixel in the displayed image. (Pixel is derived from picture element and usually denotes a single dot on a computer display.) For example, an image composed of 200 rows and 300 columns of different colored dots would be stored in MATLAB as a 200-by-300 matrix.

CHAPTER 5

Conclusion and Future Directions

The research reported in the work shows that sundry author's have proposed fusion of sundry techniques for efficacious data distribution over the unsafe media. The participants in the experimental research significantly inspirited the research student's motivation to learn the sundry techniques for securing the authenticity of the digital media. The result of present study additionally substantiated that there are numerous emerging implements that rectify the drawback of one and another. The objective of the study of sundry experimentalists remains the same that is to obviate the digital media from being comprised. The author additionally proposed the technique for robust and secure digital document transfer for the application of the E- Governance and endeavored to make the optimal balance between the major benchmark such as imperceptibility, robustness and capacity. The purpose of combined DWT-KLT is to improve the robustness of the watermark at acceptable visual quality of the watermarked image which is the prime objective of the research. However, it may have increased the computational complexity to some extent which needs to be investigated separately. The computational complexity of the proposed watermarking method can be minimized by selecting and exploring the other wavelet instead of DWT

Chapter 1 presents the basic concepts of watermarking and their importance in recent applications and characteristics of watermarking system. Watermarking techniques are divided into spatial and transform domain techniques. Various spatial, transform domain techniques are described briefly in this chapter.

Chapter 2 presents the state-of-the-art watermarking methods and compares the performance of some recent techniques in tabular form.

In chapter 3, we have proposed a watermarking algorithm based on Wavelet and KL transform for robust watermarking scheme. The performance of the method is tested in terms of PSNR and NC. The method is also robust for different attacks.

The introduction of techniques and simulation tool (MATLAB) and its important functions are presented in Chapter 4.

Conclusion and future directions of the work is presented in Chapter 5.

In future, the performance of the method can also be improved with directional transform techniques, different error correction codes, and machine learning/GAs. In addition, the robustness performance of the method can also be determined with standard benchmark software.

REFERENCES

[1] Palak Mahajan, "Steganography: A Data Hiding Technique", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, Issue 11, November 2014.

[2] Ramadhan Mstafa, Christian Bach, "Information Hiding in Images Using Steganography Techniques", 2013 ASEE Northeast Section Conference, March 14-16, 2013.

[3] Ruchika Patel, Parth Bhatt, "A Review Paper on Digital Watermarking and its Techniques", International Journal of Computer Applications (0975 – 8887) vol. 110, No. 1, January 2015

[4] Manmeet Kaur, Kamna Mahajan, "An Existential Review on Text Watermarking Techniques", International Journal of Computer Applications (0975 – 8887) vol. 120, No.18, June 2015.

[5] Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science, 2007

[6] Mehdi Khalili, "A secure and robust CDMA digital image watermarking algorithm based on DWT2, YIQ color space and Arnold transform", Signal & Image Processing : An International Journal (SIPIJ) vol. 2, No.2, June 2011.

[7] Hong Shen, Bo Chen, "From single watermark to dual watermark: A new approach for image watermarking", Computer and Electric engineering, vol. 38, pp. 1310-13124, 17 November 2011

[8] Gaurav Bhatnagar, Q.M. Jonathan Wu, Balasubramanian Raman, "A new robust adjustable watermarking scheme", Computers & Security, vol.:31, pp. 40-58, 2011

[9] Muhmmad Arslan, Sana Ambreen Malik, Asifullah Khan, "Intelligent reversible watermarking in integer wavelet domain for medical images",Journal of Systems and Software, vol.: 85, Issue 4, pp. 883–894, April 2012

[10] Dalel Bouslimi , Gouenou Coatrieux , Christian Roux, " A joint encryption encryption/ watermarking algorithm for verifying the reliability of medical images : Application to echographic images",Computer Methods and Programs in Biomedicine vol.106, pp.47-54,2011

[11]Ju Lei, Sui Zhiyuanb , Chi Yapinga, Fang Yong ,"A Haar Wavelet Transform Based Watermarking Algorithm for Binary Images",International Conference on Computer and Electrical Engineering, vol.13, pp.2972-2978,2011

[12] Didi Rosiyadi, Shi-Jinn Horng,Pingzhi Fan, Xian Wang, Muhammad Khurram Khan, Pan Yi, "An Efficient copyright protection scheme for e- government document images", in IEEE MultiMedia vol.19, Issue:3, pp.62-73, July-Sept. 2012

[13]Gaurav Bhatnagar, Q.M. Jonathan Wu, Balasubramanian Raman, "Robust Gray Scale watermarking in wavelet domain", in Special issue on Recent Advances in Security and Privacy in Distributed Communications and Image processing vol.38, Issue:5, pp.1164–1176,2012

[14]Jun Lang, Jin-ying Sun, "Digital Watermarking Algorithm Based on Hyperchaos and Fractional Fourier Transform", IEEE 14th International Conference on Communication Technology (ICCT), Chengdu, China, pp.691-694, 2012

[15] Shi-Jinn Horng, Didi Rosiyadi, Tianrui Li, Terano Takao, Minyi Guo, Muhammad Khurram Khan, "A blind image copyright protection scheme for e-government", in Journal of Visual Communication and Image Representation, vol.24, Issue:7, pp.1099-1105, Elsevier, 9 July 2013

[16] Peyman Rahmati,Andy Adler,Thomas Tran "Watermarking in E-commerce" in (IJACSA) International Journal of Advanced Computer Science and Applications, vol.4, no:6, 2013

[17] Ali Al-Haj, Alaa' Amer,"Secured Telemedicine Using Region-Based Watermarking with Tamper Localization", Journal of digital imaging, vol. 27, pp. 737–750, May 2014

[18]A. Kannammal, S. Subha Rani, "Two Level Security for Medical Images Using Watermarking/Encryption Algorithms", in International Journal of Imaging Systems and Technology, vol.24, Issue:1, pp.111–120, March 2014

[19] A K Singh, B Kumar M Dave and A Mohan "Robust and Imperceptible Dual Watermarking for Telemedicine Applications" in Wireless Personal Communications, Springer, vol.80, Issue:4, pp.1415-1433, 2014

[20]. A K Singh, M Dave and A Mohan Multilevel Encrypted Text Watermarking on Medical Images using Spread-Spectrum in DWT Domain, Wireless Personal Communications, vol. 83, Issue 3, pp. 2133–2150, 2015

[21] Lei Chen, Jiying Zhao, "Robust Contourlet-Based Watermarking for Depth-Image-Based Rendering 3D Images", IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Nara, Japan, ISSN: 2155-5052, 2015

[22] Eduardo Fragoso-Navarro, Héctor Santoyo-García, Kevin Rangel-Espinoza, Mariko Nakano-Miyatake, Rogelio Reyes-Reyes, "Visible Watermarking Technique in Compressed Domain Based on JND", in International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE), Mexico, City. Mexico, pp:1-6, IEEE,2015

[23] Jian Cao, Haodong Li, Weiqi Luo, Jiwu Huang "An Improved Spread Transform Dither Modulation for Robust and Secure Watermarking", vol.24, Issue:2, pp.2718-2722, IEEE 2016.

[24]Yevhen Zolotavkin ,Martti Juhola, "A New Scalar Quantization Method for Digital Image Watermarking" ,Journal of Electrical and Computer Engineering,vol.2016 Article ID 9029745, 16 pages , 2016

[25] Fuping Wang ,Jan P. Allebach, "Printed Image Watermarking using Direct Binary Search Halftoning", IEEE International Conference OF Image Processing (ICIP), Phoenix, AZ, USA,ISSN: 2381-8549, IEEE 2016

[26] Dhekra ESSAIDANI, Hassene SEDDIK, Ezzedine BEN BRAIEK, "Robust and Blind Watermarking Approach Based on Modified Delaunay Triangulation" , 2nd International Conference on Advanced Technologies for Signal and Image Processing - ATSIP'2016 , Monastir, Tunisia, March 21-24, 2016.

[27] Abhilasha Sharma, Amit Kumar Singh & Satya Prakash Ghrera, "Robust and Secure Multiple Watermarking for Medical Images", Wireless Personal Communications , pp 1–14 Science Business Media New York 2016.

[28] Michael Elad and Michal Aharon, “Image Denoising Via Sparse and Redundant Representations Over Learned Dictionaries”, IEEE Transcations on image processing, vol. 15, No. 12, December 2006

[29] DING Wei , YAN Weiqi and QI Dongxu, “Digital Image Watermarking Based on Discrete Wavelet Transform”, Journal Computer Science & Technology, vol. 17 No.2 March 2002

[30] Fengxiang JIN , Shifeng DING, “Analysis and Application of K-L Transform Information Features”, FIG Working Week , Paris, France, April 13-17, 2003

[31] Osama S. Faragallah, “Transmission of DWT Block-Based KLT Watermarked Images Through MC-CDMA Wireless Channel”, Journal Wireless Personal Communications : An international Journal, vol. 90, issue 3,Pages 1387 -1404 October 2016,

[32] Wadood Abdul, Philippe Carré and Philippe Gaborit, “Error correcting codes for robust color wavelet watermarking”, URASIP Journal on Information Security,2013

[33] A. M. Riad , Reham R. Mostafa and Rasha elhadry, “A commutative Encryption and Watermarking (CEW) scheme for JPEG2000 compression standard” , International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 3, Issue 4, ISSN 2278-6856 ,July-August 2014

[34] Shahrokh Heidari, Mosayeb Naseri, “A Novel LSB Based Quantum Watermarking”, International Journal of Theoretical Physics , vol.39, pp.10, 2016