Survey of Digital Image Watermarking Techniques to achieve Robustness

Seema Malshe(Gondhalekar) Hitesh Gupta Saurabh Mandloi

ABSTRACT
Digital image watermarking is widely used for copyright protection of digital information. The effectiveness of a digital watermarking technique is indicated by the robustness of embedded watermarks against various attacks. So watermarking algorithms normally prefers robustness. Because of a robust algorithm it is not possible to eliminate the watermark without rigorous degradation of the cover content. In this paper we review few different digital image watermarking techniques to achieve robustness. This paper focuses on the various domains of digital image watermarking technique. Also describing few techniques to achieve robustness and comparing those techniques against robustness for attacks.

General Terms
Digital Image processing, Watermarking

Keywords
Watermarking, Robust, Attacks, DCT, DWT, features

1. INTRODUCTION
There is extensive use of digital multimedia data over the network. It creates a new demand for copyright protection of digital data. Encryption and digital watermarking[1] are the techniques used for copyright protection. Watermarking is embedding a secret signal (a watermark) into the original data, which is always remains present.
Perceptual transparency, Robustness, Security and Capacity are the important aspects for the design of watermarking systems.

1. Perceptual transparency means the watermark embedding should cause as little degradation to the host image as possible.
2. Robustness means the watermark must be robust to common signal processing manipulations and attempts to remove or impair the watermark.
3. The embedded information must be secure against tampering.
4. Capacity is Amount of information to be embedded Multiple watermark can be embedded and extracted

Types of watermark:
Fragile watermark: It distorted after slight changes or modification is applied. Fragile watermarks are basically used for tamper detection.
Semi fragile watermark: It resists transformations, but fails detection after nasty transformations. Commonly those are used to detect malignant transformations.
Robust Watermark: It resists a designated class of transformations. Robust watermarks may be used in copy protection applications to carry copy and no access control information.
There are two main categories of digital watermarking techniques, which are based on the embedding position, spatial domain and frequency domain watermark and other new technique is feature based watermarking.

i) *Spatial domain techniques*: In this technique, the values at the image pixels are directly modified using on the watermark which is to be embedded. The last significant bits (LSB) technique[3] : One of the most earliest technique. It is implemented by modifying the last significant bits (LSB) of the image's pixel data.
ii) *Frequency domain* : In this technique the transform coefficients are modified instead of directly changing the pixel values. To detect watermark, the inverse transform is used. The transforms commonly used for watermarking purposes are the discrete cosine transforms (DCT)[4,5], discrete Fourier transforms (DFT) and discrete wavelet transforms (DWT)[6,7].
iii) Feature based watermarking
Watermarking algorithms using a feature of an image were proposed as the second generation watermark[8,9] As features of the image have high invariance to distortions, they can be used as a key to find the insertion location. The goal is to resist both geometric distortion and signal processing attacks.
The basic three processes involved in watermarking are *watermark embedding, applying attacks, watermark detection*. In watermark embedding, a watermark signal is constructed and then embedded into an original image to produce the watermarked image. After embedding is done, the watermarked image can be subjected to various attacks. During watermark detection, the watermark detector is given a test signal that may be watermarked, attacked or not. The watermark detector reports whether the watermark is present or not on examining the signal at its input.

2. ATTACKS
An "attack" [2, 11] is any processing usually aim to impair detection of the watermark or destroy the embedded watermark. Robustness against attacks is an important aspect for watermarking schemes.
There are major four types of attacks as follows.
1. Removal attacks
2. Geometrical attacks
3. Cryptographic attacks
4. Protocol attacks.

Removal attacks **:** Removal attacks attempt to completely remove a watermark from cover data but It will preserve the content so that cover data is not useless after the attack is over. Examples of this category attacks are Denoising i,e. Gaussian, uniform, or salt-pepper, Multiple watermarking, Demodulations, lossy compression(JPEG, JPEG2000), quantization, Mean/median/Gaussian filtering, Wiener-Lee filtering, Averaging N instances of the same image, bearing different watermarks. Sharpening, Contrast enhancement (histogram equalization), Gamma correction etc

Geometric attacks: This type of attack is different from removal attack as those attack will not remove the watermark but distort it using geometric distortions specific to images. Those operations are rotation, scaling, translation, cropping etc. Template based or invariant domain or feature based schemes are used to survive from these attacks.

Examples are Global geometric transforms as Translation, rotation, Jittering, mirroring, scaling, shearing, cropping, Local geometric transforms as Random bending, local shifting, rotation, scaling, Stirmark attack as Slight global stretching, shifting, shearing, and rotation, Mosaic attack is Cutting the image into pieces, Template removal attack as Estimate and remove the synchronization template, apply a geometric transform.

Cryptographic attacks : Those are similar as cryptographic attacks, which aim at cracking the security methods in watermarking schemes. It finds a way to remove the embedded watermark information or to embed misleading watermarks. Example of such technique is the brute-force search for finding the embedded secret information by exhaustive search. Oracle attack is the other example of this category, which can be used to create a non-watermarked image when a watermark detector device is available. Due to high computational complexity, use of these attacks is restricted. Statistical averaging, and collusion attacks are also types of this category. In this attack many instances of a given data set, each time signed with a different key or different watermark, are averaged to compute the attacked data. Many instance of the same data are available in the collusion attack, but the attacked data set is generate by tacking only a small part of each data set and rebuilding an new attacked data set from these parts.

Protocol attacks: The main concept of this type of attack is invertible watermarks that is it should not be extract a watermark from a non-watermarked image. Because of inversion is that the attacker may subtracts his own watermark from the watermarked data and He or she may claims to be the owner of the watermarked data. Other example of protocol attack is the copy attack. It will not to destroy the watermark or impair its detection, but to estimate a watermark from watermarked data and copy it to some other data, called target data. IBM attack is creation of a fake original by adding a watermark in watermarked image. The attacker can claim that he has both the original and watermarked image.

As above four main classes of attacks are described the attacker may apply single or combination of more attacks.

In this paper we are focusing on robustness that is resistant to attack such as filtering, additive noise, compression, RST and other forms of image manipulation, which is very important property of watermark.

3. ROBUSTNESS TESTING

Methodology for comparing the robustness of watermarking schemes is described in paper [12]. In order to compare the techniques in a fair manner, they propose to adjust the watermark strength so that a fixed model of the human visual system detects the same extent of artifacts (the spatial masking model of Girod[3] is proposed for this purpose).

Stirmark benchmark 4.0

StirMark [11]– Image-watermarking robustness test

Markus Kuhn, Computer Laboratory, University of Cambridge

In November 1997, the first version of StirMark was published as a generic tool for simple robustness testing of image watermarking algorithms. It introduced random bilinear geometric distortions to de-synchronise watermarking algorithms. Then several versions followed improving the original attack [11] but also introducing a longer lists of tests.

StirMark is a generic tool for simple robustness testing of image watermarking algorithms and other steganographic techniques. It can be applied to photographic digital images and it will distort the watermark, so that the embedded watermark or steganographic message cannot any more be detected and decoded from the watermarked image.

StirMark Benchmark 4.0 is freely available as binary and C/C++ source code. Users should read the 'copyright' file provided in the package for license information about code and libraries used in StirMark Benchmark. This program can easily be compiled using the freely available Microsoft Visual Studio Express provided you have installed the freely available Platform SDK.

Block size, embedding strength, treatment and various attacks have great influence on the imperceptibility and robustness of watermarking in image digital watermarking algorithm. PSNR and Normalized Correlation of Watermarked Image should be checked for different attacks. PSNR (Peak signal to Noise Ratio) is used to measure the quality of watermarked image., Watermarked Image quality is better if PSNR is bigger. PSNR for image with size M x N is given by:

$$PSNR = 10 * log_{10}\left(\frac{255}{\sqrt{\frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}[I(x,y) - I'(x,y)]^2}}\right)$$

where I(x,y) is the original image, I'(x,y) is watermarked image and M,N are the dimensions of the images. The maximum pixel value of image which is equal to 255 for gray scale image where pixels are represented with 8 bits. In general, PSNR more than 28 are acceptable for Watermarked Images. Robustness is measure of immunity of watermark for attacks which attempts to remove or destroy it by image modification and manipulation. Modification or manipulation are like compression, filtering, rotation, scaling, collision attraction , resizing, cropping etc. It is measured in terms of correlation factor. The correlation factor measures the similarity and difference between original watermark and extracted watermark. It' value is generally 0 to 1. Ideally it should be 1 but the value 0.75 is acceptable.

4. SURVEY OF WATERMARKING TECHNIQUES

Classification of digital watermarking techniques which are used for producing robust watermark are spatial domain-based watermarking, frequency domain based watermarking and feature-based watermarking.

4.1 Spatial domain based technique :

The watermarking system directly alters the main data elements, like pixels in an image, to hide the watermark data For example LSB technique[3] is used.

A) LSB technique

LSB hides data in the spatial domain. The image is as a matrix NxM where N and M are the dimensions of the image and the value of the pixel in the position (i,j) is a binary number. This binary number can be then divided into a most significant bit (MSB) which contains quite a lot of information and a least significant bit (LSB) which contains very few information. You can make changes to the value of the LSB without any perceptible distortion for the human user for your image is for example in gray scale, therefore you can think of taking the LSB of an image (the cover image) and change its value in every pixel with the MSB of another image, that we would like to embed in a secret / non perceptible way in the cover image.

Following are steps are used to perform LSB

1. Select the cover image and watermark image
2. Select number of bits of cover image so that it can maintain the quality of the image. Image quality depends on number of bits. If more bits are selected then it will deteriorate the quality of the image.
3. Insert the MSB of watermark or secrete image in LSB of cover image.

For Example

For example a grid for 3 pixels of a 24-bit image can be as follows:

(10110110 11111100 00110100)
(11011110 101100101 01101011)
(01010101 010111001 10110000)

When the number 302, which binary representation is 101101110 is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(10110111 11111100 00110101)
(11011111 10100100 01101011)
(01010101 01011101 10110000)

For detecting/extracting watermarking we scan through the image, get the least significant bits according the bits were used to store the secret image. The bits extracted now become the most significant bits of secrete image.
For above example 101101110 is secrete image

Limitations of LSB technique:
Spatial domain techniques such as LSB are easier to implement, but they are limited in robustness, which is not expected in any watermarking applications. It can survive simple operation such as cropping, any addition of noise. However lossy compression is going to defeat the watermark. An even better attack is to set all the LSB bits to '1' fully defeating the watermark at the cost of negligible perceptual impact on the cover object. Furthermore, once the algorithm was discovered, it would be very easy for an intermediate party to alter the watermark.

4,2 Frequency domain based technique :

To embed a watermark, a frequency transformation is applied to the host data. Then, modifications are made to the transform coefficients.

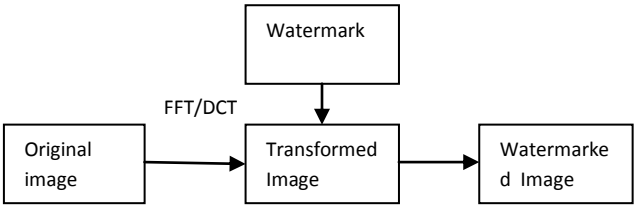


Figure 1: Watermark Embedding

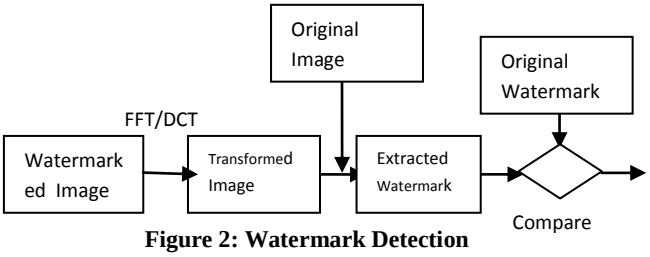


Figure 2: Watermark Detection

A)* The Discrete Cosine Transform(DCT) *Technique

Another watermarking technique is based on a direct cosine transformation (DCT)[4] transformation. One of the main components of the JPEG compression technique is the DCT algorithm.
DCT transformation separates the image into spectral sub-bands depending on the importance with respect to the image's visual quality. It can separate the Image into High, Middle and Low Frequency components. Much of the signal energy lies at low frequencies for most of images. These appear in the upper left corner of the DCT, so the modification of low frequency can be catch by human eyes. Modification of high frequencies can cause local distortion along with edges. Middle frequencies modification can not affect the image quality so transform coefficients as thus set threshold value in this area.
The one dimensional DCT is defined as

$$C(u) = \alpha(u) \sum_{x=0}^{N-1} f(x) \cos\left[\frac{\pi(2x+1)u}{2N}\right]$$

The two dimensional DCT is defined a

$$C(u,v) = \alpha(u)\alpha(v) \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right]$$

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{N}} & \text{for } u = 0 \\ \sqrt{\frac{2}{N}} & \text{for } u \neq 0 \end{cases}$$

Inverse DCT is

$$f(x,y) = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} \alpha(u)\alpha(v)C(u,v) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right]$$

Where u=1,2,…..N-1 and v = 1,2, ……M-1

DCT is faster and the complexity of it is O(n log n) operations.
Watermark Embedding Process :
The embedding watermark is as follows.
1. Sequentially extract out every 8-bit data from watermark-bit-stream.
2. Use pseudo random generation system to obtain a random number, which points to one of n blocks of host image.
3. In the block pointed by previous step, embed extracted 8-bit watermarking data into the 8 lower-band coefficients.
4. Repeat step 1 to step 3, until the watermark bit stream is run out.
5. The proposed that replace bit to embedded watermark bit stream, and it was hidden at position bit 4 in the selected 8-bit coefficient. If the watermark bit is "1" then bit 4 to "1" otherwise "0".

Extracting Watermarked Image
1) Perform DCT transform on watermarked image and original host image.
2) Subtract original host image from watermarked image.
3) Multiply extracted watermark by scaling factor to display.

Advantages
1) As DCT domain watermarking can survive against the attacks such as noising, compression, sharpening, and filtering. it is comparatively much better than the spatial domain encoding since
2) It use JPEG compression method to apply DCT watermarking as a parameter. One may use different

parameters related to image processing, and these parameters might provide equal or even stronger robustness against various attacks based on image processing.
3) It can be used as signature when discrete cosine transform (DCT), where pseudorandom sequences, such as M sequences, are added to the DCT at the middle frequencies.

B) Discrete Wavelet Transform (DWT) technique:Xia, Boncelet, and Arce proposed a watermarking scheme based on the Discrete Wavelet Transform (DWT). The watermark, modeled as Gaussian noise, was added to the middle and high frequency bands of the image. The decoding process involved taking the DWT of a potentially marked image.

- Perform 2D-DWT to divide image into LL, HL, LH and HH sub-bands.
- Select coefficients from the LL, HL, LH and HH
  Embed watermarking data via additive modification
  $t'_i = t_i + \alpha|t_i|x_i$
  x_i = watermark
  α = weighting constant

Perform 2D-IDWT to create "watermarked image"
Multi resolution decomposition of a signal is discrete wavelet transform. 1 level DWT involves applying a low pass and a high pass filters along the columns and then the rows respectively. It separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components.
These sub-bands surpass a particular threshold T1.
The low pass filter extracts the low frequency coefficients along a certain direction and the high pass filter extracts the high frequency coefficients of a signal. In two dimensional applications, for each level of decomposition, we first perform the DWT in the vertical direction, followed by the DWT in the horizontal direction. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. For each successive level of decomposition, the LL sub band of the previous level is used as the input. The process can then be repeated to compute multiple "scale" wavelet decomposition. Each tile component undergoes three levels of decomposition. This results in 10 sub-bands per component. LH1, HL1, and HH1 contain the highest frequency bands present in the image tile, while LL3 contains the lowest frequency band. The two-level DWT decomposition is shown in Fig.3.

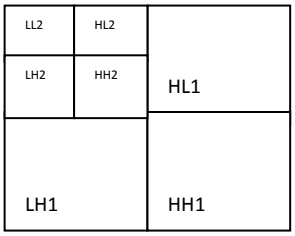


Figure 3 two-level DWT decomposition

Watermark embedding is done using

$$I_{w_{u,v}} = \begin{cases} W_i + \alpha|W_i|x_i, & u,v \in HL,LH \\ W_i & u,v \in LL,HH \end{cases}$$

In the Wavelet Domain where denotes the coefficient of the transformed image, xi the bit of the watermark to be embedded, and α a scaling factor. To detect the watermark the same process as that used in DCT is implemented i W
Advantages:
This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution 32 detail bands LH, HL, HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality.
The basic embedding algorithm in the paper can be summarized as The frequency domain watermarking methods mentioned above include robustness to waveform attacks such as JPEG compression, filtering, and noise addition, yet they are not robust to geometrical attacks such as rotation, scaling, and translation (RST).

C) PCA based watermarking:
The mathematical procedure of transforming a number of possibly correlated variables into a smaller number of uncorrelated variables is called Principal component analysis (PCA). Given a data set, the principal component analysis reduces the dimensionality of the data set. In [16] the author proposes a new digital video watermarking scheme based on Principal Component Analysis. Embedding of the watermark is done in the three color channels RGB of an input file.
The preliminary results in the paper showed a high robustness against most common video attacks, especially frame cropping, cropping and recalling for a good perceptual quality
As per paper [17] the graph plotting of PSNR versus Noise Density for LSB. DCT and DWT is shown in figure **4**

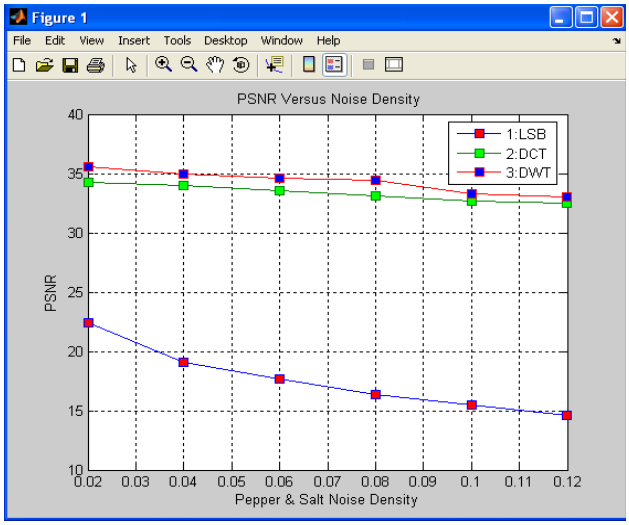


Figure 4 Comparative plotting of PSNR Versus Noise Density for LSB, DCT and DWT based watermarking as [17]

4.3 Feature-based watermarking

Now there are newer techniques are developed, which are based on feature based watermarking.
For getting robust watermark, the watermark should be embedded in silent part of the data. For these significant features of data is used. A feature is meaningful characteristics of data. Features of an image can are edge, corner, texture, color etc.
Features should have some properties for watermarking as resistant to transformations such as rotation, scaling, translation (RST), resistant to noise and localized variation. An invariant feature is a feature calculated from an image that is invariant with respect to certain transformations, i.e. it does not change when these transformations are applied to the image. The transformations considered here are mainly translation, rotation, and scaling.

As per the paper[8,9], In general, feature-based watermark algorithms are the best approaches to resisting geometric distortions since feature points provide stable references for both watermark embedding and detection.

In paper[8] they develop a robust watermarking scheme. This scheme combines the advantages of feature extraction and image normalization to resist image geometric distortion and to reduce watermark synchronization problem at the same time. Mexican Hat wavelet scale interaction method is used for Feature extraction. It allows different degrees of robustness (against distortion) by choosing proper scale parameters. and since only a few feature points in an image generally affected by local variations such as cropping or warping. The unaffected feature points can still be used as references during the detection process. It determines the feature points by identifying the intensity changes in an image. Since significant intensity changes (edges) may occur at different scaled versions of the same image. The scheme is designed for both color and gray-level images. The Mexican Hat wavelet filtering is implemented in the frequency domain using the FFT.

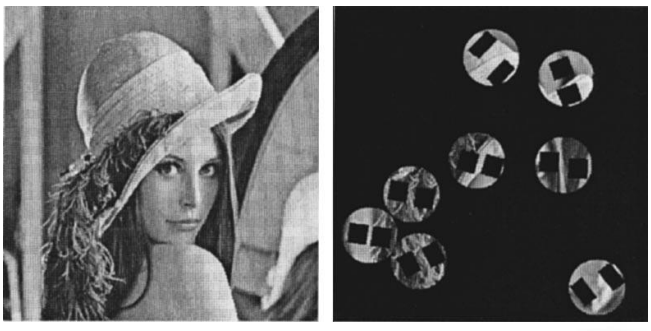
The image normalization technique developed for pattern recognition can be used for digital watermarking.

Watermark embedding process:

1. Select original image
2. Extract feature points of the image
3. Perform image Normalization on Disks in original Image
4. Transform co-ordinates of selected points from normalized image back to the original image.
5. Construct two 32x32 Blocks in each qualified disk in original Image.
6. Apply 2-D FFT on 32x32 Blocks
7. Embed watermark
8. Apply 2D IFFT
9. Replace the Disks in original image by watermarked image

Watermark detection Process:

1. Get the received image.
2. Extract features
3. Perform image normalization on each disk in received image
4. Transform Coordinates of selected points from the Normalized Image back to the Received Image.
5. Construct two 32x32 Blocks in each dsk of received image
6. Apply 2-D FFT
7. Using Secrete key K Watermark detection is done
8. Compare the watermark and the detected watermark for detection decision.



(a) (b)

As results in [8] are on the popular test images 512 512 Lena, Baboon, and Peppers, using StirMark 3.1 [10] to test the robustness of our scheme. The StirMark 3.1 attacks can roughly be classified into two categories: common signal processing and geometric distortions. The difference images between the original images and the watermarked images in the spatial domain are magnified by a factor of 30. The PSNR values between the original and the watermarked images are 49.42, 45.70,and 56.60 dB for Lena, Baboon, and Peppers, respectively. Because of their small amplitudes, the embedded watermarks are invisible by subjective inspection. They suggest that scheme performs well under other common signal processing attacks such as median filtering, color quantization, 3x3 sharpening, and Gaussian filtering. It can also resist combined signal processing and JPEG compression attacks at a quality factor of 90.

Table 1 : Correctly detected watermark disks under common signal processing attacks as per [8]

Attacks	Lena	Baboon	Pepper
Watermarked image	7/8	10/11	4/4
Median filter 2x2	1/8	6/11	1/4
Median Filter 3x3	1/8	2/11	1/4
Sharpening 3x3	4/8	4/11	4/4
Color quantization	7/8	4/11	1/4
Gaussian Filtering 3x3	5/8	8/11	1/4
Additive uniform noise (scale=0.1)	5/8	6/11	4/4
Additive uniform noise (scale=0.15)	4/8	4/11	2/4
Additive uniform noise(scale=0.2)	1/8	5/11	1/4
JPEG 80	6/8	9/11	3/4
JPEG 70	7/8	11/11	3/4
JPEG 60	6/8	7/11	1/4
JPEG 50	5/8	7/11	3/4
JPEG 40	3/8	5/11	1/4
JPEG 30	2/8	4/11	0/4
Median Filter 2x2+JPEG90	2/8	6/11	0/4
Median Filter 3x3+JPEG90	1/8	1/11	1/4
Sharpening 3x3+JPEG90	4/8	2/11	4/4
Gaussian filtering 3x3 +JPEG90	5/8	8/11	2/4

In paper [9], comparison of technique used in [8] and [9] is compared. They suggest that, the feature detector is a key role in the feature-based watermarking. Up to present, many good feature detectors have been proposed such as Hessian-Affine detector, Harris-Affine detector , MSER , IBR , and EBR etc. The paper suggest that, the Hessian-Affine and MSER detectors have better performance.

However, the MSER detector is difficultly applied to a watermark algorithm because of the irregular output region of the detector. Therefore, to obtain the feature points and the characteristic regions., the Hessian-Affine detector is adopted in the proposed algorithm Moreover, the proposed algorithm then exploits the local orientation of each pixel to embed the copyright watermark into the regions. In order to achieve different kinds of applications simultaneously, the remainder regions are also used for fragile watermarking by applying block-wise methods. The experimental results shown in paper that the proposed watermarking algorithm can resist most removal and geometric attacks. Besides, changes or modifications of an image will also be reflected in their hidden watermarks.

In this paper, a scale and affine invariant interest point detector, called Hessian- Affine detector, is proposed by Mikolojczyk and Schmid. The detector is adopted to obtain the feature points and the characteristic regions of an image in

our proposed algorithm. The procedure of the Hessian-Affine detector is as follows:
1) Detect initial points with Hessian detector and select the characteristic scale.
2) Estimate the shape with the second moment matrix.
3) Normalize the ellipse region to circular one.
4) Refine the point location and scale.
5) Go to step 2 if the second moment matrix of new point is not isotropic
After the Hessian-Affine detector, many feature points and regions are obtained in the processed image, Most of the obtained feature points in the original image are the same as those in the rotated one. Therefore, the robustness of the feature detector is exploited to resist various attacks in the proposed algorithm.

Watermark embedding process:

Block diagram of watermark embedding suggested in [9] is

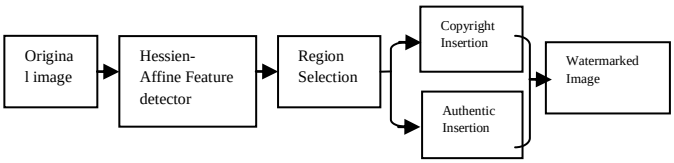


Figure 4 watermark embedding scheme

Watermark detecting:

Block diagram of watermark detecting process as per paper [9] is

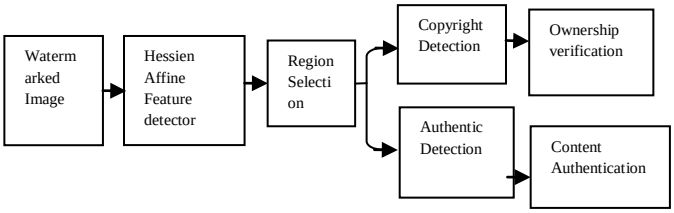


Figure 5 watermark detecting scheme

After testing Two well-known 512x512 images, Lena and Baboon they evaluate the performance of the proposed algorithm. After embedding invisible copyright and fragile watermarks by using their algorithm, the peak-signal-to-noise-ratio (PSNR) of the Lena and the Baboon images is 45.62 dB and 42.17 dB, respectively.
They have compared with other two feature-based watermarking methods, Tang's method [8] and Seo's method Using StirMark 3.1 by the benchmark program, [10] experiment result shows that most of the copyright watermarks after noise-like signal processing and geometric distortions are still detectable by the proposed algorithm. Compared with other methods, the proposed algorithm for resisting most of attacks has better results, the aspect ratio change especially.
The Table 2 The comparison among the two algorithms, the proposed method by Tsai & Huang [9], Tang and Hang's method (Tang's) [8]. The symbol, --, means no data. : which is mentioned in [9].

Images	Lena		Baboon	
Attack	Tsai & Huang	Tang's	Tsai & Huang	Tang's
None	19/19	7/8	23/25	10/11
Rotation 1	5/19	3/8	6/25	3/11
Rotation 5	5/19	0/8	4/25	0/11
Rotation Scale 1	3/19	0/8	9/25	4/11
Cropping 10%	8/19	2/8	8/25	2/11
Cropping 25%	5/19	-	3/25	-
Linear	5/19	5/8	12/25	4/11
Linear	9/19	4/8	14/25	4/11
Aspect Ratio	1/19	0/8	2/25	0/11
Aspect Ratio	2/19	0/8	8/25	0/11
Scale 50%	1/19	-	0/25	-
Median 2x2	1/19	1/8	3/25	6/11
Median 3x3	1/19	1/8	3/25	2/11
Gaussian 3x3	3/19	5/8	5/25	8/11
Sharpening 3x3	2/19	4/8	4/25	4/11
JPEG 20	0/19	-	1/25	-
JPEG 40	1/19	3/8	2/25	5/11
JPEG 60	2/19	6/8	4/25	7/11
JPEG 80	3/19	6/8	5/25	9/11
Random Bending	4/19	-	0/25	-

A robust feature-based image watermarking algorithm for copyright protection and content authentication is proposed in [9]. The Hessian-Affine detector is adopted to obtain the points and regions. Because of the invariant property of the feature points and characteristic regions, most of the removal and geometric attacks are resisted by their algorithm.. Comparing with other robust watermarking methods, the robustness of the proposed method is superior

5. CONCLUSION

As per research work done for robustness of watermarking, there are many techniques are suggested as spatial domain and frequency domain based watermarking techniques. Watermarking in frequency domain as DFT, DCT, DWT are more robust than watermarking in spatial domain because information can be spread out to entire image.
As features of the image have high invariance to distortions, they can be used as a key to find the insertion location. The goal is to resist both geometric distortion and signal processing attacks, feature based watermarking scheme is suggested in combination with frequency or spatial domain based watermarking. Since no watermarking algorithm resists all the attacks. Still we can find better which will give more robust watermark.

Future work

Future work can be done for selecting different robust features and selecting proper embedding technique can improve the robustness of watermark and different Optimization techniques can be used for selecting different regions of the watermark embedding.

6. REFERENCES

[1] "Researches on uniform meaningful watermark? liu quan, jiang xuemei, proceedings of the 2002 6t international conference on signal processing, 2002.

[2] S. Voloshynovskiy, S. Pereira, T. Pun, University of Geneva J.J. Eggers and J.K. Su, University of Erlangen-Nuremberg, Attacks on Digital Watermarks: Classification, Estimation-based Attacks and Benchmarks

[3] Neeta Deshpande, Snehal Kamalapur and Jacobs Daisy,

"Implementation of LSB steganography and Its Evaluation for Various Bits", 1st International Conference on Digital Information Management,6 Dec. 2006 pp. 173-178.

[4] Mrs Neeta Deshpande, Dr. Archana rajurkar, Dr. R. manthalkar Review of Robust Video Watermarking algorithms, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 3, March 2010.

[5] K. R. Rao and P. Yip, "Discrete Cosine Transform: Properties, Algorithms, Advantages, Applications"

[6] H. Inoue, A. Miyazaki and T. Katsura, "An Image Watermarking Method Based on the Wavelet Transform", IEEE Conf. on Image Processing, Vol. 1, pp. 296-300, 1999.

[7] hua lian; bo-ning hu; rui-mei zhao; yan-li hou; , "design of digital watermarking algorithm based on wavelet transform," machine learning and cybernetics (icmlc), 2010 international conference on , vol.5, no., 621pp.2228-2231, 11-14 july 2010

[8] Chih-Wei Tang and Hsueh-Ming Hang, "A Feature-Based Robust Digital Image Watermarking Scheme", IEEE Transactions on signal processing vol 51, NO. 4, APRIL 2003

[9] Jen-Sheng Tsai, Win-Bin Huang, Chao-Lieh Chen, Yau-Hwang Kuo, "A Feature-Based Digital Image Watermarking For Copyright Protection And Content Authentication "Image Processing,IEEE International Conference 2007

[10] Fabien A.P. Petitcolas , Ross J. Anderson, and Markus G. Kuhn "Attacks on Copyright Marking Systems"

[11] STIRMARK bench mark http://www.petitcolas.net/fabien/watermarking/stirmark/

[12] Jiri Fridrich*, Miroslav Goljan, "Comparing robustness of watermarking techniques"

[13] "Literature Survey on Digital Image Watermarking"Er-Hsien Fu , EE381K-Multidimensional Signal Processing8/19/98

[14] Hae-Yeoun Lee, Hyungshin Kim, Heung-Kyu Lee "Robust image watermarking using local invariant Features", Optical Engineering, 2006

[15] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, / Secure spread spectrum watermarking for multi-media," IEEE Trans. on Image Processing 6 (1997), 1673-1687

[16] Wu, Y, 2005. "On the Security of SVD-Based Ownership Watermarking", IEEE Trans. Multimedia 7, pp. 624-627.

[17] Baisa L. Gunjal , R.R. Manthalkar "An Overview Of Transform Domain Robust Digital Image Watermarking Algorithms", Journal of Emerging Trends in Computing and Information Sciences 2010-11

Table 3 Comparison of different techniques against robustness for various attacks as [4] and [8,9]

Spatial Domain (LSB)	Frequency domain				**Feature based**
	Secure spread spectrum	DCT	DWT	PCA	
Block-wise Compression, Block-wise Compression, Addition of Gaussian and impulse noise, Low pass filtering	Block-wise Compression, Addition of Gaussian and impulse noise, Low pass filtering	Compression Rotation, Scaling Gaussian noise attack salt and pepper attack Cropping, Rescaling, Frame dropping, Rotation, Median Filter	Frame dropping, Frame collision, Cropping, Rescaling, Noise, MPEG attack, Lossy compression, Median filter, Row column removal, Rotation,	Cropping, Rescaling, Frame dropping, Rotation, Median Filter	Mild geometric distortion and common signal processing attacks. And composite attacks of high-quality JPEG compression together with geometric distortions/signal processing