

# ENHANCED FAST ROBUSTNESS MEASUREMENT IN VIGOROUS DIGITAL IMAGE WATERMARKING VIA SELECTING OPTIMAL FEATURE POINTS

<sup>1</sup>SATHYABAMA K, <sup>2</sup>Dr.V.MANIKANDAN

<sup>1</sup>Associate Professor, Department of Electronics and Communication Engineering  
Adithya Institute of Technology, Coimbatore

<sup>2</sup>Professor, Department of Electrical and Electronics Engineering  
Coimbatore Institute of Technology, Coimbatore

E-mail: [sathyabamak0574@gmail.com](mailto:sathyabamak0574@gmail.com)

## ABSTRACT

The increasing amount of research on watermarking over the past decade has been largely driven by its important applications in digital copyrights management and protection for finding the effectiveness of the digital watermarking. The robustness of the digital watermarking has been analysed by different evolution measures and different attacks. In existing method the BER is used for selecting the optimal feature region from the watermarked image. But BER is not a more accurate image quality measure. So Modified version of Peak Signal Noise Ratio (MPSNR) is used in our proposed method. In our proposed method the optimal feature points can be selected from the watermarked image based on the enhanced quality measurement of which point resists the predefined and undefined attacks. For the enhanced quality measurement, the MPSNR value is used. Hence, our proposed method performance is analyzed by taking number of watermark images and finds the optimal feature points which resist both the predefined and undefined attacks more efficiently.

**Keywords:** *Digital image watermarking, SUSAN detector, Optimal Feature Point Set, Predefined and Undefined Attacks, MPSNR*

## 1. INTRODUCTION

Watermarking is a technique of data hiding the information considering the ownership, user identity, which was empowered to apply which can be demonstrated as proof during conflicts [19]. A dominant method is Image watermarking, which for guarding the copyright of images, vaguely changes the host digital images to implant the copyright data [1]. In order to authenticate it, Digital Watermarking is a method which implants a watermark signal into the host image [2]. Watermarking is an extremely vital field for copyrights of different electronic texts and media [4]. Four important features are there those are generally applied to find out quality of watermarking plan. Robustness, imperceptibility, capacity, and blindness are the four [6]. To oppose any alterations, robust watermarks are planned and are designed for the copyright fortification [12]. Digital water marking is known to be robust if it opposes an allocated class of transformations [3].

Digital Image Watermarking is one of the well-known techniques to complete the space among copyright issues and digital distribution of information [14]. Digital watermarking is a technique to cover some data that is incorporated with a multimedia object [9]. Two crucial necessities are authentication and recovery of tampered localization of a digital data. Hence, to guard the digital information watermarking method is extensively applied [13]. The different watermarking categorizations are Visible Watermarks, Invisible watermark, Public watermark, Fragile Watermark, Private watermark and Perceptual watermarks [17]. Spatial domain techniques and frequency domain techniques are the two techniques occupied in the water marking [5]. In spatial domain, the watermark is implanted into the particular pixels of the host image. In transform domain, the host image is initially changed to a frequency domain and next watermark is implanted into the frequency coefficients [11] [18]. To implant a watermark signal into the host data with the intention of copyright protection, access control, broadcast monitoring etc is the

fundamental scheme behind digital watermarking [16].

To guard the confidentiality, integrity, availability and authenticity of data in communication from unauthorized access, reveal, disruption, change and copy is the main plan of the watermarking technique [15]. Watermarking is extensively applied for copyright protection of images, audios and videos [10]. In watermarking functions, the robustness of watermarks to attacks is necessary to the system these attacks can be categorized into two wide categories: signal processing and geometric attacks. Whereas signal processing attacks challenge to diminish the watermark energy, geometric attacks may bring about synchronization faults among the encoder and the decoder of the watermark [8]. Watermark facilitates several applications they are Copy Control, Digital signatures, Authentication, Broadcast monitoring, Fingerprinting and Secret communication [7][20].

The remaining of this document is sorted out as follows. A short discussion about the research works associated to the watermarking is specified in section 2. The problem statement and the contribution of our suggested method have been explained in section 3. Our suggested optimal feature points choice from the watermarked images based on MPSNR value is explained in a few words in section 4. The execution results and ending of the paper is specified in section 5 and 6.

## 2. RELATED WORK

A bench-marking device based on genetic algorithms (GA) has been offered by Giulia Boato *et al.* [21] and planned to calculate the robustness of any digital image watermarking system. To assess robustness in terms of perceptual quality is the major idea, calculated by weighted peak signal-to-noise ratio. Through a stochastic strategy, optimize this quality metric, by locating the minimal degradation that requires to be brought in a marked image so as to take away the implanted watermark. According to the measured application scenario chosen, specified a set of attacks, GA sustain the optimization of the parameters to be allocated to every processing operation, to acquire an unmarked image with perceptual quality as high as feasible. Widespread experimental results showed the efficiency of the suggested assessment device.

A color image watermarking plan that conceals watermark signals in most distortion-tolerable signals inside three color channels of the host image

devoid of resulting in perceivable alteration has been suggested by Chun-Hsien Chou *et al.* [22]. The distortion-tolerable host signals or the signals that have high perceptual severance are required in the wavelet domain for watermark inclusion. To calculate the perceptual severance inherent in every wavelet coefficient of the host image, a visual model based upon the CIEDE2000 color difference equation is applied. Binary watermark signals are implanted in qualified wavelet coefficients by means of quantization index modulation. To support the robustness, the watermark signals are continual and permuted before implanting, and re-established by the majority-vote choice making procedure in watermark removal. In watermark removal, original images are not needed. Merely a little amount of data together with locations of qualified coefficients and the information related with coefficient quantization is required for watermark removal. Experimental results have demonstrated that the implanted watermark is clear and rather robust in face of different attacks such as cropping, low-pass filtering, scaling, media filtering, white-noise addition with the JPEG and JPEG2000 coding at high firmness ratios.

A hybrid image-watermarking plan based on discrete wavelet transform (DWT) and singular value decomposition (SVD) has been suggested by Chih-Chin Lai *et al.* [23]. The watermark is never implanted openly on the wavelet coefficients however rather than on the ingredients of singular values of the cover image's DWT subbands. Experimental results has pointed up that the suggested strategy is competent to endure a range of image-processing attacks.

Ming Chen *et al.* [24] have spotlighted on the theoretical test and experimental study of model order choice in reversible image watermarking. Prediction and context modelling are the two modelling devices engaged. Using particularly obtained criteria for reversible image watermarking, classic forecast models are compared and assessed. The CALIC, a device uniting the Gradient-Adjusted Prediction with a context modelling among them, stands out as the superlative by offering the most aggressive model-fitness with comparatively low complexity. Besides, full context forecast, a model unique to reversible image watermarking, is moreover explained. Highly fitted modelling at an extremely low order is accomplished by utilizing severance to higher extent. Experimental results showed that it is competent of offering yet improved presentation than the CALIC with only insignificant computation.

For robust digital image watermarking, Jen-Sheng Tsai *et al.* [25] has suggested feature region selection technique. The technique plans to choose a non overlapping feature region set, which has the maximum robustness against a range of attacks and can conserve image quality as much as feasible following watermarked. Using a few predefined attacks, it first executes a simulated attacking process to assess the robustness of every candidate feature region. According to the assessment results, it then implemented a track-with-pruning process to look for a minimal primary feature set which can oppose the most predefined attacks. The primary attribute set is next expanded by adding into some auxiliary attribute areas to improve its conflict to vague attacks under the restraint of preserving image quality. This effort is prepared as a multidimensional knapsack problem and worked out by a genetic algorithm based strategy. The tentative results for StirMark attacks on a few benchmark images hold up our belief that the primary attribute set can oppose all the predefined attacks and its addition can improve the robustness against un-defined attacks. The suggested method shows improved presentation in robust digital watermarking comparing with some well identified attribute based methods.

### 3. PROBLEM STATEMENT

Section 3, reviews the recent research works related to provide a better enhanced fast robustness measurement in digital watermarking. Digital watermarking is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. The effectiveness of a digital watermarking algorithm is indicated by the robustness of embedded watermarks against various attacks. In the literature, different evolution measures and different attacks were utilized to analyze the robustness of the digital watermarking algorithm. Besides the other, one of the recently developed robust digital watermarking techniques [25] is to select a non-overlapping feature region set, which has the greatest robustness against various predefined and undefined attacks and can preserve image quality. This technique performs the primary feature region selection by finding the BER rate between the original feature regions and the watermarked feature region whereas the feature extension stage is performed by considering the two image characteristics namely, corner response and integration scale. Based on the above process, this

technique efficiently finds the optimal feature regions. But this technique has the drawback in the quality measurement which is utilized in the primary feature region selection i.e. the BER is not a more accurate image quality measure because most specifically we compute the BER in the networks communication process. Hence, this BER is not a standard metric in the image quality measurement. So, there is a need to develop a faster robustness measurement in the digital watermarking.

### 3.1 Contributions of the Paper

The main contributions of the paper are,

- Analysis of various predefined and undefined attack
- Optimal feature point's selection from the watermarked images has been found out by applying various predefined and undefined attacks.
- Performance is analyzed by taking number of watermark images.

### 4. PROPOSED OPTIMAL FEATURE POINTS SELECTION METHOD

Digital watermarking is the process of embedding copyright information such as author/owner/ usage restrictions into the original file. Securing digital images while transferring through networks and later extracting it in the original form is a very challenging task. Several advance computation techniques have been developed which provide security to digital media while transmission through open networks. Digital watermarking describes the process of embedding additional information into a digital media, without compromising the media's value. Depending on the real world applications, this technique requires a number of properties such as perceptual quality, robustness, capacity and efficiency. A watermarked image may undergo some attacks and in order to overcome these attacks some attack resistance points have been selected. For finding the optimal feature points the proposed method has been developed. Our proposed method consist of four stages namely,

- ❖ SUSAN detector
- ❖ Watermarking
- ❖ Attacking
- ❖ Optimal feature points selection using MPSNR

These four stages are consecutively performed and the optimal feature points selection using MPSNR are discussed in Section 4.1, 4.2, 4.3 and 4.4 respectively. Structure of our proposed optimal feature point set detection using is illustrated in fig. 1

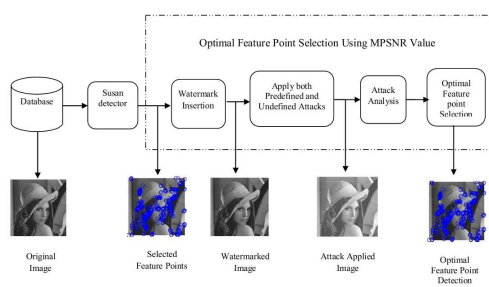


Figure 1: Block Diagram For Proposed Digital Image Watermarking Via Selecting Optimal Feature Points

Let  $V_d: d = 1, 2, \dots, N_v$  be a database images, where  $N_v$  is the total number of images and  $V_x$  is the one of the image in the database  $V_d$ . In image  $V_x$  the feature points can be selected by Susan detector and this feature point's detected image is called as  $R_i$ , where  $i = 1, 2, \dots, n$  is the number of points selected by using SUSAN detector. In next stage watermarking technique has been applied to the image  $R_i$  and obtains a watermarked image as  $W_i$ . Afterward, the different predefined and undefined attacks are applied to the watermarked image called  $W_i$  and the optimal feature points has been finding out by using MPSNR value.

#### 4.1 SUSAN Detector

Smallest Univalve Segment Assimilating Nucleus is SUSAN detector. This technique is applied for corner recognition and edge detection and noise suppression. The algorithm is suggested by Smith and Bray is based on glow comparisons inside a circular mask. Based on the edge reaction, the feature points are chosen in our method. In SUSAN detector, they exploit a circular. The Points of the mask that have the similar value of intensity of the centre, known as nucleus, form the USAN region (Univalve Segment Assimilating Nucleus). The data offered by USAN (size, barycentre) permits distinguishing edges and taking away false detections. The last step is the exclusion of non maxima. Its robustness to noise is the main benefit of SUSAN. From SUSAN by applying a circular

mask, however they merely think the points on the circle. At the suitable edge the SUSAN area edges will have centers of gravity adequately far from the nucleus of the mask. At the suitable edge, the structuring part of the SUSAN region are those pixels lying on a straight line from the nucleus of the mask to its center of gravity, so the left over regions of the mask will only have false edges and can be thrown away. For the edge recognition a spherical mask with Gaussian weighting is located at every point in the image and for every point the glow of each pixel inside the mask is compared with that of the nucleus (the center point).

$$S(N_p^{V_x}, M_p^{V_x}) = \begin{cases} 1 & \text{if } |B(N_p^{V_x}) - B(M_p^{V_x})| \leq T \\ 0 & \text{if } |B(N_p^{V_x}) - B(M_p^{V_x})| > T \end{cases} \quad (1)$$

Where  $N_p^{V_x}$  is the position of nucleus in  $V_x$  image,  $M_p^{V_x}$  is the position of any other points within the image  $V_x$ .  $B(N_p^{V_x})$  is the brightness of pixel  $N_p^{V_x}$  in image  $V_x$  and  $B(M_p^{V_x})$  is the brightness of pixel  $M_p^{V_x}$ .  $T$  is the brightness difference threshold and  $S$  is the output of comparison. For getting a smoother version this equation can be written as

$$S(N_p^{V_x}, M_p^{V_x}) = e^{-\frac{(B(N_p^{V_x}) - B(M_p^{V_x}))^2}{T^2}} \quad (2)$$

Summing of result in each pixel within the mask is given us

$$C(M_p^{V_x}) = \sum_{N_p^{V_x}} S(N_p^{V_x}, M_p^{V_x}) \quad (3)$$

This is the number of pixels inside Univalve Segment Assimilating Nucleus (USAN). Next, the response of the edge is calculated by

$$A(M_p^{V_x}) = \begin{cases} G - C(M_p^{V_x}) & \text{if } C(M_p^{V_x}) < G \\ 0 & \text{Otherwise} \end{cases} \quad (4)$$

Where  $G$  is the geometric threshold of SUSAN algorithm and is set to  $3 * C \max / 4$  and  $C \max$  is the maximum value which can take and it is necessary for image that suffer from noise. After applying the SUSAN detector the watermarking technique has been applied in the selected feature point image  $R_i$  and is described in section 4.2.

#### 4.2 Watermarking

Watermarking is a technique which you can sign your name on the photo. If anyone trying to copy

that photo he cannot be done, because the watermark will be there in the photo. In our paper a method for authenticating the image using lossless water marking is being proposed [26]. In our work the signed message has been embedded into the each feature detected points from an image  $R_i$  using LSB (Least Significant Bit). Initially the image  $R_i$ , each points selected from the SUSAN detector, has been split into  $L$  number of blocks  $R_i^M$  and select  $n$  number of pixel from every block by using raster scanning. The  $n$  value computation is stated as,

$$n = \frac{4 * X(\text{msg elements})}{L} \quad (5)$$

Increment the value of  $\text{msg elements}$  value by 1 until the condition given in Equation (6) is satisfied.

$$n = 4 * X(\text{msg elements}) \bmod L = 0 \quad (6)$$

The extracted  $n$  pixel values corresponding binary values are computed and determined the least significant bit value (LSB) from each pixel binary value. The least significant bit values of each pixel from points  $R_i^L$  are replaced by the signed message  $\text{msg}$  element values.

**For example**, consider a text message 'HELLO'. The ASCII value of each character is [72, 69, 76, 76, and 79] and the binary value is [01001000, 01000101, 01001100, and 01001111]. The signed message

$\text{msg} = (01001000, 01000101, 01001100, 01001111)$   
Image pixel values  
(00101100, 01001100, 00110010) from block 1 are represented as (10000111, 10000110, 10000100, 10000001 (n=4)) and the least significant bit values are obtained and substituted as

10000111-> 10000110  
10000110->10000111  
10000100->10000100  
10000001->10000000

Then, these values (10000110, 10000111, 10000100, and 10000000) are embedded into the point pixel values of block 1. Similarly, other blocks values are replaced by the signed messages. After the message embedding process, we obtain the water marked image is called  $W_i$  and the various predefined and undefined attack has been applied in this image for the robustness calculation for the optimal feature points.

### 4.3 Attacking

Normally in watermarked image, the messages will affect some changes after applying the attacks. In order to avoid this problem in our work various attacks are applied previously to the watermarked image for find out the points those are resist attacks. In this attack resistance points, we can encrypt the messages in later. For finding this optimal feature point from watermarked image  $W_i$  there are two types of attacks used. They are:

#### A. Predefined Attack

Attack like geometric distortion is called as the predefined attack. This type of attack, which results in synchronization errors by geometric distortions, makes a detector fail to detect the existence of watermarks even if they are still on the image. The different predefined attacks used in our work are:

- Intensity(50)
- Intensity(100)
- Line(1)
- Line(5)

#### B. Undefined Attack

Attack like noise like signal processing is called as the undefined attack. This type of attack intends to remove embedded watermarks from the cover image by a signal processing approach. The different undefined attacks used in our work are:

- Format(PNG)
- Format(JPEG200)
- Noise(0.05)
- Noise(0.1)

The aforementioned predefined and undefined attacks are applied in the image  $W_i$  and that attack applied image is represented as  $WA_i$ . From  $WA_i$  the points that are more stable after attacking has been find out, for that MPSNR value is used and is described in section 4.4.

### 4.4 Optimal feature point selection using MPSNR

The optimal feature point has been selected by using the MPSNR value and MPSNR is the modified version of the peak-signal noise ratio. MPSNR value is inversely proportional to that of attack resistance stability of points in an image.

Less MPSNR value of the image shows that image contains more attack resistance points. If the MPSNR value of an image is high which shows that the image contain less number of attack resistance points. In here the number of points which are generated from the SUSAN detector is randomly selected and each point MPSNR value has been calculated. In each point we have to apply the predefined attacks and undefined attacks and check which points are resisting the attacks. The points which are resisting various attacks are considered as the optimal feature points. For finding the MPSNR value equation (7) is used. The performance of the attack resistance point can be considered based on the MPSNR value. The low MPSNR valued images have the high attack resistance points.

$$MPSNR(db) = 10 \log_{10} \frac{H_{peak}^2}{MSE \times ANVF^2} \quad (7)$$

Where,  $H_{peak}^2$  is the peak value of the input image. The ANVF can be calculated based on equation (8).

$$ANVF = norm \left\{ \frac{1}{1 + \delta_{block}^2} \right\}, \in [0,1] \quad (8)$$

Where  $norm$  is normalization function and  $\delta_{block}^2$  is the difference between the minimum point and maximum point of a  $WA_i$  image. After finding the optimal feature points we can enter the signed messages into this point. So after applying the attacks on the watermarked images, the message content present in this points does not affected by any attacks.

## 5. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed Enhanced Fast Robustness Measurement in Vigorous Digital Image Watermarking via Selecting Optimal Feature Points is implemented in the working platform of MATLAB (version 7.12) with machine configuration as follows.

Processor: Intel core i7

CPU Speed: 3.20 GHz

OS: Windows 7

RAM: 4GB

In our proposed work the optimal feature points can be selected from the watermarked image by

applying various predefined and undefined attacks, for that the MPSNR value is considered. The SUSAN detector is used for the feature point selection from the original image. After that the watermarking is applied in this feature points and select the optimal feature points by applying various pre defined and the undefined attacks. In figure 2 the three different image samples from the database and feature points selection result by the SUSAN detector is shown.

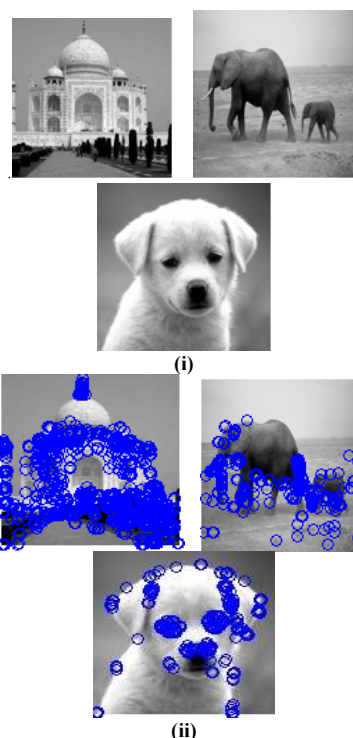


Figure 2: Image From (I) Original Image From Database, (Ii) Points Selection Using SUSAN Detector

The watermarking technique has been applied to the each feature points and that watermarked result images is given in Fig. 3.



Figure 3: Watermarked Image

After that in the watermarking process, we analyse the points which resist the attacks. For the analyses of attack resistance, various attacks are applied in the watermarked images. The image results from both predefined and undefined attacks which are shown in Fig. 4 and 5.

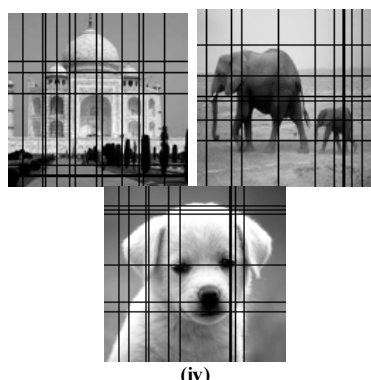
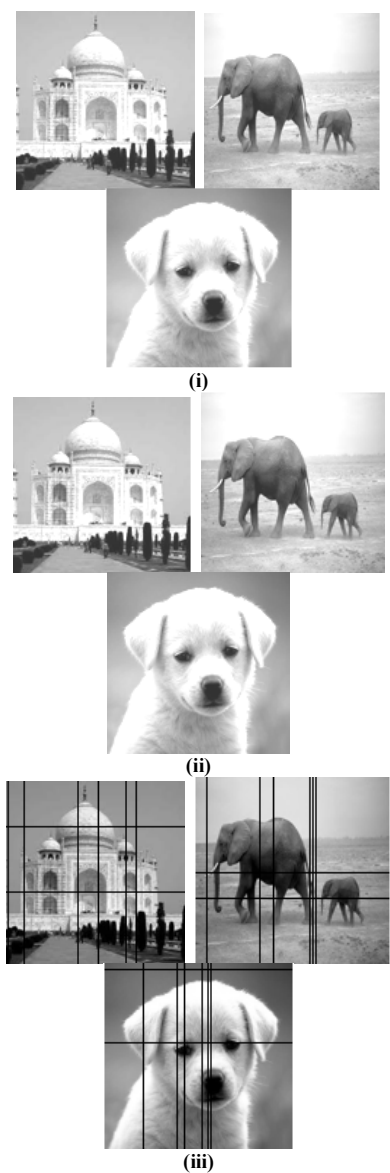
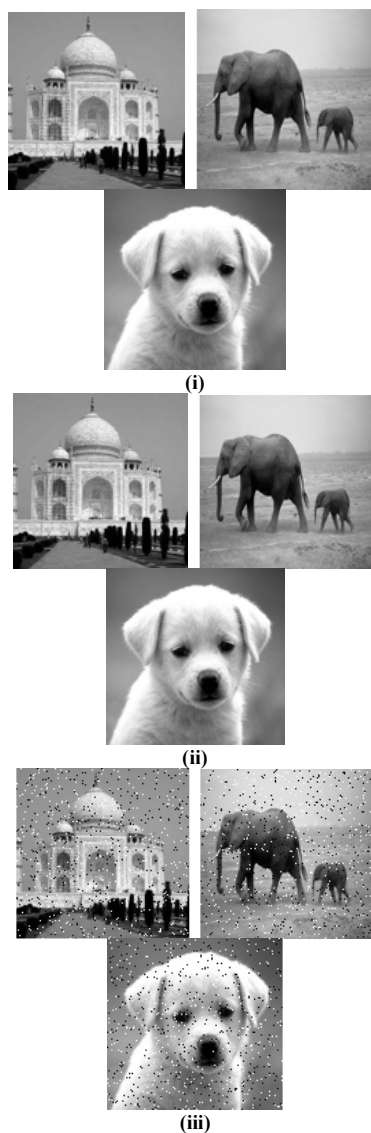


Figure 4: Predefined Attack Applied Image. (I) Intensity (50), (Ii) Intensity (100), (Iii) Line (1), (Iv) Line (5)





(iv)

Figure 5: Undefined Attack Applied Image. (I) Format (PNG), (Ii) Format (JPEG200), (Iii) Noise (0.05), (Iv) Noise (0.1)

In figure 6 shows the number of optimal feature points selected after analysing the attack resistance of each points by using the MPSNR value and the points which represent in the below three image does not affected by any attacks.

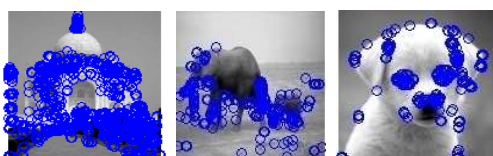

















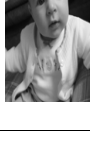



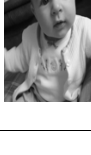
Figure 6: Result For Proposed Technique Of Optimal Feature Selected Points

After selecting the optimal feature points from the watermarked image the message that we want to encrypted in this optimal feature points. The optimal feature points have attack resistance stability. So the hackers cannot do any illegal and unwanted activities in this watermarked image.

### 5.1 Performance Analysis

Five image samples are taken from the database and the robustness of these five images after watermarking can be find out by applying various predefined and undefined attacks. Here table 1 various predefined attacks are applied in five images and the corresponding number of optimal feature points which resist the attacks is shown. E is the number of points which resist both predefined and undefined attacks. F shows that the number of points which are selected from SUSAN detector. The attack resistance of proposed method is described in this table.


















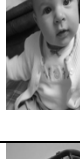





Table 1: PERFORMANCE OF PROPOSED METHOD WITH (I) INTENSITY (50,100), (Ii) LINE (1, 5)

Message	Serial No.	Original Image	Water marked Image	MPSNR	Applying Intensity Attack in watermarked Image		No of Feature points Resist the Attack(E/F)		Retrieved Image	MPSNR	
					(50)	(100)	(50)	(100)		(50)	(100)
HAI	1			11.84			24/24	24/24		76.90	76.90
	2			20.30			24/24	24/24		44.21	44.21
	3			0.5			24/24	24/24		65.25	65.25
	4			8.07			24/24	24/24		74.43	74.43



	5			27.63			24/24	24/24		36.87	36.87
--	---	-----------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	-------	-----------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	-------	-------	-------------------------------------------------------------------------------------	-------	-------

(i)

Message	Serial No.	Original Image	Water marked Image	MPSNR	Applying Line attack in watermarked Image		No of Feature points Resist the Attack(E/F)		Retrieved Image	MPSNR	
					(1)	(5)	(1)	(5)		(1)	(5)
HAI	1			11.84			24/24	16/24		75.47	77.02
	2			20.30			16/24	8/24		40.52	43.84
	3			0.5			16/24	16/24		62.75	65.51
	4			8.07			16/24	16/24		71.44	73.81
	5			27.63			24/24	16/24		33.02	36.33


(ii)

The performance of the predefined attacks of the five images is shown in table 1, from the performance analyse result shows that more number of feature points are resist the intensity (50) and intensity (100) attacks. Also there may an average
















level of feature points can the ability to resist the line (1) and Line (5) attacks. Similarly various undefined attacks are applied in this five images and corresponding optimal feature points has been shown.











TABLE 2: PERFORMANCE OF PROPOSED METHOD WITH, (I) FORMAT (PNG, JPEG200), (II) NOISE (0.05, 0.1)

Message	Serial No.	Original Image	Water marked Image	MPSNR	Applying Format Change Attack in watermarked Image		No of Feature points Resist the Attack (E/F)		Retrieved Image	MPSNR	
					PNG	JPEG200	PNG	JPEG200		PNG	JPEG200

HAI	1			11.84			24/24	16/24		11.84	36.40
	2			20.30			24/24	0/24		20.30	3.30
	3			0.5			24/24	0/24		0.514	24.57
	4			8.07			24/24	0/24		8.072	34.33
	5			27.63			24/24	16/24		27.63	4.272

(i)

Message	Serial No.	Original Image	Watermarked Image	MPSNR	Applying Noise Attack in watermarked Image		No of Feature points Resist the Attack (E/F)		Retrieved Image	MPSNR	
					0.05	1	0.05	1		0.05	1
HAI	1			11.84			16/24	8/24		73.38	76.22
	2			20.30			16/24	8/24		39.87	43.14
	3			0.5			24/24	8/24		61.61	64.80
















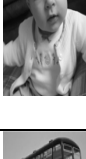
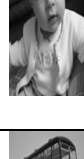


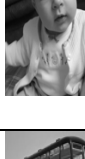





	4			8.07			24/24	8/24		70.9 1	73.58
	5			27.63			24/24	16/24		33.0 5	36.20

(ii)


















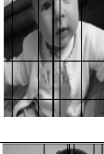

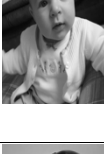





Performance analyse of the result shows that more point have the ability to resist format (PNG) attack and only limited points resist Format (JPEG200) while comparing with Format (PNG). The average number of points in a watermarked image has the ability to resist the undefined attack

(Noise (0.05)), but applying Noise (0.1) only limited point in the watermarked image has the resistance. The attack resistance of both predefined and undefined attacks in existing Method [25] represented in Table 3 and 4.

TABLE 3: PERFORMANCE OF EXISTING METHOD [25] WITH (I) INTENSITY (50,100), (II) LINE(1,5)











Message	Serial No	Original Image	Water marked Image	MPSNR	Applying Intensity Attack after watermarked Image		No of Feature points Resist the Attack (E/F)		Retrieved Image	MPSNR	
					(50)	(100)	(50)	(100)		(50)	(100)
HAI	1			13.09			48/48	32/48		73.62	78.80
	2			14.01			32/48	32/48		73.76	79.49
	3			14.01			48/48	32/48		73.66	78.89
	4			15.02			48/48	32/48		73.68	79.14
	5			16.23			48/48	0/48		73.75	79.17










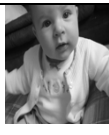





(i)

Message	Serial No	Original Image	Water marked Image	MPSNR	Applying Line attack after watermarked Image		No of Feature points Resist the Attack (E/F)		Retrieved Image	MPSNR	
					(1)	(5)	(1)	(5)		(1)	(5)
HAI	1			13.09			48/48	48/48		71.01	73.10
	2			14.01			48/48	0/48		70.01	73.26
	3			14.01			48/48	48/48		70.87	73.88
	4			15.02			48/48	48/48		69.66	73.70
	5			16.23			48/48	48/48		70.82	73.15
















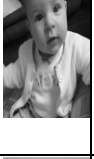
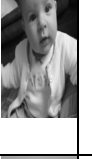








(ii)

TABLE 4: PERFORMANCE OF EXISTING METHOD [25] WITH (I) FORMAT (PNG, JPEG200), (II) NOISE (0.05, 0.1)

Message	Serial No	Original Image	Water marked Image	MPSNR	Applying Format Change Attack after watermarked Image		No of Feature points Resist the Attack (E/F)		Retrieved Image	MPSNR	
					PNG	JPEG200	PNG	JPEG200		PNG	JPEG200
	1			11.84			48/48	0/48		13.09	36.40
	2			20.30			48/48	0/48		14.01	3.30

HAI	3			0.5			48/48	0/48		14.01	24.57
	4			8.07			48/48	0/48		15.02	34.33
	5			27.63			48/48	0/48		16.23	4.272

(i)

Message	Serial No	Original Image	Watermarked Image	MPSNR	Applying Noise Attack after watermarked Image		No of Feature points Resist the Attack (E/F)		Retrieved Image	MPSNR	
					0.05	1	0.05	1		0.05	1
HAI	1			11.84			32/48	32/48		70.10	73.14
	2			20.30			48/48	16/48		69.18	72.69
	3			0.5			32/48	16/48		70.09	73.10
	4			8.07			16/48	48/48		70.09	73.07
	5			27.63			48/48	32/48		70.36	73.10

(ii)

The number of attack resistance points present in the existing method is less while comparing with the proposed technique. But in existing method, Line attacks have the more attacks resistance points than the proposed technique. The low MPSNR

value shows that points have the high attack resistance.

## 5.2 Comparative Analysis

In comparative analysis the performance of the proposed and the existing method is analysed based on the predefined and the undefined attacks. The performance of averaged MPSNR value of the existing and the proposed method are shown in figure 7.

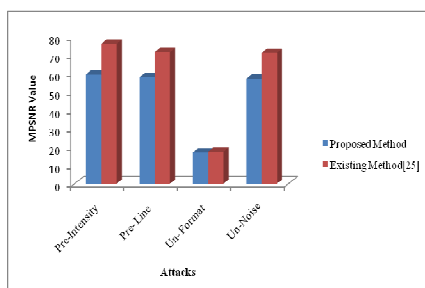


Figure 7: Comparative Analysis Of Proposed Method And The Existing Method

Here figure 7 the Pre-Intensity represents the predefined intensity attacks, Pre-Line represents the predefined line attacks, Un-Format represent the undefined format attacks and Un-Noise represents the undefined noise attacks. The MPSNR value and the attack resistance of the points are inversely proportional, i.e. increasing value of the MPSNR value has poor number of attack resistance points and the decreasing value of the MPSNR value has shown better number of attack resistance points. The Proposed methods have the average MPSNR value as 59.532, after applying the Predefined Intensity attacks. Similar way existing method [25] have the average MPSNR value as 76.396, which shows that the proposed method have 16.864 better performance than existing method. The predefined line attacks of our proposed method have the better attack resistance points comparing to the existing method. That means the average MPSNR value of the proposed method is less than that of existing method and the proposed method have 13.975 better performances than existing method. In undefined format attacks and undefined noise attacks also the attack resistance points of the proposed method is also high than that of existing method. From this we can conclude that the proposed method have better attack resistances than the existing technique.

## 6. CONCLUSION

In this paper, optimal feature points of the watermarked image have been found out. For finding the optimal feature point we used the MPSNR value. The proposed technique performance has been analyzed by taking five images from the database. The experimental results

proved that our proposed Optimal Feature Points selection from watermarked images has given high performance of optimal feature points and also which gives high robustness result. Moreover, in comparative analysis, our proposed technique performance is compared with the existing techniques. The comparison result shows that our proposed SUSAN detector with MPSNR value has given more Optimal point selection than the existing methods. In this we have applied various predefined (intensity (50,100), line (1, 5)) and various undefined attacks (format (PNG, JPEG200)) for finding the optimal feature points. The number of attack resistance points (Optimal feature points) of our proposed method is higher than that of existing method. In our proposed method have the both predefined and undefined attack resistance points comparing with the existing method. Hence, it is proved that our proposed technique more precisely detect the optimal feature region set.

## REFERENCES

- [1] Li Li, He-Huan Xu, Chin-Chen Chang and Ying-Ying Ma, "A novel image watermarking in redistributed invariant wavelet domain", *Journal of Systems and Software*, Vol. 84, No. 6, pp. 923–929, 2011.
- [2] Sujatha and Mohamed Sathik, "A Novel DWT Based Blind Watermarking for Image Authentication", *International Journal of Network Security*, Vol.14, No.4, pp. 223-228, 2012.
- [3] Babu, "A Robust Watermarking Algorithm for Image Authentication", *In Proceedings of International Conference on Information and Network Technology, Singapore*, Vol. 37, pp.220, 2012.
- [4] Manpreet Kaur, Sonika Jindal and Sunny Behal, "A Study of Digital Image Watermarking", *International Journal of Research in Engineering and Applied Sciences*, Vol. 2, No. 2, pp. 126, 2012.
- [5] Navnidhi Chaturvedi, "Various Digital Image Watermarking Techniques And Wavelet Transforms", *International Journal of Emerging Technology and Advanced Engineering*, Vol. 2, No. 5, pp. 363, 2012
- [6] Nallagarla Ramamurthy and Varadarajan, "The Robust Digital Image Watermarking using Quantization and Fuzzy Logic Approach in DWT Domain", *International Journal of Computer Science and Network (IJCSN)*, Vol. 1, No. 5, pp. 555, 2012.

- [7] RoslineNesaKumari, VijayaKumar, Sumalatha and Krishna, "Secure and Robust Digital Watermarking on Grey Level Images", *International Journal of Advanced Science and Technology*, Vol. 11, No. 1, pp. 1, 2009.
- [8] Nasir, Khelifi, Jiang and Ipson, "Robust image watermarking via geometrically invariant feature points and image normalisation", *Institution of Engineering and Technology Image Process*, Vol. 6, No. 4, pp. 354 – 363, 2012.
- [9] Aree Ali Mohammed and Haval Mohammed Sidqi, "Robust Image Watermarking Scheme Based on Wavelet Technique", *International Journal of Computer Science and Security (IJCSS)*, Vol. 5, No. 4, pp. 394, 2011.
- [10] Hamza A. Ali and Sama'a A. K. khamis, "Robust Digital Image Watermarking Technique Based on Histogram Analysis", *World of Computer Science and Information Technology Journal (WCSIT)*, Vol. 2, No. 5, pp. 163-168, 2012.
- [11] Habibollah Danyali, Morteza Makhloghi and Fardin Akhlagian Tab, "Robust Blind DWT Based Digital Image WaterMarking Using Singular Value Decomposition", *International Journal of Innovative Information and Control*, Vol. 8, No. 7, pp. 4691-4703, 2012.
- [12] Parthiban and Ganesan, "Hybrid Watermarking Scheme for Digital Images", *Journal of Computer Applications*, Vol. 5, No. 1, pp. 85, 2012.
- [13] Megha Kansal, Sukhjeet K. Ranade and Amandeep Kaur, "Fragile Watermarking For Image Authentication Using a Hierarchical Mechanism", *International Journal of Engineering Research and Applications*, Vol. 2, No. 4, pp.1759-1763, 2012.
- [14] Puneet Kr Sharma and Rajni, "Analysis of Image Watermarking Using Least Significant Bit Algorithm", *International Journal of Information Sciences and Techniques*, Vol. 2, No. 4, pp. 95 2012.
- [15] Priya, Santhi and Swaminathan, "Image Watermarking Techniques - A Review", *Research Journal of Applied Sciences Engineering and Technology*, Vol. 4, No. 14, pp. 2251-2254, 2012.
- [16] Mona M. Soliman, Aboul Ella Hassanien, Neveen I. Ghali and Hoda M. Onsi, "An adaptive Watermarking Approach for Medical Imaging Using Swarm Intelligent", *International Journal of Smart Home*, Vol. 6, No. 1, pp. 37, 2012.
- [17] Keshav S. Rawat, Sachin Goyal and Roopam Gupta, "Discrete wavelet based image watermarking: An idea leads to security", *Journal of Biometrics*, Vol. 1, No. 1, pp. 6-10, 2010.
- [18] Nikita Kashyap and Sinha, "Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)", *International Journal of Modern Education and Computer Science*, Vol. 4, No. 3, pp. 50-56, 2012.
- [19] RaghavenderRao, Nagabhooshanam, Bashu, SaidaNaik and Nikhil, "Image Watermarking Using Hybrid Wavelets and Directional Filter Banks", *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, Vol. 1, No. 3, pp. 146, 2012.
- [20] Venkatesan, Kannan and Raja Balachandar, "Optimization of Fidelity in Digital Image Watermarking Using a New Genetic Algorithm", *Applied Mathematical Sciences*, Vol. 6, No. 73, pp. 3607 – 3614, 2012.
- [21] Giulia Boato, Valentina Conotter, Francesco G. B. De Natale and Claudio Fontanari, "Watermarking Robustness Evaluation Based on Perceptual Quality via Genetic Algorithms", *IEEE Transactions on Information Forensics and Security*, Vol. 4, No. 2, pp. 207, 2009.
- [22] Chun-Hsien Chou and Kuo-Cheng Liu, "A Perceptually Tuned Watermarking Scheme for Color Images", *IEEE Transactions on Image Processing*, Vol. 19, No. 11, pp. 2966, 2010.
- [23] Chih-Chin Lai and Cheng-Chih Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition", *IEEE Transactions on Instrumentation and Measurement*, Vol. 59, No. 11, pp. 3060, 2010.
- [24] Ming Chen, Zhenyong Chen, Xiao Zeng, and Zhang Xiong, "Model Order Selection in Reversible Image Watermarking", *IEEE Journal of Selected Topics In Signal Processing*, Vol. 4, No. 3, pp. 562, 2010.
- [25] Jen-Sheng Tsai, Win-Bin Huang, and Yau-Hwang Kuo, "On the Selection of Optimal Feature Region Set for Robust Digital Image Watermarking", *IEEE Transactions on Image Processing*, Vol. 20, No. 3, pp. 735, 2011
- [26] Arathi Chitla and Chandra Mohan, "Authentication of Images through Lossless Watermarking (LWM) Technique with the aid of Elliptic Curve Cryptography (ECC)", *International Journal of Computer Application*, Vol. 57, No. 6. pp. 17-25, 2012.