Multimed Tools Appl (2018) 77:19235–19260
https://doi.org/10.1007/s11042-017-5351-0

A semi-blind HVS based image watermarking scheme using elliptic curve cryptography

Ritu Gupta[1] · Anurag Mishra[2] · Sarika Jain[1]

Received: 3 December 2016 / Revised: 23 October 2017 / Accepted: 25 October 2017 /
Published online: 11 November 2017

Abstract In the present paper, an advanced encryption technique commonly known as Elliptic Curve Cryptography (ECC) is used to embed a binary image as a watermark in five grayscale host images in a semi-blind manner. The ECC algorithm is a fast encryption technique which successfully encrypts the subject with significantly less number of bits as compared to other popular encryption algorithms such as Rivest-Shamir-Adleman (RSA) and Direct Selling Association (DSA). In the proposed watermarking scheme, embedding in the grayscale host images is carried out in DWT-SVD domain. First, entropy based Human Visual System (HVS) parameters are computed block wise to identify the most appropriate blocks in spatial domain. First level DWT is computed for these selected blocks and watermark embedding is carried out by using the calculated Singular Value Decomposition (SVD) parameters. Preliminary results of this work show that proposed scheme outperforms the other similar schemes carried out in DCT-SVD domain without using any encryption method. It is concluded that the use of DWT-SVD hybrid architecture along with the fast encryption technique ECC is responsible for better performance in present case. In the second part of this simulation, an established HVS model working in DCT domain is implemented and compared with the entropy based HVS model implemented in transform domain to embed the ECC encrypted binary watermark in images. In this case also, proposed scheme performs better both in terms of visual imperceptibility and robustness as compared to other scheme. It is concluded that HVS parameters – Luminance, Contrast and Edge Sensitivity are better placed

✉ Ritu Gupta
ritu4006@gmail.com

Anurag Mishra
anurag_cse2003@yahoo.com

Sarika Jain
ashusarika@gmail.com

[1] Amity University, Uttar Pradesh, India

[2] Deendayal Upadhyay College, University of Delhi, Delhi, India

in comparison to entropy parameters to examine image features and characteristics for watermarking purpose.

Keywords Human visual system · Elliptic curve cryptography · Discrete wavelet transform · Singular value decomposition · Image watermarking

Career:

I have started working in 2007 just after completing my B.Tech. My first job was in N.C college of engineering as a faculty in September, 2007. After that, I worked as a computer science faculty in Hindu College of Engineering and after that in B.M.I.E.T till June 2010.

I started working in Amity University, Noida from July 2010 onwards. I got enrolled in Ph.D part time from Amity itself from 2013 onwards..

1 Introduction

Digital watermarking is a method to minimize fraudulence, illegitimate replication and to improve copyright assurance and content authentication in the present era of web expansion on an exponential scale. The three essential requirements of digital watermarking are: 1) Visual quality of signed images, 2) Robustness of the embedding scheme and 3) Capacity of the host signal to hold the embedded watermark. However, there exists a trade-off between aforesaid requirements which means any two can be achieved at the cost of the remaining one. When the size of the watermark is kept too small, the capacity can be perceived to be a small contributor in this specific case. If some watermarking scheme focuses on improving the visual quality of the signed content, the robustness is compromised and vice versa. Therefore, the problem of watermarking of the digital content is presently taken up as an optimization problem. To this effect, several groups have proposed their schemes which are claimed to be efficient schemes in terms of maintaining a balance between the visual quality of watermarked image and the robustness.

Digital watermarking of images can be carried out in spatial and transform domain. The spatial domain watermarking exhibits low resistance against several image processing operations and is therefore classified as weak watermarking. On the contrary, the frequency domain methods such as those using DCT and DWT techniques are helpful to identify the potential locations to embed the watermark in order to obtain better results. The watermarking carried out in transform domain is therefore classified as robust watermarking. Cox et al. [9] have given a very detailed scientific description on how to enhance robustness of the watermarking scheme by using DCT technique and other issues related to this. They have also advocated the use of multiple scaling factors suitable for different image regions exhibiting different image characteristics such as variation in contrast level to get the watermark embedded. They claim it to be a better method which gives better quantified results mapped to robust watermark embedding and visual quality. Later, many other such methods have been proposed and published. However, an organized work in this direction was started when for the first time an attempt was made to optimize visual quality and robustness by the use of soft computing techniques. These soft computing techniques involve artificial neural networks of different architectures, fuzzy inference system, support vector regression methods and meta-heuristic techniques such as genetic algorithms and others [1, 3, 4, 11, 26, 27, 31, 33, 34]. All of these techniques attempt to maintain a balance between these two parameters and thus try to optimize the embedding and extraction processes. There is another development in this area which is quite important and interesting. This is the use of the Human Visual System (HVS) models for identifying suitable image locations either in spatial domain or in transform domain to embed the watermark. The HVS characteristics of the image are employed both with and without using the soft computing techniques for watermark insertion and extraction. To this effect, several groups have proposed successful HVS models to develop robust watermarking schemes. In the next section, a compilation of these HVS models is given.

In this paper, an advanced encryption technique – Elliptic Curve Cryptography (ECC) which uses less number of bits in comparison to its other popular counterparts such as RSA and DSA algorithms, is implemented to carry out image watermarking in DWT-SVD domain. The results are compared with a different scheme implemented in DCT-SVD domain without using any encryption / permutation of the watermark prior to its embedding. Further, we compare and analyze two commonly used HVS models to embed encrypted binary watermarks in gray scale images.

This paper optimizes the model designed by Chih-Chin Lai [16] by embedding encrypted watermark instead of a plain watermark. It enhances security because an advanced and fast Elliptic Curve Cryptography technique is used to encrypt the watermark. We extend this work by implementing it in DCT domain along with that in the spatial domain. The HVS model used by Agarwal et al. [2] to embed the encrypted watermark in DCT domain using DWT-SVD is used in the present work. The ECC technique is a powerful algorithm which has been used for number of other applications including those of image processing. However, we use ECC technique for the first time for image watermarking to the best of our information. This was done with a view to improve upon the existing results usually obtained by simple permuting of the watermark.

This paper is organized as follows: Section 2 describes earlier similar research work carried out in this direction. It compiles a number of Human Visual System (HVS) formulations used from time to time, followed by SVD method used for image watermarking. It further gives an introduction of the ECC technique which is used in the present work. Section 3 gives the motivation of the present work, followed by experimental details. Section 5 shows experimental results, discussion and analysis. It also deals with the second part of this simulation which analyses a comparison between two common HVS models used for watermarking in transform domain. Finally, Section 6 gives conclusion of the present work.

2 Earlier related work

This section discusses the literature survey on HVS based Watermarking, SVD based watermarking and Elliptic Curve Cryptography.

2.1 Human visual system based watermarking

As mentioned earlier, the HVS models can be successfully used to carry out watermarking in gray scale images both in spatial and transform domain. This is a powerful technique which is responsible for identification of appropriate image coefficients to carry out watermark embedding. The watermark coefficients embedded into these image coefficients using HVS yield a signed image better placed in terms of visual quality and robustness. The following is a brief survey of various HVS model based watermarking schemes developed by different research groups worldwide. Note that all these researchers have emphasized upon the importance of HVS characteristics to enhance visual quality and robustness of the watermark embedding algorithm.

Lou et al. [22] have used three parameters namely – luminance, frequency and texture sensitivities to model HVS watermarking of healthcare / medical images using a back-propagation neural network (BPN). They have carried out this watermarking in DCT domain by developing ten neural inference rules using three HVS parameters as input. They obtain an output which is used to embed the watermark in the host image using a pre-specified formula. Their results show that this scheme is able to survive various attacks in general and the JPEG lossy compression in particular. The authors claim that by the use of this technique, the medical practitioners can handle various difficulties on internet in the management of healthcare images.

Motwani et al. [29] have used Mamdani type Fuzzy Inference System (FIS) to embed watermarks in the host gray scale images. For this purpose, they use three HVS parameters namely – input brightness, texture and edge sensitivities. These parameters are initially fuzzified and fed to a Mamdani type FIS. The crisp output of the FIS is used to embed the watermark in the host image in the DWT domain. Their FIS uses a set of 20 fuzzy inference rules primarily based on the following observations of the Human Visual System:

1. *The eye is less sensitive to noise in those areas of the image where brightness is high or low.*
2. *The eye is less sensitive to noise in highly textured areas, but among these, more sensitive near the edges.*
3. *The eye is less sensitive in the regions with high brightness and changes in very dark regions.*

They use the formula given in Eq. (1) to embed watermark within the host image.

$$W_i^\theta(i,j) = I_i^\theta(i,j) + \alpha w_i^\theta(i,j) x_i^\theta(i,j) \tag{1}$$

where α = 0.001, w_i^θ= weighting factor computed by FPM, x_i^θ= pseudo random binary sequence, $I = 0,1,2,3$ and orientation θ ϵ 0,1,2.

Thus, the authors use the fuzzy logic for non-linear HVS model for perceptual masking in wavelet domain. They claim to have developed the fuzzy perceptual masks (FPM) with application to watermarking and compression without causing perceptual distortion. They further claim that the fuzzy based watermarks are robust to attacks and at the same time achieve a high level of imperceptibility. The fuzzy based masks also achieve a high compression ratio without causing perceptual distortion.

Mohanty et al. [28] have also analyzed HVS model for image watermarking. Their watermarking scheme is done block wise. A watermarked image block i_n' is obtained by modifying the original block i_n according to Eq. (2).

$$i_n' = \alpha_n i_n + \beta_n w_n, \quad n = 1, 2, \ldots\ldots \tag{2}$$

where α_n and β_n are scaling and embedding factors respectively, depending on the local statistics of the image computed by mean and variance of each block. They have used three parameters namely:- edge blocks of the image to be watermarked, the effect of variance across the blocks available in the host image and the computed value of the block intensity. According to the authors, the choice of α_n and β_n are governed by certain characteristics of Human Visual System which for the watermarking of the images can be translated to the following requirements:

1. The edge blocks of the image (to be watermarked) should be least altered to avoid any significant distortion within the image. For this purpose, only a small amount of watermark gray value can be added in the edge blocks of the host image. In other words, the scaling factor α_n should be close to α_{max} (the maximum value of scaling factor) and embedding factor β_n should be close to β_{min} (the minimum value of the embedding factor).
2. It is a well known fact that blocks with uniform intensity (having low variance) are more sensitive to noise than blocks with non-uniform intensity (having high variance). Therefore, only a small watermark should be added to the blocks having low variance and a stronger watermark can be added to the blocks with high variance. In view of this, we expect the scaling factor α_n to be inversely proportional to the variance where as the embedding factor β_n to be directly proportional to variance.
3. Another characteristics of HVS is that the blocks having mid-intensity values($\mu_n \approx \mu$) are more sensitive to noise than that of low intensity blocks ($\mu_n < \mu$) as well as high intensity blocks ($\mu_n > \mu$). This implies that α_n should increase with μ_n as long as ($\mu_n < \mu$) and should decrease with μ_n as long as ($\mu_n > \mu$). The mean gray value of each block is given by its DCT DC coefficient.

By using this HVS model exploiting the texture sensitivity of the image regions, they have implemented a visible watermarking scheme for gray scale images successfully.

Agarwal et al. [2] have used Luminance sensitivity, edge sensitivity as a function of threshold value and contrast sensitivity as a function of variance as three primary HVS characteristics which are block wise computed for the image in DCT domain. These characteristics are computed over the image blocks as follows:

(1) The Luminance Sensitivity: The DC coefficients obtained by computing DCT blocks of the host image are used to calculate Luminance sensitivity (L_i) according to formula given in Eq. (3),

$$L_i = \frac{X_{DC,i}}{X_{DCM}} \tag{3}$$

where L_i is the luminance sensitivity, $X_{DC,\ I}$ denotes the DC coefficient of the ith block and X_{DCM} is the average value of the DC coefficients of all the blocks combined together.

(2) The Edge Sensitivity: The edge is detected within the image by using threshold operation, in this case the edge sensitivity is computed by calculating the block threshold T. The Matlab image processing toolbox implements graythresh() routine. This routine computes the block threshold (T) using histogram – based Otsu's method [13]. The implementation of this routine passes the sub-image or block (f) during its call and is given by Eq. (4).

$$T = graythresh(f) \tag{4}$$

where graythresh is the matlab function for thresholding, f is the host sub-image (block) in question and T is the computed threshold value.

(3) The Contrast Sensitivity: It is well known that the regional image texture is represented by its contrast value which is further represented by the variance of the sub-image or the block in question. Thus, a Matlab routine proposed by Gonzalez et al. [13] to compute the block variance is successfully used for this purpose. The implementation of this routine passes the sub-image or the block (f) during its call and is given by Eq. (5).

$$\mathrm{T} = statxture(\mathrm{f}) \tag{5}$$

where statxture is the matlab function for computing block variance, f is the input image or the sub-image (block) and T is the output in the form of a 7 – element row vector, one of which is the variance of the block in question.

The three computed parameters – Luminance sensitivity, Edge sensitivity and Contrast sensitivity are fed to a *MAMDANI* type Fuzzy Inference System (FIS) as three inputs. The FIS is configured by the set of 10 inference rules as proposed by Lou et al. [22]. The FIS produces a crisp numerical value known as weighting factor as its output. The weighting factor is used to embed a watermark in the DCT domain of the host image using a formula given by Eq. (6).

$$\mathrm{X}^{'} = \mathrm{X} + \mathrm{k}^{*}\mathrm{w}^{*}\mathrm{p} \tag{6}$$

where X represents DCT coefficients of the low frequency band of the host image, w is the weighting factor as output of FIS, p is the watermark coefficient, k is the watermark multiplier coefficient or watermark embedding strength and X' is the DCT coefficient of the signed image.

The authors claim to have successfully implemented the FIS based watermarking of gray scale images. Their watermarking scheme is found to be robust against selected image processing attacks.

Maity and Kundu [23] have highlighted the usefulness of the average information (entropy) followed by appropriate mathematical formulations to select suitable embedding regions that satisfy the criteria of imperceptibility and robustness for image watermarking. They argue that when an image is perceived by HVS, the perceptual information is extracted not from a single pixel but from a group of pixels in its neighborhood. They report that a good measure of spatial correlation based on based on neighborhood criteria of pixels is average information or the entropy. For this purpose, they employ a modified form (exponential variant) of a widely used definition of Shannon's entropy as given by Eq. (7). This modified definition of Shannon's entropy is primarily developed by Pal and Pal [30] to estimate 2D spatial correlation for object segmentation and is used for image watermarking by [24].

$$\mathrm{H} = \sum \mathrm{p_i} \exp^{(\mathrm{u_i})} = \sum \mathrm{p_i} \exp^{(1-\mathrm{p_i})} \tag{7}$$

where $u_i = 1 - p_i$ is the ignorance or uncertainty of the pixel value. According to the authors, for calculation of average edge information, *i.e.* edge entropy of the image block in spatial domain, first the edge map is calculated using the conventional gradient operator. The strength of edge of a pixel automatically considers the effect of neighborhood pixel values. Therefore, the measure of edge entropy of the sub-image is dependent on the relative occurrence of the edge strength irrespective of their position. This implies that Shannon's form of entropy can be applied to calculate the average edge information of each block using the edge map. The entropy of the image blocks in spatial domain is calculated in this manner and is subsequently arranged in ascending order [15]. The authors claim that the blocks which exhibit median entropy values are the most suitable for watermark embedding after converting them into transform domain by using Discrete Hadamard Transform (DHT) technique.

Chih-Chin Lai [16] has proposed an improved SVD based watermarking technique considering the HVS characteristics. In the proposed watermarking plan, the characteristics of the image are taken into account to identify and select the blocks for watermark embedding. The twin criteria of visual entropy and edge entropy are used to identify the appropriate watermark embedding locations. The identified image blocks are then subjected to DCT and SVD. The watermark is inserted into these blocks by modifying the entries in the U orthogonal matrix component of each block. This is done with a view to preserve the visual quality of watermarked images and to increase the robustness of the watermark. This technique is claimed to satisfy both the requirements of the watermarking system - imperceptibility and robustness. This HVS model relies on the texture content of the image block in question. The author argues that the HVS model can be used both for measuring the perceptibility of watermarks after embedding and to control it during the embedding process. In this paper, Chih-Chin Lai considered the visual entropy and edge entropy, which are also used by Maity & Kundu [23] to identify appropriate regions within the host images which can satisfy the twin requirements of imperceptibility of the watermarks and the robustness of the embedding scheme. The main steps performed to incorporate the block selection for watermark embedding using the HVS model are: (1) A cover image is divided into n × n blocks and subsequently the visual entropy and edge entropy of each block are calculated (2) The two types of entropy for each block is then added up and the values obtained are sorted in ascending order. The entropy being a measure of disorder into the system, the block with the lowest value is therefore used for inserting the watermark. This is done until the number of selected blocks is equal to the number of bit-size of the watermark. The watermark insertion is carried out by computing the SVD of the DCT block selected by employing the HVS criteria based on entropy calculation described above. The author concludes that the use of HVS characteristics in this algorithm helps to identify appropriate regions of the image to achieve a good compromise between the robustness and visual quality of the signed image. According to the author, the results of this technique show significant improvement both in the visual quality and the robustness under different types of attacks.

2.2 Singular value decomposition based watermarking

The Singular Value Decomposition is a method to break down the image matrix into its three different components U, S and V. This is found to be connected to numerous applications which involve image pre-processing such as image compression [5], face acknowledgement [7], image improvement [32], watermarking [8, 14] and so on. As said earlier, the SVD decomposes the image matrix of size M × N into 3 different matrices:- U, S and V separately in a manner given below in Eq. (8).

$$[\mathrm{USV}] = \mathrm{svd}(\mathrm{A}) \tag{8}$$

Where the size of U is M × M and the size of V is N × N and both are unitary and orthogonal matrices. Eq. (9) gives the mathematical form of the column vector U.

U = $[u_1, u_2, \ldots\ldots, u_r, u_{r+1}, \ldots\ldots, u_m]$are the column vectors forming an orthonormal set i.e.

$$u_i^t u_j = \begin{cases} 1 & \textit{if } \mathrm{i} = \mathrm{j} \\ 0 & \textit{otherwise} \end{cases} \quad \textit{for } i = 1, 2, \ldots\ldots\ldots, m \tag{9}$$

Similarly, V is an N × N orthogonal matrix and is given by Eq. (10).

V = $[v_1, v_2, \ldots\ldots v_r, v_{r+1}, \ldots\ldots, v_n]$ are column vectors forming an ortho-normal set i.e.

$$v_i^t v_j = \begin{cases} 1 & \textit{if } \mathrm{i} = \mathrm{j} \\ 0 & \textit{otherwise} \end{cases} \textit{for } i = 1, 2, .., n \tag{10}$$

The S is a diagonal matrix of size M × M whose diagonal elements are singular values λ_i given by Eq. (11) as

$$\mathrm{S} = \mathrm{diag}(\lambda_i) \tag{11}$$

Where i = 1....m arranged in descending order.

2.3 Elliptic curve cryptography (ECC) technique

Elliptical curve cryptography (ECC) is a public key encryption algorithm which uses the concept of elliptic curve theory. It is primarily used to create faster, smaller and very efficient cryptographic keys. ECC relies on the properties of the elliptic curve equation instead of the traditional method of the product of very large prime numbers to generate keys. This algorithm can be used in conjunction with most public key encryption methods, such as RSA and Diffie-Hellman. Some research groups claim that ECC can yield a level of security with a 164-bit key which other systems require a 1024-bit key to achieve. The ECC also helps to establish equivalent security with a requirement of low computing power, it is becoming widely used for mobile applications. The ECC was developed by Certicom, a mobile e-business security provider, and was recently licensed by Hiffn, a manufacturer of integrated circuits and network security products. Little key size is the fundamental point of interest of ECC. The operations of elliptic bend cryptography are characterized more than two limited fields: Prime field and Binary field [6]. The suitable field is chosen with limitedly immense number of focuses for cryptographic operations. Here, we have utilized prime field operations by picking a prime number N, and unendingly substantial quantities of base focuses are produced on the elliptic curve, such that the created focuses are between 0 to N. At that point, we haphazardly select one base point P_i(x, y) for cryptographic operations and this point fulfils the mathematical statement of the elliptic bend on a prime field, which is characterized by Eq. (12) as

$$\mathrm{Y}^2 = \mathrm{x}^3 + \mathrm{ax} + bmodN \tag{12}$$

where (a, b) are the coefficients that define the curve, and x and y are the coordinate values of the generated point P. Fig. 1 depicts a real elliptic curve used in this algorithm.

Table 1 compiles the comparable key size in number of bits to implement encryption by the use of Elliptic Curve Cryptography and RSA / DSA techniques. It is clear ECC only requires 160 bit key to generate a security level which the RSA / DSA can only achieve with 1024 bit key. This feature of ECC makes it a faster technique to encrypt the original signal. May be in the future, this can further be improved so that it is successfully used to meet real time constraints.

3 Motivation of the present work

Nearly all image processing applications require "Secure Signal Processing (SSP) of the digital content. One of a very important branch which offers several cutting edge technology

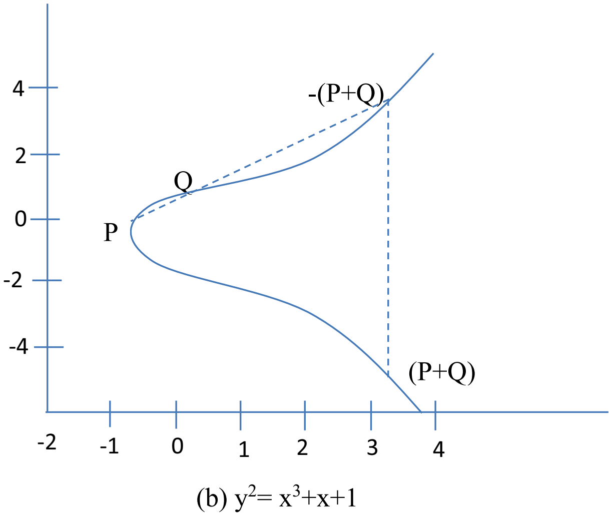


Fig. 1 Real elliptic curve

applications of image processing is computer vision. This branch is evolving in a close association of pattern recognition and itself requires strict implementation of SSP. It works equally well both for still images and video. Another category of image processing applications is based on regression problem which requires prediction of image features and processing based on selected features is carried out majorly in transform domain. The digital watermarking of images is a potential image processing application focussed towards checking copyright violations and content authentication, it requires secure processing of the digital content. There are two main issues involved into this problem. These are (1) embedding the watermark into the host signal and (2) extraction of the processed watermark from the signed and attacked signal to establish robustness of the embedding scheme. While there are numerous algorithms and techniques to carry out embedding, the watermark extraction may be blind, semi blind or non-blind. Although, watermark detectors are mainly classified as hard decision or soft decision detectors, yet the blind watermark extraction is widely evolving as a problem of pattern recognition. This may be carried out with or without using un-supervised machine learning techniques. Therefore, it becomes even more important to study few established research works in pattern matching of multimedia objects, especially those which are handled by using fusion of multiple datasets to obtain its reduced dimensionality. Ye Liu et al. [17] have successfully fused multiple datasets from different

Table 1 Comparable key sizes

Symmetric Scheme (Key size in bits)	ECC based Scheme (size of n in bits)	RSA/DSA (modulus size in bits)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15,360

domains to forecast the water quality of a station over a few next hours. Li Liu et al. [18] have developed a novel technique for recognizing complex activities by implementing a probabilistic interval based model. Their empirical evaluations on benchmark datasets indicate their technique outperforms existing state of the art methods for this problem. A very interesting seamless fusion of the data from multiple social networks for prediction of the futuristic career path is exhibited by Ye Liu et al. [20]. They fuse multiple data to comprehensively describe a user and characterize progressive properties of his or her career path. They accomplish it via multisource learning framework which jointly regularizes the source and career-stage relatedness. It may be possible to use the prediction framework proposed in this paper to predict selected coefficients suitable for potential image processing applications such as image watermarking.

The image and video watermarking may also find few security applications such as those of sensor based activity recognition. Ye Liu et al. [19, 21] have developed these applications. The proposed watermarking scheme can be integrated with these applications to enhance security. Jinshi Cui et al. [10] have developed an approach to track generic human motion via fusion of low and high dimensional tracking approaches. The tracking database may also need secure authentication. The proposed encrypted watermarking scheme can be integrated with this approach to accomplish this task.

With a target to establish SSP, the present experimental work derives its motivation from the use of encrypted watermark embedding within the given grayscale host images by using a hybrid DWT-SVD embedding scheme. This is particularly because it is clear that embedding of permuted watermarks usually produce better results in terms of robustness. First, the watermark is encrypted by using an advanced and fast Elliptic Curve Cryptography (ECC) technique in place of an ordinarily permuted watermark using an unknown key. The ECC algorithm is a fast encryption technique which successfully encrypts the subject with significantly less number of bits as compared to other popular encryption algorithms such as RSA and DSA. Moreover, the embedding in the grayscale host images is carried out in DWT-SVD domain. First, entropy based HVS parameters are computed block wise to identify the most appropriate blocks in spatial domain. First level DWT is computed for these selected blocks and watermark embedding is carried out by using the calculated SVD parameters. The proposed watermark embedding scheme is different from the one proposed by Chih-Chin Lai [16] on account of using ECC to encrypt the binary watermark. In addition to this, the proposed watermarking scheme is implemented in DWT-SVD domain while the one proposed by Chih-Chin Lai is implemented in DCT-SVD domain without using any permuted or encrypted watermark. This was done with an expectation to obtain better results in DWT-SVD domain using an encrypted watermark as compared to one proposed by Chih-Chin Lai [16]. Further, few operations such as – Median Filter (3 × 3), Gaussian Noise (10%), White Noise (5%), JPEG Compression (Q = 90) and Cropping are applied as attacks to examine the issue of robustness of the embedding scheme. Note that these are the same operations except white noise addition which are used by Chih-Chin Lai and are implemented in this work to establish comparison between the two schemes.

We further compare two established HVS models to carry out encrypted watermark embedding. In the second part of our simulation, a different HVS model proposed by Agarwal et al. [2] is implemented in DCT domain. As, the entropy based HVS model used by us in our first part and Chih-Chin Lai works in spatial domain, the watermark embedding scheme carried out in this part of the simulation is different than that used in the first part. Note that the HVS model used by Agarwal et al. [2] can only be applied in DCT domain. We therefore now modify and apply the entropy based HVS model used by Chih-Chin Lai in DCT domain. Moreover, both these HVS models are used for selection of appropriate blocks to carry out insertion of the binary watermark in DWT-SVD domain. For this purpose, a binary watermark which is first encrypted by ECC technique is used to improve the embedding results. The watermark embedding and extraction are followed by execution of five different operations as attacks to examine robustness of the present scheme. Our results are discussed, analyzed and compared with other similar works in section 5. Figure 2 shows a generic diagram of the embedding and extraction processes as carried out in the proposed work.

4 Experimental details

As mentioned in section 3, the complete simulation is divided into two parts. The embedding and extraction schemes carried out in this work use hybrid DWT-SVD architecture. Before that, the HVS parameters - visual entropy and edge entropy are computed block wise and appropriate blocks are selected. These blocks are subject to first level DWT which is further

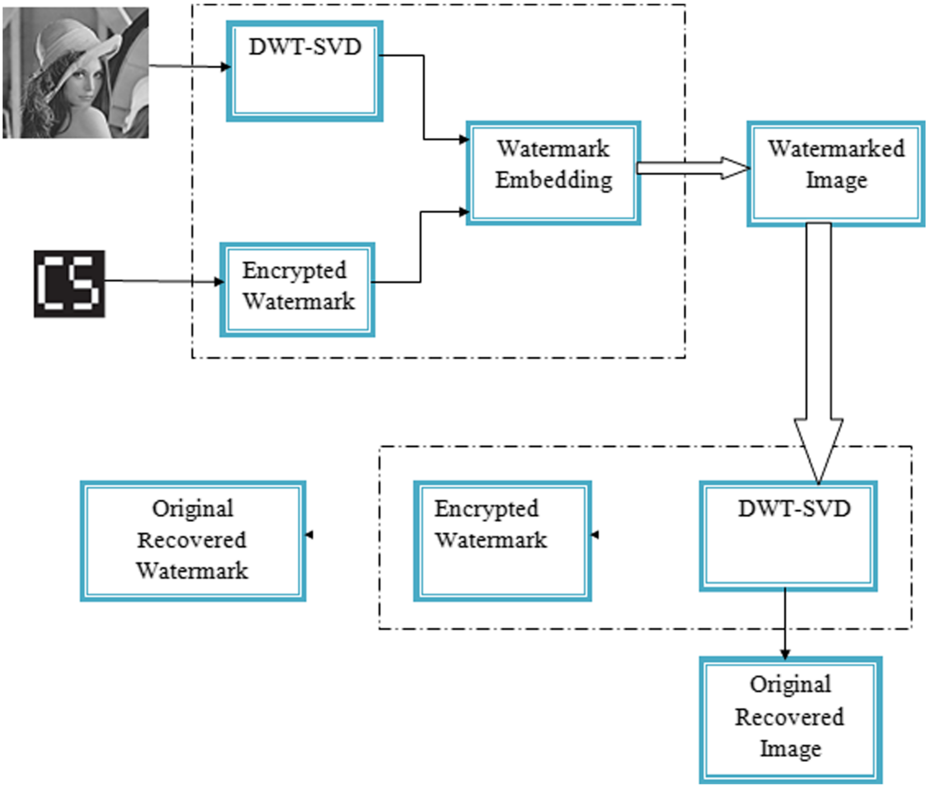


Fig. 2 Generic diagram of embedding and extraction processes of encrypted watermarking of the proposed technique

subject to computation of SVD parameters for the same block. The watermark is embedded by using a well defined formulation based on computed SVD parameters.

4.1 Watermark embedding scheme

For this purpose, a DWT-SVD hybrid architecture is used which decomposes the LL sub-band of the given host image matrix in its DWT domain into its three components:-[U, S, V]. In the present work, U component is used for insertion of an encrypted watermark. Listing 1 gives a step wise procedure of inserting the watermark into the host images in the present work. In this scheme, the gray scale host images are of size 512 × 512 and the watermark is a binary image of size 32 × 32.

4.1.1 Listing 1: Watermark Embedding Scheme

1) Encrypt the watermark using Elliptic Curve Cryptography (ECC) technique.

*2) The cover image is divided into 8*8non-overlapping blocks.*

3) Compute visual entropy and edge entropy of each block (as discussed in section 2.1) in spatial domain and arrange them in ascending order on the basis of total entropy obtained by adding the two values. Select the most appropriate blocks equal to the number of watermarked bits from the top of this sequence.

4) First level DWT is computed to the selected blocks and the CA sub-band is taken.

$$[\mathrm{CA}, \mathrm{CH}, \mathrm{CV}, \mathrm{CD}] = \mathrm{dwt2}\left(\mathrm{Bi},\ '\mathit{haar}'\right) \tag{13}$$

where CA is approximation sub-band,CH, CV and CD are detailed sub-bands, Bi is block under consideration and haar is the wavelet used for decomposition. SVD algorithm is applied on this sub-band and hence obtain U, S and V components by using Eq. (14)

$$[\mathrm{U\ S\ V}] = \mathrm{svd}\ (\mathrm{CA}) \tag{14}$$

where U and V are unitary matrices and S is diagonal matrix with non-negative integers arranged in descending order

5) Insert binary image watermark in first and second coefficients of the 1st column of the U matrix as per the equation:

If watermark = 1 bit, then

$$\mathrm{U}'(1,1) = -||\mathrm{U}(1,1)| + \left(\mathrm{Th}-\frac{\mathrm{D}}{2}\right)| \tag{15}$$

$$\mathrm{U}'(2,1) = -||\mathrm{U}(2,1)|-\left(\mathrm{Th}-\frac{\mathrm{D}}{2}\right)| \tag{16}$$

If watermark = 0 bit, then

$$\mathrm{U}'(1,1) = -||\mathrm{U}(1,1)|-\left(\mathrm{Th}-\frac{\mathrm{D}}{2}\right)| \tag{17}$$

$$\mathrm{U}'(2,1) = -||\mathrm{U}(1,1)| + \left(\mathrm{Th}-\frac{\mathrm{D}}{2}\right)| \tag{18}$$

where 'Th' is a threshold value,

$D = \left| U(1,1)U(2,1) - U(2,1) \right|$ and U' is the watermarked element.

6) Carry out inverse SVD on separate blocks to obtain watermarked low frequency sub-band by using Eq. (18)

$$CA' = U'^{*}S^{*}V' \tag{19}$$

where CA’ is the approximate watermarked band.

7) Compute Inverse DWT to obtain watermarked image.

Figure 3 shows the descriptive watermark embedding procedure.

4.2 Watermark extraction scheme

The watermark extraction scheme used in this work is semi-blind in nature. We neither use original host images nor any other parameter used while embedding for the purpose of extraction. We, however, use the same DWT-SVD hybrid scheme for extraction. This usage makes our extraction algorithm a semi-blind one. Listing 2 gives the extraction scheme in detail.

4.2.1 Listing 2: Watermark Extraction Scheme

*1) The signed image is divided into 8*8 non-overlapped blocks.*

2) The HVS parameters – Visual Entropy and Edge Entropy are computed for the blocks in spatial domain. Thus, calculate the total Entropy of the blocks and arrange them in ascending order to identify the most appropriate blocks. Select the blocks from top of this sequence equal to the number of bits in the binary watermark.

3) Compute first level DWT of the selected blocks of the signed image and apply SVD over the low frequency sub-band CA’ by using Eq. (20). Thus obtain three components U', S', V' of CA’.

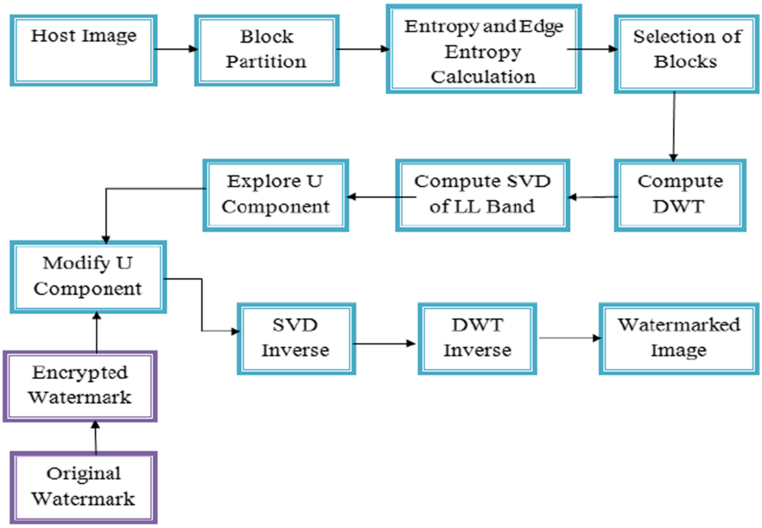


Fig. 3 Watermark embedding procedure of the proposed technique

$$\left[U^{'}S^{'}V^{'}\right] = \text{svd}\left(CA^{'}\right) \tag{20}$$

4) Extract the watermark bits from the first and second coefficient of the first column of U′ as follows:

If (| U(1,1)U(2,1) - U(2,1) |) > 0.

Watermark = 1 bit.

else.

Watermark = 0 bit.

5) Decrypt the watermark using ECC in order to reconstruct the original watermark.

Figure 4 shows a descriptive watermark extraction procedure of the proposed technique.

4.3 Quantitative analysis

The quality of the watermarked / signed images is quantified by using two full reference quality assessment metrics – PSNR and SSIM. The mathematical formulations for these two metrics are given by Eq. (21) and Eq. (22) respectively.

$$PSNR = 10log_{10}\frac{255}{MSE}(db) \tag{21}$$

$$SSIM = \frac{\left(2\mu_x\mu_y + C_1\right)\left(2\sigma_{xy} + C_2\right)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)} \tag{22}$$

where $\mu_x = \frac{1}{n}\sum_{i=1}^{n} x_i$ and $\mu_y = \frac{1}{n}\sum_{i=1}^{n} y_i$ are mean intensity or luminance component of image signals x and y respectively. $C_1 = (K_1\ L)^2$ and $C_2 = (K_2\ L)^2$ are constants with L being the dynamic range of the grayscale image (0–255) and $K_1 <<1$ and $K_2 <<1$ being small constants. Besides this,

$$\begin{aligned} \sigma_x^2 &= \frac{1}{n-1}\sum_{i=1}^{n}(x_i-\mu_x)^2, \qquad \sigma_y^2 = \frac{1}{n-1}\sum_{i=1}^{n}\left(y_i-\mu_y\right)^2 \text{ and} \\ \sigma_{xy}^2 &= \frac{1}{n-1}\sum_{i=1}^{n}(x_i-\mu_x)\left(y_i-\mu_y\right) \end{aligned} \tag{23}$$

In Eq. 23, σ_x and σ_y are signal contrast given by standard deviation for x and y respectively and is used to estimate contrast comparison for SSIM_Index. The structure of the two images is associated with the correlation (inner product) σ_{xy} between two unit vectors $(x_i$ - $\mu_x)/\ \sigma_x$ *and* $(y_i$ - $\mu_y)/\ \sigma_y$ lying in the image hyper plane.

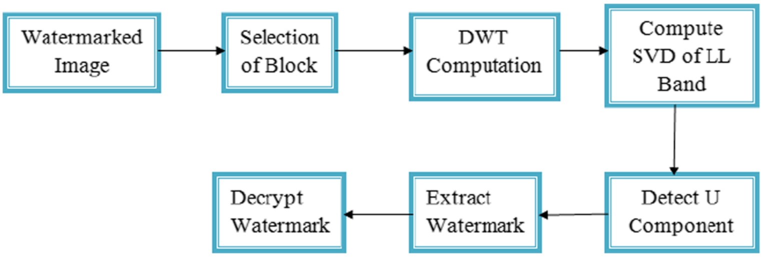


Fig. 4 Watermark extraction procedure of the proposed technique

4.4 Robustness of the watermarking scheme

In this part of the simulation, robustness studies are carried out over signed images. For this purpose, few image processing operations such as – Median Filter (Filter Aperture 3 × 3), 10% Gaussian Noise, 5% White Noise, JPEG Compression with Quality Factor Q = 10 and Cropping of a vertical rectangular section of size equal to 256 × 60 pixels from the upper left corner of the signed image which is replaced with white pixels (gray value = 255) are used as attacks to examine the issue of robustness of the proposed embedding scheme. Note that these are the same operations which are used by Chih-Chin Lai and are implemented in this work also to establish a comparison between the two schemes. The watermarks are extracted from the attacked images and the extracted watermark is compared with the embedded one by using Bit Correction Rate or.

BCR(W, W′) parameter. Here, W and W′ respectively are embedded and the extracted binary watermarks. The formulation for the Bit Correction Rate or BCR(W, W′) is given in Eq. 24. The results obtained after applying these attacks are compiled and analyzed in detail in Section 5.

$$BCR = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} \overline{W_{ij} \otimes W'_{ij}}}{M \times N} \tag{24}$$

Where W_{ij} and $W_{ij}{}'$ are embedded and recovered watermarks and M and N are dimensions of the image. For a square image, as in case of the proposed work, M = N.

5 Experimental results: discussion & analysis

Figure 5 depicts five different standard grayscale host images – Lena, Pepper, Baboon, Goldhill and Cameraman used for watermarking in the present work. Note that these are all 512 × 512 size images. A binary watermark of size 32 × 32 and its encrypted variant used in this work are shown in Fig. 6. The watermark is encrypted before embedding it into the host image to obtain better results. The embedding is carried out for four different numerical values of the threshold parameter ‘Th’. These value are Th = 0.002, 0.012, 0.02 and 0.04. Note that Chih-Chin Lai [16] has also used same numerical values for this threshold. He has given his computation results only for two standard grayscale images – Lena and Pepper with a binary logo watermark. We have presented our results on five grayscale images by using one binary image as watermark. The signed images for a threshold value Th = 0.02 are shown in Fig. 7.

Fig. 8 shows the recovered watermarks (CS) for the same threshold value Th = 0.02 from the signed images depicted in Fig. 5.

Note that there is no visual difference between the original host grayscale images and their signed counterparts. The computed values of PSNR and SSIM_Index are also high indicating that the visual quality of the signed images is quite good. The results here are shown for a threshold of Th = 0.02. The detailed results for all threshold values Th = 0.002, 0.012, 0.02 and 0.04 are compiled in Table 2 which also gives a comparison between the results obtained by us and those by Chih-Chin Lai [16] and Mehta et al. [25].

A comparison of the proposed watermarking scheme with that given by Chih-Chin Lai [16] and Mehta et al. [25] yields the following outcome:

Fig. 5 Host grayscale images:-(i) Lena, (ii) Pepper, (iii) Baboon, (iv) Goldhill and (v) Cameraman

1. Our scheme clearly outperforms the one proposed by Chih-Chin Lai [16] and Mehta et al. [25] except for Th = 0.002 for the Lena image.
2. There is a large difference between PSNR values for the two images – Lena and Peppers obtained by us and that reported by both [16, 25]. Although, we have reported the computed values of SSIM_Index which is another full reference metric to assess quality of the signed image, watermarking scheme reported in [16, 25] do not give any such result.
3. It is well known that a higher values of PSNR and SSIM_Index indicate better image quality, the reportedly obtained high values for this metric indicates that visual quality is not at all compromised in our watermarking scheme. This authenticates our contention that encrypting the watermark in fact improves the results.

Table 3 compiles the Bit Correction Rate (BCR) results obtained by us and one reported in [16, 25].

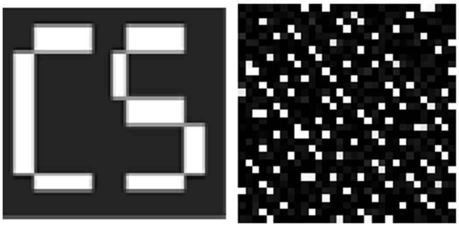
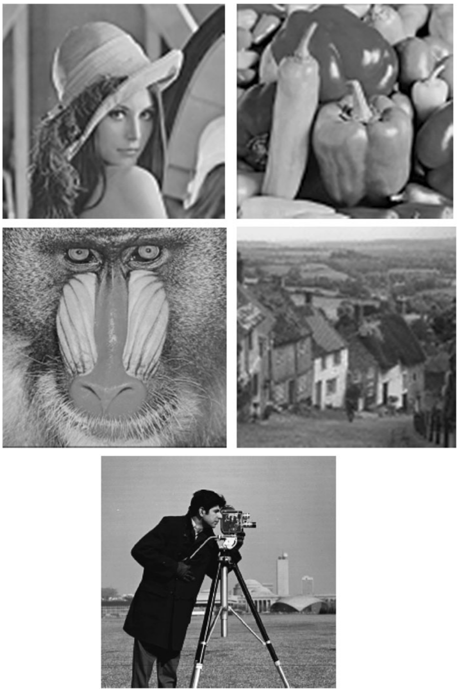


Fig. 6 Binary Watermark of size 32 × 32 and its encrypted variant

Fig. 7 Signed images for the binary watermark CS for Th = 0.02



It is clear from the Table 3 that except for Th = 0.002 for all five grayscale host images, the BCR is exactly equal to 1 which indicates perfect match between original and recovered watermarks. This also indicates that the recovery of the watermark from the signed images is quite successful. Chih-Chin Lai [16] and Mehta et al. [25] did not report numerical values for BCR parameter between embedded and extracted watermarks for their algorithm. Hence, no comparison can be done for this part of the experiment.

Table 4 presents a comparison for two signed images – Lena and Peppers for two different threshold values Th = 0.012 and 0.04 given for five different attacks used in this work. These two images and the two threshold values are taken into consideration as Chih-Chin Lai [16] and Mehta et al. [25] have used only these images and threshold values to simulate their watermarking scheme.

A comparison between the results presented in Table 4 clearly reveals the following:

1. In case of Lena image, the Cropping attack yields better results for the algorithm proposed by Chih-Chin Lai [16] and Mehta et al. [25] for both the threshold values. For all other attacks, the results obtained by our scheme are either same as that of other two works or better than them.
2. The similar or better results obtained by us are true for both the threshold values and for both the images into consideration here.

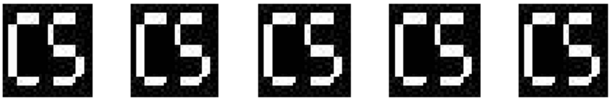


Fig. 8 Extracted watermarks from watermarked images for Th = 0.02

Table 2 PSNR and SSIM_Index computed values for all five images at different threshold

Name of Image	Threshold Value (Th)	PSNR Performance			SSIM_Index
		Chih-Chin Lai [20] (Binary Logo)	Mehta et al. [28]	Proposed Scheme	Proposed Scheme
Lena	0.002	61.69	61.73	61.32	0.9989
	0.012	49.37	50.87	51.77	0.9895
	0.020	44.75	47.55	47.61	0.9744
	0.040	38.51	41.08	41.68	0.9245
Peppers	0.002	56.20	60.08	69.29	0.9891
	0.012	50.20	52.16	52.08	0.9925
	0.020	45.73	48.24	49.11	0.9825
	0.040	39.61	42.41	43.91	0.9486
Baboon	0.002	N.A	N.A	50.76	0.9970
	0.012	N.A	N.A	48.24	0.9927
	0.020	N.A	N.A	45.54	0.9855
	0.040	N.A	N.A	40.69	0.9583
Goldhill	0.002	N.A	N.A	49.95	0.9949
	0.012	N.A	N.A	47.79	0.9876
	0.020	N.A	N.A	45.53	0.9775
	0.040	N.A	N.A	40.95	0.9497
Cameraman	0.002	N.A	N.A	59.18	0.9988
	0.012	N.A	N.A	53.12	0.9914
	0.020	N.A	N.A	49.09	0.9793
	0.040	N.A	N.A	43.38	0.9398

3. We attribute better results and proposed watermarking scheme outperforming the ones by Chih-Chin Lai [16] and Mehta et al. [25] to the combination use of advanced Elliptic Curve

Table 3 Bit Correction Rate (BCR) after extraction of watermarks for all five images at different thresholds

Name of Image	Threshold Value (Th)	Bit Correction Rate (BCR)		
		Chih-Chin Lai [20] (Binary Logo)	Mehta et al.[28]	Proposed Scheme
Lena	0.002	N.A	N.A	0.9916
	0.012			1
	0.020			1
	0.040			1
Peppers	0.002	N.A	N.A	0.9665
	0.012			1
	0.020			1
	0.040			1
Baboon	0.002	N.A	N.A	0.9529
	0.012			1
	0.020			1
	0.040			1
Goldhill	0.002	N.A	N.A	0.9627
	0.012			1
	0.020			1
	0.040			1
Cameraman	0.002	N.A	N.A	0.8941
	0.012			1
	0.020			1
	0.040			1

Table 4 Comparison of attacks for our scheme with the one proposed by Chih-Chin Lai [16] and Mehta et al. [25] for two threshold values Th = 0.012 and 0.04

Attacks	Lena						Peppers					
	For Th = 0.012			For Th = 0.04			For Th = 0.012			For Th = 0.04		
	Chih-Chin Lai [20]	Mehta et al.[28]	Proposed Scheme	Chih-Chin Lai [20]	Mehta et al.[28]	Proposed Scheme	Chih-Chin Lai [20]	Mehta et al.[28]	Proposed Scheme	Chih-Chin Lai [20]	Mehta et al.[28]	Proposed Scheme
Median Filter	0.96	0.99	0.98	1	1	1	0.83	0.86	0.89	0.94	0.95	0.95
Cropping	0.84	0.87	0.75	0.84	0.87	0.75	0.79	0.90	0.94	0.82	0.92	0.94
Gaussian Noise	0.59	0.65	0.98	0.95	0.88	1	0.59	0.61	0.94	0.85	0.82	0.99
White Noise	N.A	N.A	1	N.A	N.A	1	N.A	N.A	0.86	N.A	N.A	0.98
JPEG Compression	0.98	0.97	0.98	1	1	1	0.91	0.94	0.93	0.96	0.95	0.96

Table 5 Attacks applied to Baboon, Goldhill and Cameraman for Th = 0.012 and 0.04

Attacks	Baboon		Goldhill		Cameraman	
	For Th = 0.012 Proposed Scheme	For Th = 0.04 Proposed Scheme	For Th = 0.012 Proposed Scheme	For Th = 0.04 Proposed Scheme	For Th = 0.012 Proposed Scheme	For Th = 0.04 Proposed Scheme
Median Filter	0.82	0.99	0.60	0.94	0.75	0.97
Cropping	0.98	0.98	0.72	0.72	0.88	0.88
Gaussian Noise	0.77	0.98	0.63	0.94	0.79	0.96
White Noise	1	1	0.95	1	0.60	0.89
JPEG Compression	0.90	0.99	0.87	0.99	0.91	0.98

Cryptography encryption technique and hybrid DWT-SVD algorithm. This technique has not only resulted in better results in terms of visual quality of the signed images but also for the robustness studies carried out by applying attacks. Note that the use of DWT techniques improves the results only marginally over those obtained in case of DCT. The wide difference in results obtained in our case is primarily due to the use of ECC technique.

Table 5 compiles the results for attacks applied to remaining three signed grayscale images – Baboon, Goldhill and Cameraman for the two threshold values Th = 0.012 and 0.04 respectively.

As Table 5 compiles the results for additional images used in the present simulation, no comparison is made. But, one pattern is observed from both Table 4 and 5. That is, for a threshold value Th = 0.04, the results are the best for all attacks and for all images. A similar pattern is obtained by Chih-Chin Lai [16] and he uses Th = 0.04 to carry out further studies related to extraction of binary watermark logo from the attacked images. We also present attacked images for Th = 0.04 to carry out robustness studies. BCR parameter is used to establish match between embedded and recovered watermarks W and W′. Figs. 9, 10, 11, 12 and 13 respectively depict the watermarks extracted from Lena, Peppers, Baboon, Goldhill and Cameraman for Median Filter, Cropping, Gaussian Noise, White Noise and JPEG Compression attacks.

Note that all these watermarks are extracted after having these images undergone the attacks for Th = 0.04. A common observation can be made for watermarks extracted from attacked images for Th = 0.04. That is, the extraction in all these cases is quite successful. This indicates that the embedding scheme is robust enough at least against the selected attacks. The scheme proposed by Chih-Chin Lai [16] has also been able to resist these attacks and the binary logo watermark is successfully recovered for signed images obtained for Th = 0.04. The extracted watermarks are visually recognizable to be close to the embedded ones both in our scheme as well as that proposed by Chih-Chin Lai. Thus, both these schemes show successful watermark embedding and extraction processes. Moreover, both these schemes are found to be robust to

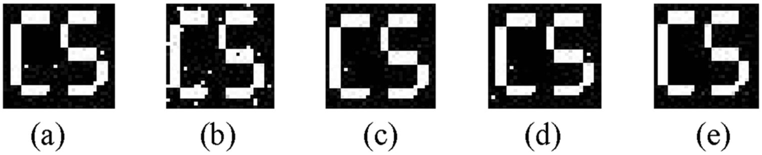


Fig. 9 Binary watermarks recovered from Lena after attacks for Th = 0.04 (a) Median Filter (b) Cropping (c) Gaussian Noise (d) White Noise (e) JPEG Compression

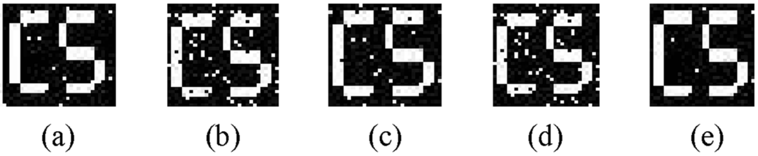


Fig. 10 Binary watermarks recovered from Peppers after attacks for Th = 0.04 (a) Median Filter (b) Cropping (c) Gaussian Noise (d) White Noise (e) JPEG Compression

the selected five attacks. However, in case of our scheme, the visual quality of the images after watermark embedding and the results obtained after executing attacks over the signed images are clearly superior to those proposed by Chih-Chin Lai. In case of Cropping geometrical attack, for the Lena image, the result obtained by Chih-Chin Lai is better in comparison to our result. As, both of these schemes have used entropy based Human Visual System (HVS) model in the spatial domain, we primarily attribute overall better results obtained in our watermarking scheme to the use of Elliptic Curve Cryptography method. A wide gap between the results of the two schemes indicates this. However, a marginal improvement in these results may also be due to the use of hybrid DWT-SVD architecture for embedding. This gap between the results should have been only minimal in case we had used a simple permuted watermark using an unknown key. Therefore, it is concluded that ECC is found to be quite suitable for watermarking applications.

6 Comparison on the basis Of HVS models

In the first part of this experiment, the inherent difference between the two schemes is on account of the use of Elliptic Curve Cryptography (ECC) technique used in our watermarking scheme. In both the cases, the HVS model used is based on computation of entropy parameters. In the second part of this experiment, we replace the entropy based HVS model with that proposed by Agarwal et al. [2] working in DCT domain. This model block wise computes three basic HVS parameters – Luminance Sensitivity, Contrast Sensitivity and Edge Sensitivity of the image. As this HVS model is only available in DCT domain, the watermarking scheme proposed by Chih-Chin Lai [16] was also modified to be applied with Entropy based HVS model in DCT domain itself. We call this as modified algorithm by Chih-Chin Lai and is done to establish a leveled comparison between the two watermarking schemes based on the use of HVS model. Tables 6 and 7 respectively present a set of compiled results for Lena and Peppers images for the two schemes in comparison both for the visual quality in terms of PSNR and SSIM_Index and for similarity between embedded and recovered watermarks in terms of BCR. Note that taking a clue from the first part of this simulation, the threshold value used in this part is Th = 0.04 only.

A close observation of results compiled in Table 6 and 7 yield following observations:

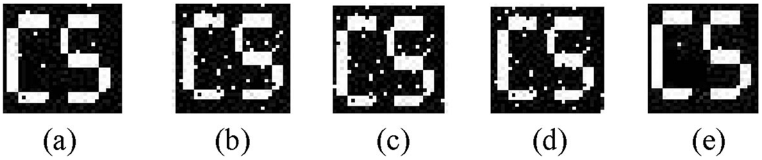


Fig. 11 Binary watermarks recovered from Baboon after attacks for Th = 0.04 (a) Median Filter (b) Cropping (c) Gaussian Noise (d) White Noise (e) JPEG Compression

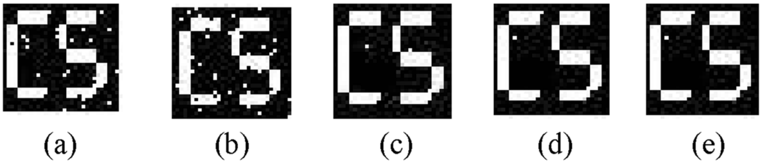


Fig. 12 Binary watermarks recovered from Goldhill after attacks for Th = 0.04 (a) Median Filter (b) Cropping (c) Gaussian Noise (d) White Noise (e) JPEG Compression

1. From both these tables, it is clear that the results obtained for PSNR, SSIM_Index and for Bit Correction rate (BCR) are all comparatively better in case of HVS model proposed by Agarwal et al. [2]. This proves that in DCT domain the HVS model used by Agarwal et al. [2] is more suitable for grayscale image watermarking. This is true because of the fact that entropy based HVS model will only compute the visual entropy and edge entropy parameters. As the entropy in any system indicates disorder into the system and the sum total of visual and edge entropy constitute total entropy of the image, usually a large perturbation within the image is required to be effective for a small variation in this quantity. On the contrary, in case of watermarking schemes as the size of the binary watermark is very small as compared to the size of the host or attacked image, the entropy based HVS parameters may not be exactly suitable to carry out watermarking. On the other hand, the HVS model relying on computing quantities such as Luminance, Contrast and Edge Sensitivities which represent image features is more suitable for this purpose. This is because these quantities do tend to change with even a small perturbation in the low frequency coefficients belonging to most appropriate regions of the image for watermarking purpose. In the first part of this simulation, we also implement the entropy based HVS model in spatial domain, hence the comparison between the schemes only accounts for the use of ECC by our scheme.
2. Having decided that ECC produces better outcome both for visual quality of signed images and the robustness parameters, a different ground is prepared to compare the two schemes based on the use of the HVS models – in this case, both the schemes use different HVS models applied in DCT domain. As stated earlier, our scheme outperforms the modified watermarking scheme proposed by Chih-Chin Lai. However, for cropping attack, the results obtained by modified Chih-Chin Lai scheme are better for both Lena and Peppers images. This observation is on the similar lines as obtained in the first part of the simulation.
3. It can be concluded that the watermarking scheme proposed by us is suitable for grayscale image watermarking both in the spatial domain and transform domain. The use of the advanced Elliptic Curve Cryptography (ECC) technique improves the performance of the scheme both in terms of the visual perceptibility and the robustness. The entropy based

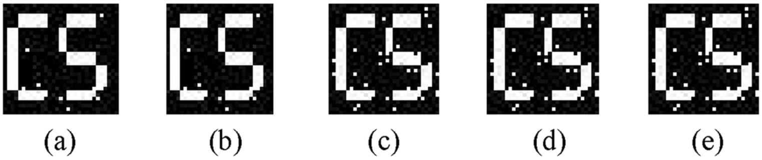


Fig. 13 Binary watermarks recovered from Cameraman after attacks for Th = 0.04 (a) Median Filter (b) Cropping (c) Gaussian Noise (d) White Noise (e) JPEG Compression

Table 6 Values of PSNR, SSIM and BCR of proposed schemes based on HVS models in DCT domain for Lena image for Th = 0.04

Attacks	PSNR		SSIM_Index		Bit Correction Rate (BCR)	
	Using Agarwal HVS Model [14]	Using Entropy based HVS Model	Using Agarwal HVS Model [14]	Using Entropy based HVS Model	Using Agarwal HVS Model [14]	Using Entropy based HVS Model
No Attack	40.9713	40.1289	0.9914	0.9861	1	1
Median Filter	35.7230	35.5820	0.8841	0.8783	0.8904	0.7420
Cropping	13.9271	13.9248	0.8514	0.8415	0.6968	0.8135
Gaussian Noise (10%)	30.1684	30.1332	0.8511	0.8466	0.8692	0.7582
White Noise	38.5055	37.9987	0.8158	0.8078	1	1
JPEGCompression (Compression ratio = 10%)	33.0121	32.9394	0.8874	0.8770	0.8117	0.6260

HVS model is not as suitable as the other model based on Luminance, Contrast and Edge sensitivity for all attacks except the Cropping attack.

7 Conclusions

In this research paper, a grayscale image watermarking scheme by taking into account the Elliptic Curve Cryptography (ECC) in the DWT-SVD hybrid domain is implemented. The Entropy based HVS parameters computed in spatial domain are used to embed a binary image as watermark in five different grayscale host images. The results for visual quality assessment and robustness before and after applying five attacks are analyzed with reference of another similar watermarking scheme proposed by Chih-Chin Lai. Our results are found to be superior in comparison to those of the other scheme. It is concluded that the better results obtained in our case is primarily due to the use of ECC which carries out a fast and efficient permutation of the binary image

Table 7 Values of PSNR, SSIM and BCR of proposed schemes based on HVS models in DCT domain for Peppers image for Th = 0.04

Attacks	PSNR		SSIM_Index		Bit Correction Rate (BCR)	
	Using Agarwal HVS Model [14]	Using Entropy based HVS Model	Using Agarwal HVS Model [14]	Using Entropy based HVS Model	Using Agarwal HVS Model [14]	Using Entropy based HVS Model
No Attack	41.6678	39.0961	0.9857	0.9710	1	1
Median Filter	40.7320	38.3491	0.9652	0.9639	0.7961	0.7031
Cropping	12.3500	12.3466	0.8819	0.8813	0.6968	0.6982
Gaussian Noise (10%)	31.4372	31.2960	0.9427	0.9420	0.7918	0.6583
White Noise	38.8810	37.3433	0.8921	0.8916	0.9724	0.9944
JPEG Compression (Compression ratio = 10%)	37.3908	36.4823	0.9493	0.9491	0.8746	0.8212

resulting in better embedding and extraction from the signed and attacked images. In the second part of this simulation, a well established HVS model given by Agarwal et al. [2] working in DCT domain is first implemented. As the entropy based HVS model is initially implemented in spatial domain, this was modified to be implemented in DCT domain. A comparison is made between the results on the basis of HVS models used. The HVS model used by Agarwal et al. [2] is found to outperform the entropy based HVS model both in terms of the visual imperceptibility and the robustness parameters. Overall, it is concluded that the proposed watermarking scheme is superior to the one proposed by Chih-Chin Lai and that the ECC is a very good candidate to improve watermark embedding and extraction performance.

8 Scope of the future work

We have used only two full reference metrics to assess the image quality of the signed and attacked images used in this work. These are PSNR and SSIM_Index. The first metric is a simple metric which actually amplifies the differential of luminance values between the source and target images and is not considered as a robust metric. On the other hand, SSIM_Index is widely being used as a replacement metric for quality assessment of images. This computes the structural properties of the images and is considered more robust as compared to PSNR. There is continuous research being done in this domain and newer quality assessment metrics are being evolved, some of which are quite suitable to these applications. As a scope to future work, we suggest that the quality assessment of signed and attacked images may also be carried out by using other metrics specifically used to compute the multimodal distortion such as GLZ model [12]. In this mode, the final score known as Most Probable Opinion Score or MPOS is calculated to subjectively assess the image quality [12].

References

1. Agarwal C, Mishra A (2010) A Novel Image Watermarking Technique using Fuzzy-BP Network. Proc Sixth Int Conf Intell Inform Hiding Multimed Sign Process, 102–105
2. Agarwal C, Mishra A, Sharma A (2011) Digital image watermarking in DCT domain using fuzzy inference system. In Twenty fourth IEEE Canadian conference on electrical and computer engineering (CCECE 2011); 822–825
3. Agarwal C, Mishra A, Sharma A (2013) Gray-Scale image watermarking using GA-BPN Hybrid Network. J Visual Commun Image Represent, Elsevier 24:1135–1146
4. Agarwal C, Mishra A, Mishra A (2015) A novel gray-scale image watermarking using hybrid Fuzzy-BPN Architecture. Egypt Inform J, Elsevier 16:83–102
5. Ashino R, Morimoto A Michihiro Nagase and Remi Vaillancourt "Image Compression with Multiresolution Singular Value Decomposition and Other Methods", http://www.crm.umontreal.ca/pub/Rapports/2900-2999/2939.pdf, pp. 1–17
6. Bakhtiari S, Ibrahim S, Salleh M, Bakhtiari M (2014) "JPEG Image Encryption with Elliptic Curve Cryptography" International Symposium on Biometrics and Security Technologies (ISBAST), Malaysia, 144–149
7. Cao L "Singular Value Decomposition Applied to Digital Image Processing" https://www.math.cuhk.edu.hk/~lmlui/CaoSVDintro.pdf, pp. 1–15
8. Chandra Mohan B, Srinivas Kumar S (2008) A Robust Image Watermarking Scheme Using Singular Value Decomposition. J Multimed 3(1):7–15
9. Cox IJ, Kilian J, Thomson Leighton F, Shamoon T (1997) Secure Spread Spectrum Watermarking for Multimedia. IEEE Trans Image Process 6(12):1673–1687

10. Cui J, Liu Y, Xu Y, Zhao H, Zha H (2013) Tracking generic human motion via fusion of low- and high-dimensional approaches. IEEE Trans Syst, Man, Cybernet: Syst 43(4)
11. Dey N, Samanta S, Chakraborty S, Das A, Chaudhuri S, Suri J (2014) Firefly Algorithm for Optimization of Scaling Factors during Embedding of Manifold Medical Information: An Application in Ophthalmology Imaging. J Med Imag Health Inform (4), 384–394
12. Głowacz A, Grega M, Gwiazda P, Janowski L, Leszczuk M, Romaniak P, Romano SP (2009) Automated Qualitative Assessment of Multi-Modal Distortions in Digital Images Based on GLZ. Ann Telecommun - Annales des Télécommunications 65(1):3–17
13. Gonzalez RC, Woods RE, Eddins SL (2005) Digital Image Processing Using MATLAB. Pearson Education, 406
14. Gupta R, Jain S, Mishra A (2015) Watermarking System for Encrypted Images at Cloud to check reliability of Images in IEEE Conference in NGCT-2015, 4-5 September. UPES, Dehradun
15. Kankanahalli M (1998), "Content Based Watermarking for Images", Proc. 6th ACM International Multimedia Conference, ACM-MM 98, Bristol, UK, 61–70
16. Lai C-C (2011) An improved SVD based watermarking scheme using human visual characteristics. Optics Commun (Elsevier) 284:938–944
17. Liu Y, Yu Z, Liang Y, Liu S, Rosenblum DS (2016) Urban Water Quality Prediction Based on Multi-task Multi-view Learning. Proc Twenty-Fifth Int Joint Conf Artif Intell (IJCAI-16)
18. Liu L, Cheng L, Liu Y, Jia Y, Rosenblum DS (2016) Recognizing Complex Activities by a Probabilistic Interval-Based Model", Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence (AAAI-16) February 12-17, Phoenix Arizona, USA
19. Ye Liu, Liqiang Nie, Li Liu, David S.Rosenblum," From action to activity: Sensor-based activity recognition", in Neurocomputing, Elsevier,Volume 181, 12 March 2016, Pages 108–115
20. Liu Y, Zhang L, Nie L, Yan Y, Rosenblum DS Fortune Teller: Predicting Your Career Path", Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence (AAAI-16)
21. Liuy Y, Niey L, Hanx L, Zhangy L, Rosenblum DS (2015) Action2Activity: Recognizing Complex Activities from Sensor Data. Proc Twenty-Fourth Int Joint Conf Artif Intell (IJCAI)
22. Lou D-C, Hu M-C, Liu J-L (2008) Healthcare image watermarking scheme based on human visual model and back-propagation network. J C.C.I.T 37(1):151–162
23. Maity SP, Kundu MK (2002) Information theoretic approach in spatial image watermarking. ICCVG 2002(25–29):1–6
24. Maity SP, Kundu MK, Nandi PK (2003) "Robust and Low Cost Watermarking Using Image Characteristics", In the Proceedings of ICAPR, Kolkata, India , pp. 351-354
25. Mehta R, Rajpal N (2013) A Hybrid Semi-Blind Gray Scale Image Watermarking Algorithm Based on DWT-SVD using Human Visual System Model", in Contemporary Computing (IC3), 2013 Sixth International IEEE Conference
26. Mehta R, Mishra A, Singh R, Rajpal N (2010) Digital Image Watermarking in DCT Domain Using Finite Newton Support Vector Regression. Sixth IEEE Int Conf Intell Inform Hiding Multimed Sign Process (IIH-MSP 2010), 123–126
27. Mishra A, Goel A, Singh R, Chetty G and Singh L (2012) "A Novel Image Watermarking Scheme Using Extreme Learning Machine", In Proceedings of IEEE World Congress on Computational Intelligence (WCCI 2012), Brisbane, Australia, June 10-15, 1–6
28. Mohanty SP, Ramakrishnan KR, Kankanhalli M (1999) A Dual Watermarking Technique for Images. ACM Multimedia, Part 2, pp. 49–51
29. Motwani MC, Harris FC Jr, (2009) Fuzzy Perceptual Watermarking for Ownership Verification. Proceedings of the 2009 International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV'09), Las Vegas, Nevada, July 13–16
30. Pal NR, Pal SK (1989) Object-background segmentation using new definitions of entropy. IEE Proceedings 139(4):284–295
31. Piao C-R, Beack S, Woo D-M, Han S-S (2006) A Blind Watermarking Algorithm Based on HVS and RBF Neural Network for Digital Image. ICNC 2006, Part I, LNCS 4221:493–496
32. Rowayda A. Sadek "SVD Based Image Processing Applications: State of The Art, Contributions and Research Challenges". Int J Adv Comput Sci Appl, Vol. 3, No. 7 (2012), pp. 26–34
33. Singh R, Dabas N, Chaudhry V and Mishra A (2014) "On Extreme Learning Machine for Watermarking of Images in Discrete Wavelet Transform Domain", In Proceedings of IEEE 10th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2014), 27–29 August, , Kitakyushu, Japan
34. Tsai H-H, Jhuang Y-J, Lai Y-S (2012) An SVD-based image watermarking in wavelet domain using SVR and PSO. Appl Soft Comput 12(8):2442–2453

Ritu Gupta (born October 25th, 1985) is an assistant professor in Amity University, Noida, Uttar Pradesh.