Analysis of Image Security Techniques using Digital Image Watermarking in Spatial Domain

Rachana V.Mahule
MCA Department,
P.R.P.C.E.M,
Amravati (M.S.) India.

Chitra A. Dhawale, PhD
MCA Department,
P.R.P.C.E.M,
Amravati (M.S.) India.

ABSTRACT
Digital watermarking is the process of hiding the important digital information into another one. There are three main watermarking techniques, Digital image watermarking, digital audio watermarking and digital video watermarking. Watermarking can be done majorly in two domains, Spatial Domain and Frequency Domain. This paper is analysis of Digital image watermarking and different techniques used for digital image watermarking in Spatial Domain based on LSB-Based, Statistical-Based, Feature-Based and Block-Based.

General Terms
Watermarking Classification, Image Watermarking Techniques in spatial domain, Improvement Image Security and Robustness using various watermarking methods.

Keywords
Digital image watermarking, Spatial Domain, LSB, Feature-based, Statistical-Based, Blocked-Based, Robustness, Security.

1. INTRODUCTION
Multimedia data like text, images, audio, video are traveling widely and rapidly through email and across the Internet to the destinations. Security of such data is a today‘s essential need. Security means protecting the data against the illegal copying, tempering and modifications. There are several techniques to protect the different types of digital data which include Fingerprinting, Cryptography, Steganography and Watermarking.

Fingerprinting uses some kind of hash functions to create fingerprint, original file remain intact. Cryptography is about protecting the document and to maintain data confidentiality, data Integrity, Authentication and Access control .Cryptography is study of encryption principles/methods. There are two types of encryption techniques Private Key (Symmetric) encryption and Public Key (Asymmetric) Encryption. Steganography is about hiding users data into another format like text, images, audio , video . Watermarking is one of the steganographic techniques. Watermarking is about robustness against possible attacks, Watermark need not be hidden. Watermarking can be applied to Images, Text, Video, Audio or Software. The Digital Image watermarking is a technique to insert a Digital Signal or pattern into a digital image.

2. GENERAL WATERMARKING SYSTEM
The general process in watermarking is illustrated in Figure 1[1]. The system consists of three processes, Embedding (Encode), Data across the network (Transmission) and Extraction (Decode). The first process started at the source side. The data you want to hide and transmit is called as” watermark” may be encoded into the original data using Insertion Algorithms and a specific key. The key may be private key or public key depending on the type of encryption. This key is used to encrypt the watermark as an additional protection level. The output of the embedding process is the watermarked image .This image is then transmitted to the destination. Now data is across the network, the watermarked image may be subjected to unauthorized access and a modification i.e. attacks either deliberately or due to transmission error or noise. Therefore, the recipient may or may not receive the exact original data as that sent by the transmitter. This data need to be decoded to extract the watermarked image. When the original data is needed in the extraction process which is the third process of this model then it is called a blind technique .In the extraction process the watermark and the original data is separated by using Extraction algorithm and again the specific key.

3. CLASSIFICATION OF DIGITAL WATERMARKING TECHNIQUES
The figure 2 shows brief classification of digital watermarking techniques. The digital image watermarking is basically divided according to working domain and Human Perception. According to Human perception the inserted watermark may be visible, invisible or may have partial property ‘dual’. Logos and paper watermarks are the example of visible watermark. The invisible watermarking includes three properties robust, fragile and semi fragile.[3] A digital watermark is called "fragile" if it fails to be detectable after the slightest modification. Fragile watermarks are commonly used for tamper detection (integrity proof). Modifications to an original work that clearly are noticeable commonly are not referred to as watermarks, but as generalized barcodes .A digital watermark is called semi-fragile if it resists benign transformations, but fails detection after malignant transformations. Semi-fragile watermarks commonly are used to detect malignant transformations. A digital watermark is called robust if it resists a designated class of transformations. Robust watermarks may be used in copy protection applications to carry copy and no access control information. It is divided into four major categories Private, Semi Private, Public and Asymmetric.

According to working domain watermarking has two major areas; the first is Spatial Domain and second is Frequency Domain. Spatial domain we deal with each pixel of the image .The value of pixel change with respect to scene. It directly inserts raw data into the image pixel. Whereas in frequency domain, we deal with the rate at which the pixel values are changing in spatial domain. In this domain the image is processed with different transformations like Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete wavelet-Based Transform(DWT) etc. It is also called as ‘Transform Domain’. The comparison between spatial domain and frequency domain is given in Table-1[4]

The watermarking in Spatial Domain is generally based on some approaches like LSB, Statistical-Based, Feature-Based and Blocked Based. Most of the techniques are proposed depending on these or combination of these approaches.

In LSB (Least Significant Bit)-Based image watermarking the Least Significant Bits of original image pixels are replace by the watermark information .The original image may be Binary, Line drawings, cartoons, maps, Gray scale or RGB images. The watermark may be Binary data , Text, Logo, Digital Signature, Message Digest, or any type of image like Binary, Gray or RGB. Different methods are proposed for LSB which uses one or the combination of bits. Appearance of Watermarked image depends on the position of the replaced bits.

Feature-Based image watermarking is used to find feasible matches between image features and watermark features. The first step in Feature based watermarking is feature point detection. The applicable watermark is constructed by appropriate watermarking algorithm. This watermark is then embedded in the cover image at detected feature point. At destination the watermark detection process is carried out .Correlation between Cover image and watermark is detected. This type of watermarking is use to check different attacks on the watermarked images and robustness.

Statistical Based image watermarking is again generally used to improve the robustness of the image watermarking. Some statistical methods are applied on the original image and the watermark image. Then find out the differences and identify the attacks done on these images.

Blocked based digital image watermarking is used to include more complexity for the opponent. The original image is divided into blocks. Apply different methods to embed the watermark in this Blocked image.

Table 2. Shows few techniques (methods) that gives idea about the Spatial Domain Digital image watermarking.

3.1 Previous work

3.1.1 LSB Based-Digital Image Watermarking

3.1.1.1 Amit Singh [6] proposed the digital image watermarking method by replacing the second Least significant bit(LSB) with inverse LBS. The original (cover) image used is RGB or grayscale .The watermark image may be gray scale or RGB. If it is RGB image it should be converted to gray scale using HSV model .Author first insert watermark text binary bits in LSB place and inverse of Least Significant Bit (LSB), to insert second LSB for security. After embedding second LSB option without any order. In embedding process input is Original image and watermark text and the output is Watermarked image. The proposed algorithm is flexible depending on the length of watermark text. Using simple LSB method they Improve image authentication and copyright protection.

3.1.1.2 A. Siva Sankar [16] proposed the lossless digital image watermarking for Digital Rights Managements (DRM) using polynomials .This is also the LSB-Based watermarking. The input to the embedding algorithm are secrete message (Text file) ,the host image and Pseudorandom seed generated by polynomial. First take the original image and the text file i.e. which have to embedded into original image. Then convert the text data into binary format. Binary conversion is done by taking the ASCII value of the character and converting those ASCII values into binary format and steam of bits are generated. Counter variable is taken which holds the total number of bits of message. Similarly, in cover image, bytes representing the pixels are taken in single array and byte steam is generated. Message bits are taken sequentially and then are placed in LSB bit of image byte. The index number of the image byte where replacement of LSB is to be done is controlled by polynomial equation, which is given in the key. Same procedure is followed till all the message bits are placed in image bytes. The number sequence generated by the polynomial is unique therefore identifying the image bytes where LSB encoding is done is very difficult without polynomial key. Image generated is called watermarked image. The steps are explained clearly in the paper[16].This method is lossless and robust. The use of polynomial results in high security because the hacker should try all possible combinations of keys.

3.1.1.3 Mr. Rohith.S [8] proposed the LSB-Based digital watermarking against the salt and pepper noise using simple error control coding technique. The encoded watermark is inserted into cover image by using the repetition codes. Watermarking is applied on gray scale image and the watermark is binary text pattern. This method is simple and more robust for salt and pepper noise attack.

3.1.2 Blocked-Based Digital Image Watermarking

3.1.2.1 Most of the watermarking methods are fragile. Ying Zhang [5] proposed the fragile watermarking algorithm with side information for high security. This method is Block-Based .The original gray scale image is segmented into blocks. The logo as watermark is also divided into blocks i.e. subsections. The previous watermarking subsection is considered as side information, and the current watermarking subsection is treated according to XOR algorithm by using the side information Calculate the embedding position of watermark with side information. Before embedded, the image is considered as side information and the embedding position is calculated according to the mathematical thought of Hill Cipher algorithm by using the side information. The watermark is embedded by using LSB algorithm.

3.1.2.2 Mehmet Utku Celik [9] proposed the block based hierarchical watermarking .Author propose a hierarchical modification of Wong's scheme. A hierarchical block-based watermarking technique inserts and extracts a watermark in a multilevel hierarchy. The original image may be Gray scale or RGB and the watermark may be Digital signature, Binary image or logo. The Figure 3 shows how watermark information is inserted into each block of original image. For the private key version, author use a 64 bit MAC (message authentication code) based on MD5 algorithm as a digital signature, and for the public key version the 320 bit DSA (digital signature algorithm) is employed.

3.1.2.3 M.Venkatesan [7] proposed a secure authentication watermarking for binary images using pattern matching (SAWT-PM).It provides high authentication to the binary images. It is one of the fragile watermarking techniques. The original image is partitioned into m × n sub blocks (say 3 × 3). In each sub block only the middle pixel is used to hide the information. Each 3 × 3 sub-block is checked against predefined patterns. If a sub-block matches with any of the valid patterns, it is ready to hide the information. It is referred as Ready Block, and the middle pixel of it can be used to hide the information. Figure.4 shows the predefined block pattern

used for hiding the information. This method provides security, authentication and Integrity of the image.

3.1.3Feature-Based Digital Image Watermarking

3.1.3.1 Ashwary Rajpoot [10] proposed the feature based robust digital image watermarking technique using edge feature. Here the first step is exactly dividing the image into fix size blocks. Apply Discriminant Analysis Method (DAM) to convert a gray scale image into binary image. Calculate Between-class variance (BCV) to find the edge in the block and then insert the Watermark at Edge pixels. In extraction process the watermark is extracted by using again the DAM and BCV.

3.1.3.2 Wei Wang [11] presents a novel gray-level featured based and robust image watermarking algorithm based on Singular Value Decomposition (SVD) feature and neural network is presented for copyright protection. Singular Value Decomposition (SVD) is one of the most powerful numeric analysis techniques. The method makes use of three algorithms, Embedding algorithm, Extraction algorithm and Neural Network Training. The watermark is recovered based on BPNN.

3.1.3.3. Lei-Da Li[12] proposed the geometrically robust digital image watermarking using odd–even quantization.

The first step is watermark synchronization; it is performed using Harris feature point and scale normalization. The figures 5,6,7 shows watermark synchronization, local invariant region generation and watermark extraction .The scheme is tested on to rotation, scaling, moderate translation and various signal processing attacks and is highly robust.

3.1.3.4 Wei Lu [13] demonstrates the feature based watermarking. A scale interactive model based filter is used to extract the feature points of original image, based on which a watermark template is constructed and embedded adaptively into the local region of these points. Firstly, the noise visibility function (NVF) is used to improve the robustness and imperceptibility. Figure 8 shows watermark embedding process and figure 9 shows the watermark detection process. This method is basically tested on JPEG image aiming robustness against common signal processing attacks and geometric distortions.

3.1.4 Statistical Based Digital Image Watermarking

3.1.4.1 Mir Shahriar Emami [14] used statistical based method for EISB Information Watermarking Scheme. EISB (Enhanced Intermediate Significant Bit) are not enough robust so the statistical method using L2Norm technique is used to increase the robustness of the EISB watermarking approach. Author technique is performed on different image watermarks and results in improvement in robustness of EISB watermarking scheme.

Figure 10.shows the proposed watermarking scheme.
The L2Norm is given in Eq.1.

$$L2Norm = \sqrt{\sum_{i=1}^{|L|}(Hi - Hi')^2} \qquad (1)$$

Where Hi denotes the histogram of the first image, Hi' denotes the histogram of the second image and L denotes the number of components in each of mentioned histograms. The scheme is experimented on under JPEG 2000 lossy compression attack. Almost none of the extracted watermarks could be used as proofs of ownership because they were severely attacked. However, the ownership of the watermarked images was successfully identified by utilizing the proposed approach because, in all cases, OSR were greater than 0.65.

3.1.4.2 B.Surekha [15] also used the statistical based Watermarking using Visual Secret Sharing (VSS). The proposed technique has three main advantages: Provides greater convenience in carrying and storing the intermediate images called shares; Provides high security; Reduce tradeoff between spatial and frequency domain techniques in terms of robustness. The basic VSS splits a binary secret image into two binary noise images called shares. The shares are generated in such a way that for each pixel in the secret image, a code block consisting of four sub-pixels is substituted in each of the shares using a codebook as shown in Table 3.

The inputs to the watermark hiding scheme are Original Cover image I of size (m×n), Binary watermark of size (w×h) and the output is Private share of size (w×h). Input to the watermark Extraction Phase are Cover image I' of size (m×n), Private Share of size (w×h) and the output is Extracted Watermark of size (w×h).

The proposed technique has three main advantages. 1. Since unique features of the cover image are used, it reduces the chances of false positives thereby improving the security of the watermarking scheme 2. Since a modified version of VSS called Multi-Pixel VSS (MPVSS) with no pixel expansion, is used, it is convenient to carry and store the intermediate images called shares. 3. Since the chosen feature vector depends on spatial correlation of pixels, it reduces tradeoff between spatial and frequency domain techniques in terms of robustness against range of attacks.

3.2 Figures and Tables

Table 1. Comparison between Spatial Domain and Frequency Domain[4]

Factors	Spatial domain	Frequency domain
Computation Cost	Low	High
Robustness	Fragile	More Robust
Perceptual quality	High control	Low control
Computational complexity	Low	High
Computational Time	Less	More
Capacity	High	Low
Example of Application	Mainly Authentication	Copy rights

Table 2. Some Digital image Watermarking Methods in Spatial Domain

Author	Approach	Method	Original Image used	Watermark inserted	Property (Invisible)	Results
Amit Singh[6]	LSB Based	Replacement of second LSB with Inverse LSB	Gray Scale or RGB image	Gray Scale , if RGB image convert it into Gray scale using HSV ,Text	Flexible-depends on length of watermark text	Good for Image authentication and Copyright protection
A. Siva Sankar [16]	LSB Based	Watermarking using polynomials for DRM	Windows Bitmap images	Text file	Lossless and robust	More secure , Difficult to decode image watermark for hackers
Mr. Rohith.S [8]	LSB Based	Repetition Code	Gray Scale	Binary text Patterned	Robust	Simple and robust against salt and pepper noise
Ying Zhang [5]	Blocked Based	Fragile watermarking with 'Side information'	Gray Scale image Segmented in blocks	Logo	Fragile	Idea of Cryptograph is proposed and effectively improves image security
Mehmet Utku Celik[9]	Blocked Based	Hierarchical watermarking Wong's Scheme	Gray Scale or RGB image	Digital Signature, Binary image, Logo	Public Key Fragile	Provide graceful tradeoff between security and temper localization
M.Venkatesan [7]	Blocked Based	SAWT-PM	Binary image, Line drawings, Cartoons, Maps	Message Digest of original image	Fragile	Appling security, Authentication and Integrity
Ashwary Rajpoot[10]	Feature-based	Edge feature using DAM and BCV algorithms	Gray Scale, If RGB-Convert to Gray Scale	Gray Scale image or logo	Robust	Area units maintain the size ,image Quality and Robustness against varied attacks
Wei Wang[11]	Feature Based	Watermarking based on SVD feature and Neural Network	Gray Level	Gray Level	Robust	Excellent performance on both robustness and transparency of proposed scheme
Lei-Da Li[12]	Feature Based	Localized watermarking by extracting feature points and watermarks by OED	Gray Scale	N bit long Binary Watermark	Robust	Resist both geometric attacks and traditional signal processing attacks
Wei Lu[13]	Feature Based	feature point detection and watermark template match	JPEG Image	Any	Robust	demonstrates a strong robustness against JPEG compression.
Mir Shahriar Emami[14]	Statistical based	L2Norm technique for EISB information	Standard 8-bit Gray Scale Lena image	Four different trademarks of size 100×50pixels	Robust	Increase robustness of EISB watermarking

		watermarking				
B.Surekha [15]	Statistical based	Visual Secret Sharing (VSS) and unique statistical properties	Gray Scale 512×512	Binary watermark 100×150	Robust	Secure watermarking, it is convenient to carry and store the intermediate images called shares, improves robustness

Table 3. Codebook of basic VSS [15]

Pixel	White		Black	
Probability	50%	50%	50%	50%
Share1				
Share2				
Share1 + Share2				

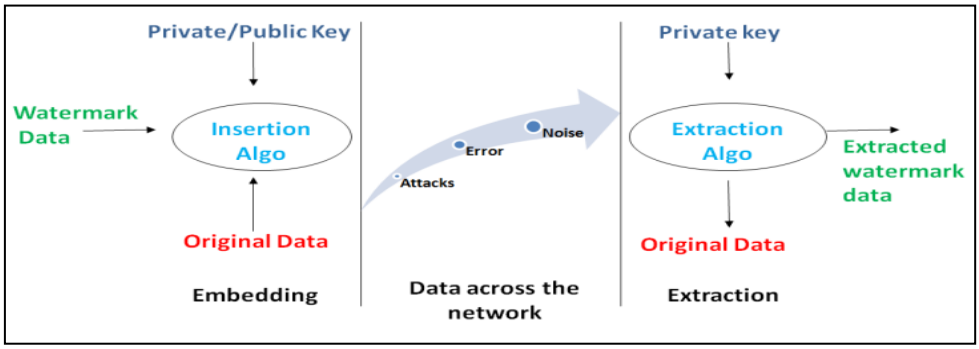

Fig 1: General watermarking system – Processes [1]

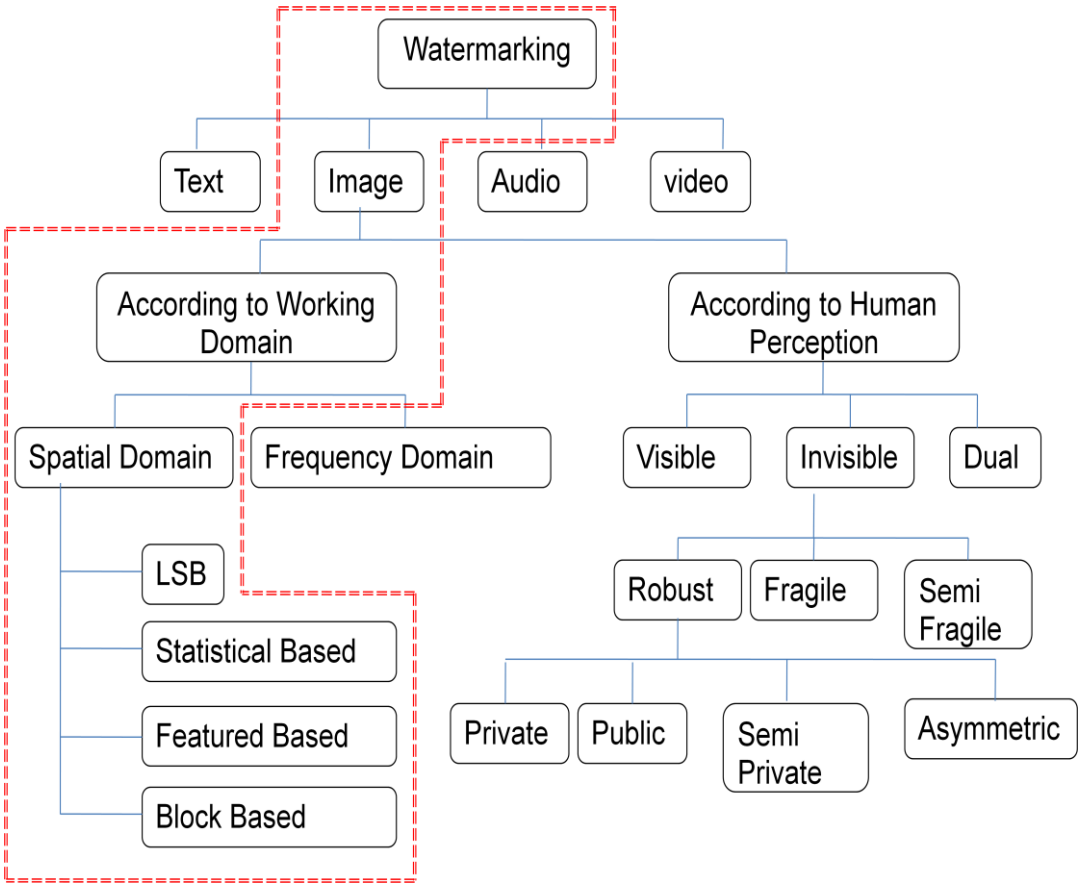

Fig 2: Types of digital image watermarking techniques.[2]

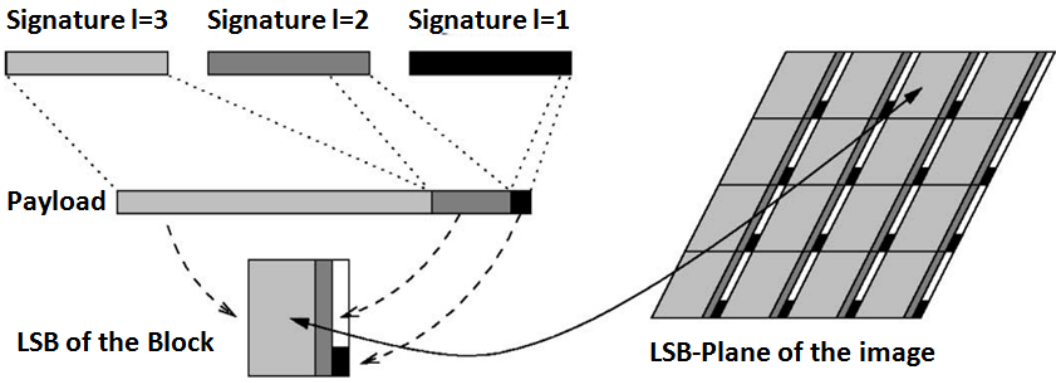

Fig.3: Concatenation of signature blocks to form a payload (left) and spatial placement of resulting payload in LSB-plane of the image.[9]

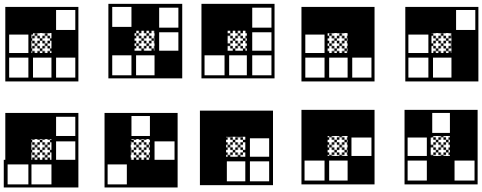

Fig.4: The 3 × 3 patterns used for hiding the information.[7]

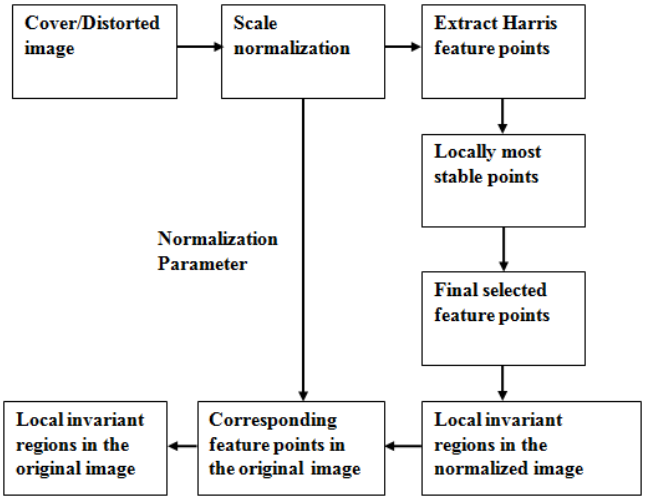

Fig.5: Diagram of watermark synchronization.[12]

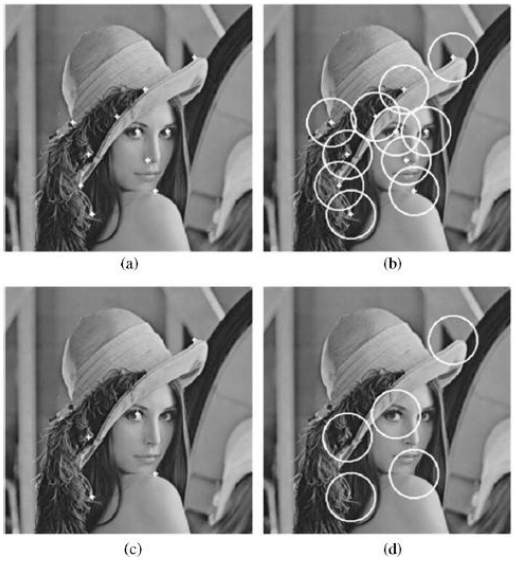

Fig.6:An example of local invariant region generation: (a) locally most stable points, (b) circular regions generated by LMSPs, (c) finally selected points, and (d) local invariant regions.[12]

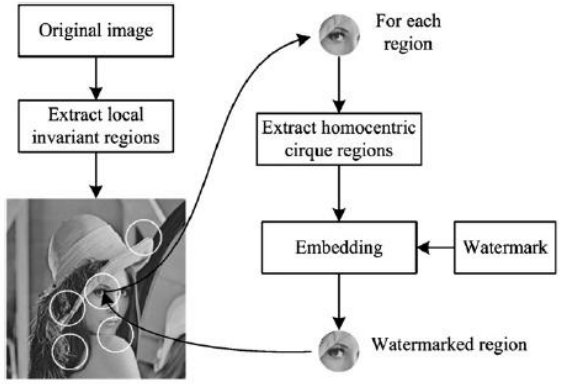

Fig.7: Watermark Extraction [12]

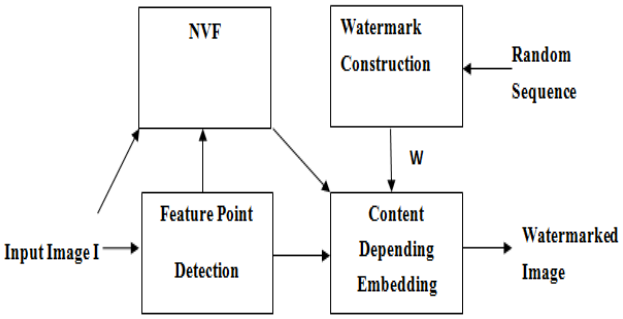

Fig.8: The watermark embedding process. [13]

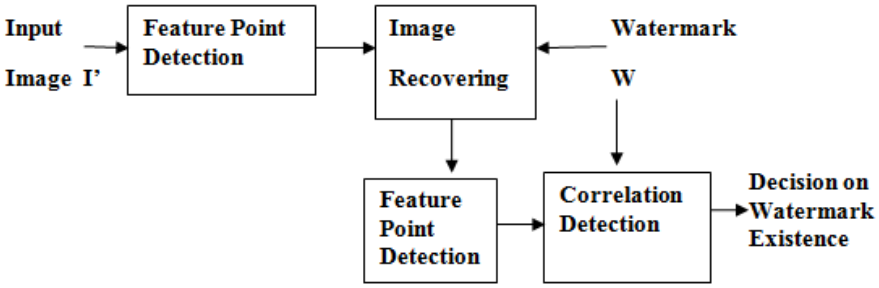

Fig. 9: The watermark detection process[13]

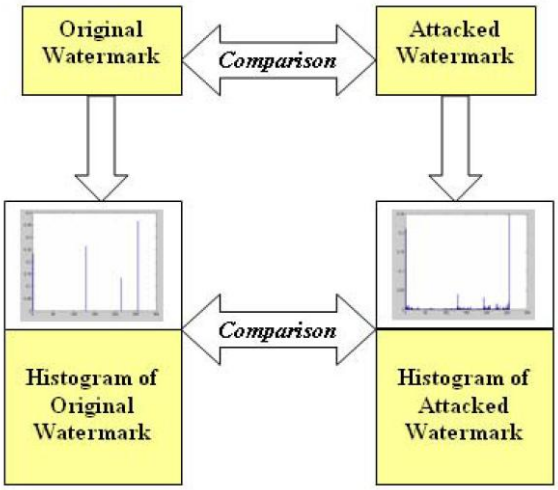

Fig. 10:Statistical Based method using L2Norm for EISB information watermarking scheme [14]

4. CONCLUSION

Most of watermarking techniques are proposed in the spatial domain because of its simplicity. This paper is a review of different techniques used in digital image watermarking in spatial domain .These techniques are classified in LSB-Based, Statistical-Based, Block-Based and Feature-Based. Different types of cover data and watermark data are used. Most of the methods are used for improving robustness of previous schemes, Authentication and maintaining the integrity of the digital document.

5. REFERENCES

[1] Chunlin Song, Sud Sudirman, Madjid Merabti. 2009. Recent Advances and Classification of Watermarking Techniques in Digital Images. Liverpool John Moores University, UK .

[2] Keta Raval, Rajni Bhoomarker, Sameena Zafar. February 2013. Implementation of Digital Watermarking For Image Security with EBCOT Algorithm and Error Correcting Codes.IJEAT.

[3] Digital watermarking available at

http://en.wikipedia.org/wiki/Digital_watermarking.

[4] Prabhishek Singh, R S Chadha. March 2013. A Survey of Digital Watermarking Techniques, Applications and Attacks. IJEIT.

[5] Ying Zhang, Jun Xiao , Ying Wang , and Yan.dd. 2009. Secure Fragile Watermarking Algorithm with Side Information.

[6] Amit Singh, Susheel Jain, Anurag Jain. 2013. Digital Watermarking Method Using Replacement of Second Least Significant Bit (LSB) with Inverse of LSB.

[7] Mr.M.Venkatesan, Mrs. P.MeenakshiDevi, Dr. K.Duraiswamy, Dr.K.Thyagarajah. 2008. Secure Authentication Watermarking for Binary Images using Pattern Matching. IJCSNS.

[8] Mr. Rohith.S, Dr. K.N.hari bhat. Jan 2012. A Simple Robust Digital Image Watermarking against Salt and Pepper Noise using Repetition Codes. ACEEE.

[9] Mehmet Utku Celik, Gaurav Sharma, Eli Saber, and Ahmet Murat Tekalp. JUNE 2002. Hierarchical Watermarking for Secure Image Authentication with Localization. IEEE TRANSACTIONS ON IMAGE PROCESSING

[10] Ashwary Rajpoot, Ranjana Batham and Navin Chourasia. Oct 2014.Spatial Domain base Image Watermarking by Edge Features .International Journal of Current Engineering and Technology.

[11] Wei Wang, Wenhui Li, Yongkui Liu, Borut Žalik. JUNE 2014 A SVD Feature based Watermarking Algorithm for Gray-level Image Watermark. JOURNAL OF COMPUTERS.

[12] Lei-Da Li, Bao-Long Guo. November 2007. Localized image watermarking in spatial domain resistant to geometric attacks, Institute of Intelligent Control and Image Engineering, Xidian University, Xi'an, China

[13] Wei Lu, Hongtao Lu, Fu-Lai Chung. 2005 .Feature based watermarking using watermark template match, Applied Mathematics and Computation Elsevier Inc.

[14] Mir Shahriar Emami Ghazali Bin Sulong. 2011. A Statistical Method based on L2Norm Technique for EISB Information Watermarking Scheme. International Conference on Future Information Technology, IPCSIT IACSIT Press, Singapore.

[15] B. Surekha, Dr. G. N. Swamy. May 2012 . Visual Secret Sharing Based Digital Image Watermarking, IJCSI.

[16] A. Siva Sankar, T. Jayachandra Prasad, M.N. Giri Prasad. ICWET 2011 .LSB Based Lossless Digital Image Watermarking using Polynomials in Spatial Domain for DRM, IJCA.