EAI Endorsed Transactions
on Energy Web

Research Article EAI.EU

A Novel Hybrid Watermarking scheme with Image authentication based on frequency domain, 2- Level SVD using chaotic map

Shahzad Alam[1,*], Tanvir Ahmad[1] and M. N. Doja[1]

[1]Department of Computer Engineering, Faculty of Engineering and Technology, Jamia Millia Islamia, New Delhi-110025, India

Abstract

INTRODUCTION: In order to protect the owner's visual multimedia data, various watermarking methods have introduced in the last few years. In image watermarking techniques, a secret watermark image inserted into another image.
OBJECTIVES: The main aim of this paper is to implement an image watermarking technique having high security from stealing the information hidden in image and make the resultant image more robust against various attacks.
METHODS: In this paper, frequency domain based techniques like DWT, DCT has used with 2 Level SVD and a new 3D discrete hyper chaotic map. The digital signature and other image parameters have appends in the watermark image to ensure the security and copyright protection of the original image using RSA, Arnold transforms, and SHA-1, techniques. At the receiver side, digital signature and information parameters have retrieved from the watermark image and identify to detect whether an unauthorized person attacks the watermark image or not. To verify the originality of image, the extracted information parameter, and the hash value of the extracted watermark have compared with the original value of the parameters and source hash value of the watermark image, respectively. The secret key used in the proposed scheme that makes the system more robust and adds security to the system. It helps to authenticate the originality of the received image.
RESULTS: We compare the result with the present scheme proposed by Lin at el. The experiments have conducted to check various standard image processing attacks, and the watermark extraction process generates a high-quality image after different attacks. The primary purpose of the suggested watermarking scheme is to ensure reversibility and high security.
CONCLUSION: The experimental outcomes confirmed that not only the recommended scheme attained higher robustness and imperceptibility in comparison to our earlier scheme. The Watermark image also recovered successfully with the known secret key.

Keywords: DCT, DWT, SVD, SHA-1, RSA, Arnold transform, Chaotic Map, Secret Key

Received on 29 March 2020, accepted on 30 June 2020, published on 07 July 2020

doi: 10.4108/eai.13-7-2018.165512

*Corresponding author. Email:shahzad5alam@gmail.com

1. Introduction

Today the Internet has transformed the whole world into a global village of sharing and transferring digital data such as video, audio, images, etc. [1]. At the same time it creates illegal duplicate copies by hackers or unauthorized persons that seriously affect the author's copyright. The resulting problems cause copyright protection and security [2]. Therefore, how to avoid copyright violations and protect intellectual property has attracted worldwide attention from some researchers. The varieties of methods used for the purpose are cryptography, steganography and watermark.

To handle the first issue of copyright protection, Information Hiding Techniques (IHT) is necessary [23]. Generally, the IHT should satisfy four basic requirements such as volume, security, robustness, and noiselessness. But normal IHTs do not meet all these requirements, cause a tradeoff relationship. The embedding of a large amount of message inside the digital image cause apparent artifact, but enhancing the noiselessness will reduce the volume of the embedding message. Hence, needs of suitable information (data) hiding techniques based on the applications [4] is required. According to that, the IHTs are categorized into two groups of Transform Domain (TD) and Spatial Domain (SD) [17]. In SD, a direct modification is performed inside the content value of the pixel of the input image during message embedding. The following types of techniques used are Least Significant Bit Insertion (LSBI), patchwork, and vector quantization. The advantage of SD has a higher embedding capacity, and it has lower computational complexity. But in TD, the message embedding is performed by modulating the transform domain coefficients such as Discrete Cosine Transformer (DCT) [32], Lifting Wavelet Transform (LWT), Discrete Fourier Transformer (DFT), Discrete Wavelet Transformer (DWT) and Singular value Decomposition (SVD) [7,9]. They can be applied either separately or together according to the need of requirements. Recently, reversible data embedding techniques are introduced [8].

Considering the second issue of security in the information system, proper image identity assurance and integrity is necessary [22]. The image integrity means identifying the received image is a correct image from an accurate source. Image integrity involves making a confirmation on original images that no changes have been made during processing and transferring acquired from a medical imaging device. To undergo identity and integrity security issues, Digital Image Watermarking (DIW) techniques are introduced for images for copy right protection [26]. DIW embeds the secret information in the form of a digital image, hence it is difficult to remove or change the content from a digital image. According to their robustness, they are categorized into fragile, semi-fragile, and robust techniques. On the receiver side the hidden image is retrieved by the watermark extraction process. The tamper detection of digital data and copy control is considered as the main objective in digital watermarking to be achieved. The requirement should be consider while performing good watermarking technique is, the embedded information do not degrade the quality of the host image[28].

Sometimes, information present in an image is in non-uniform nature and distributed across the images. Some of the parts include more information than other parts. Thus several schemes are utilized in separating various regions and objects in medical images. According to that, the medical image has split into two areas, such as the Area of Interest (AOI) and Area of Non-Interest (AONI) [19,16]. The two domains utilized for inserting the watermark that contains secure information in the image is Pixel Domain (PD) and Coefficient Domain (CD). In PD original image pixels are directly altered with the watermark bits. This method is easy to implement, produces less computational cost and has a high payload, but most of the PD offers the least robustness. In CD, the frequency coefficient of any transform is altered based on watermark bits. Where DCT and DWT are the most common frequency domain transform techniques used in the CD watermark method [21]. The PD and CD also called SD and TD. Performing digital watermark in SD, the data is directly embedded in pixels in replace of the pixel bits into data bits. But it is not robust when a high payload is required and produces lossless compression. But performing digital watermark in TD, the coefficients of the cover medium are highly modified offers more security and high robustness during inner and outside attacks [15].

The main aim is, to make the algorithm robust and secure. In this paper, a secure hybrid and robust image watermarking (RIW) scheme based on DWT, DCT, 2-Level SVD and a new 3D discrete hyper chaotic map for the information hiding technique is proposed.

The paper is organized in different sections. In section 2 literature survey has done. In section 3 preliminaries, a brief overview of the above terms is discussed. In section 4, the proposed schemes, tools, and techniques used have discussed. In the next section 5, the experiment result has discussed. In the last section, conclusions have discussed.

2. Literature Review

Some of several encryptions transform domain and steganography techniques used in watermarking to improve the security and robustness is given below.

Hurrah et al. [1] aimed a hybrid transformation domain watermark scheme for an efficient watermark. The main goal is to resist dual attacks of image processing attacks and geometric attacks. For this, the author uses multiple encryption techniques to increase the security of the information content present in the watermark image and used a principle of maximum probability to select the bits of encrypted watermark for a color image. The resultant evidence is highly robust in image processing attacks not for geometric attacks.

Anand et al. [29] proposed a robust and secure watermarking technique. In this paper secure patient data is embedded using DWT-SVD techniques in medical image then the resultant image is encrypted and compressed. Finally encrypted image is transmitted for communication channel.

Ye, et al. [30] propose a new image encryption algorithm based on compressive sensing and information hiding technology using DWT. In this logistic-tent map is used for creating randomness in image pixel. Ramasamy, et al. [31] proposed enhanced logistic map to encrypt the image using modified zigzag transformation. The results show that system is secure, reliable and good efficiency.

Chen and Xu [6] proposed a robust and secure color image watermark scheme for copyright protection based on the LWT domain to decompose the watermark and

host image into multiple sub-bands. The text and watermark images used are RGB color images. To demonstrate the solidity of the scheme in the watermark image various medium filtering image processing attacks, cropping attacks, etc. are applied. But in this method, only the original image is calculated for imperceptibility, do not consider volume and robustness.

Abdel hakim et al. [5] proposed a Time Efficient Optimization (TEO) method based on Machine Learning (ML) approach. The aim of this method is to find best-embedded strength parameters for RIG technique. Initially, they designed the DCT domain to find the common watermarking attacks. Then applied a watermarking to train the image and used an Artificial Bee Colony (ABC) algorithm to optimize the parameters to extract the features of the image with best fitness value. Finally, the optimum embedded parameters are predicted by the K-Nearest Neighborhood regression method.

Loan et al. [10] presented a DMI technique with Chaotic Encryption (CE) for both color and gray scale images [20]. Before embedding the secured watermark in the input image, the DCT coefficient operation has performed to avoid the overlapping problem. Then double-layer security is used in the embedding stage using the Arnold transformation in CE. The result shows better achievement in terms of security, noiselessness, and robustness.

Singh AK [11] used three TD techniques of DCT, DWT, and SVD for hybrid watermarking. In the initial stage, the S vector of the watermark information inserted in the S segment of the source image. The generated watermark is performed by inverse Singular value decomposition in a modification of S vector and by U, V vector by inverse DWT and DCT. An extraction algorithm extracts the secured watermark. Finally, an encryption method is embedded into the cover image to perform security and reduce the storage capacity and bandwidth in the source image[33].

Yahya et al. [12] explain a robust watermarking algorithm which is based on the Probabilistic Neural Network (PNN) in the DWT domain with the Haar filter. The Haar filter is used to incorporate the image of the binary watermark into the corresponding coefficient wavelet blocks. To extract the image of the watermark, PNN is applied between the watermarks to evaluate the efficiency and quality of the image. Finally, the demonstration is performed in Normalized Cross Correlation (NCC), Peak to Noise Ratio (PSNR) and some common attacks.

Chen et al. [13] designed a scheme based on DWT in which logo is verified without using original host image. Sanjay Rawat and Balasubramaniam Raman [3,14] proposed a scheme using discrete cosine transform and logistic regression on grey scale image without the presence of host image for logo verification[24,25]. The secret key is obtained using the original source image but can't be easily seen by human eyes. This theory was applicable only for grey scale image but not for the color image. This paper presents the application on color host image and color watermark embedding / extraction method.

In the different watermarking schemes, some use secret text images to be hidden in digital images and finally encrypted the image to obtain an encrypted watermarked image. Many algorithms use a different encryption algorithm to encrypt the watermarked image. In our paper, we have the first encrypted watermark logo with some additional information on it. And embed encrypted watermark image into source image using a new proposed chaotic map. The new chaotic map is hyperchaotic and very sensitive to the initial value of the map as discussed in section 3, which adds security in the system that prevents sensitive information from the unauthorized person.In this paper, hybrid digital watermarking is carried out using DWT, DCT, 2- Level SVD and new chaotic map which is a novel scheme for image has discussed.

3. Preliminaries

In this preliminaries section, we explain the DCT, DWT, SVD, SHA-1, RSA, Arnold transform and proposed 3D discrete hyper chaotic map requisite needed in our proposed technique.

3.1. 2D Discrete Cosine Transform (DCT)

The transformation is a major component in the processing of multimedia data applications. In the transformation for an image, pixels display some correlation with their neighbouring pixels in a single image. Also, pixel value is easily calculated from its nearest neighbours by using this correlation. Therefore, a transformation of pixels shows how correlated coefficients maps into uncorrelated coefficients [18].

The DCT converts/transforms an image pixels or the signal values from the spatial (correlated) to the frequency domain (uncorrelated).

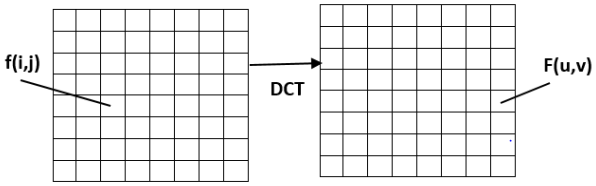

Fig 1. Pixels transformation

The following equation governs 2D discrete cosine transform (DCT):

$$F(u,v) = \frac{2}{\sqrt{MN}} P(u)P(v) \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} f(i,j)$$

$$* \cos\frac{(2i+1)u\pi}{2M}\cos\frac{(2j+1)v\pi}{2N} \quad (1)$$

The inverse cosine tranform for the aboce eqaution is:

$$f(i,j)=\frac{2}{\sqrt{MN}}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}P(u)P(v)F(u,v)$$
$$* \cos\frac{(2i+1)u\pi}{2M}\cos\frac{(2j+1)v\pi}{2N} \quad (2)$$

Here f (i, j) is pixel without transformation and F (u, v) is pixel after transformation. M and N are block size for DCT.

$$P(u)=\begin{cases}\frac{1}{\sqrt{2}} & if\ u=0\\ 1 & otherwise\end{cases}$$

$$P(v)=\begin{cases}\frac{1}{\sqrt{2}} & if\ v=0\\ 1 & otherwise\end{cases}$$

When m=0 and n = 0, then Eq. (1) can be represented as:

$$F(0,0)=\frac{1}{sqrt(MN)}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}f(i,j) \quad (3)$$

where F(0,0) in eq. 3 is DC coefficients and others are AC coeeficients.

3.2. Discrete Wavelet Transform

The wavelet transform of signal done by discrete wavelet transform (DWT) using distinct sets. It has widely used in image watermarking techniques. The DWT decomposes an image into the frequency domain having frequency sub-bands. DWT is the most common frequency domain transform technique used in the coefficient domain. It converts the signal into two parts; one part contains the high-frequency component (HFC), and the other includes the low-frequency component (LFC). The information about the edge component of the image is contained in the high-frequency component. And low-frequency component is further decomposed into low and high-frequency components. The human eyes are sensitive to changes made in non-edge portions. Usually, HFC is suitable for watermarking techniques because changes done in HFC are indistinguishable by the human eye. In an image processing first DWT is applied in a vertical direction than in the horizontal direction. After using the DWT image is converted into the frequency domain, it contains four frequency sub-bands named as High High (HH), Low High (LH), Low Low (LL), and High Low (HL). The LL frequency sub-bands has used as input for further decomposition.

3.3. Singular Value Decomposition (SVD)

Singular value decomposition (SVD) is a standard transform applied in various numerical analysis. By using SVD, a matrix could be decomposed into eigenvalues and eigenvectors. For a given matrix, the SVD can be represented as given below:

$$A \Rightarrow USV^T \quad (4)$$

In equation 4, 'V' represents the right singular vectors and 'U' represents left singular vectors. S matrix are called diagonal matrix. S is represented as:

S = diagonal (λ_1, λ_2 , λ_3, …. , λ_r)

where $\lambda 1 \geq \lambda_2 \geq \lambda_3 \ldots\ldots\ldots\ldots \geq \lambda_r$ are called the singular values of A matrix. The singular values have high energetic parts and produce excellent stability. It can resist the slight irregularities in image processing. Also, the SVD can be applied to any arbitrary matrix [34]. In addition to that, the SVD transform technique has widely utilized in various robust watermarking schemes.

3.4. SHA-1 Hash Generation

SHA-1 is an acronym as a “Secure Hashing Algorithm.” It is proposed by the US National Security Agency (USNSA) and issued by NIST. It is a hash algorithm and has better performance than the previous SHA-0 algorithm. It becomes more popular after published in 1995. It produces the 160 bits of message digest size. Nowadays, there are various versions of secure hash function has implemented like SHA-224, SHA-256, SHA-384, and SHA-512. SHA-512 hashing uses 512bits for message digest size, and block size is 1024bits. In this paper, SHA-1 hashing technique has used, which generates 160bits for any input or file. For example, suppose the message is “hello word” then its hash value using SHA-1 hashing algorithm the calculate value has represented as “e0738b87e67bbfc9c5b77556665064446430e81c”.

3.5. RSA

RSA algorithm is a public-key cryptography technique. It is broadly useful in various secure information transmission channels. RSA's name derived from the three scientists named Ron Rivest, Adi Shamir, and Leonard Adleman. They introduced the RSA encryption algorithm in 1978. It is an asymmetric cryptographic algorithm that uses two keys i.e., private and public key. In the RSA encryption algorithm, the public and private keys collectively encrypt a message in plain text, and the different key is a key used to decrypt a message which is encrypted. It ensures data integrity, authenticity, and confidentiality. The RSA bits may be typically 1024 or 2048bits, and the key derived from the large prime numbers.

3.6. Arnold Transform

Arnold transform is a simple and most common encryption technique widely adopted to hide sensitive information from the external world i.e., from unauthorized persons. The general form of Arnold transform can be represented as given below:

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod W \tag{5}$$

Where (x_i, y_i) is the original coordinate of image pixel; (x_{i+1}, y_{i+1}) is the scrambled coordinate, and W denotes the width of the input image. The Arnold conversion has the periodicity property, which means that after a certain amount of iterations, the original image will reappear. The numbers of times of iteration act as a secret key for Arnold transform. For secure transmission of watermark, the Arnold transform is performed on the watermark to get encrypted watermark that can be inserted securely into the source image. Without the knowledge of secret key watermark cannot be decrypted.

3.7. 3D Discrete Hyper Chaotic Map

In this paper, a new 3D discrete hyper chaotic map with strong chaotic behavior is proposed for digital watermarking scheme. The new 3-dimensional discrete cosine hyper chaotic (HCM) map is governed by the following equation.

$$HCM\ \ (Map) = \begin{cases} x_{n+1} = -\cos(y_n) - \cos(z_n) \\ y_{n+1} = \cos(x_n) + a * \cos(y_n) \\ z_{n+1} = 0.2 + \cos(z_n)(\cos(x_n) - b) \end{cases} \tag{6}$$

Where x_0, y_0, and z_0 are initial conditions. The variables a and b are the control parameter of the HCM map in equation (6). The variable n is the number of times to iterate HCM map. In experiments the initial value of x_0, y_0, z_0, a and b are taken as 1.123, 0.479, 2.317, 7.123 and 5.7 respectively. The sensitivity to initial condition of any chaotic map or system is quantified by Lyapunov Exponent (LE) metric.

LE is the rate of separation between two close trajectories

The System is said to have chaotic behavior if one LE is positive and if it has at-least two positive LEs, then system is hyper-chaotic The LE diagram of HCM map versus parameter a and time are shown in Figs. 2(a) and 3(b) respectively. The Bifurcation plot and spatiotemporal diagram of HCM maps is presented in Figs. 2(b) and 3(a), respectively.

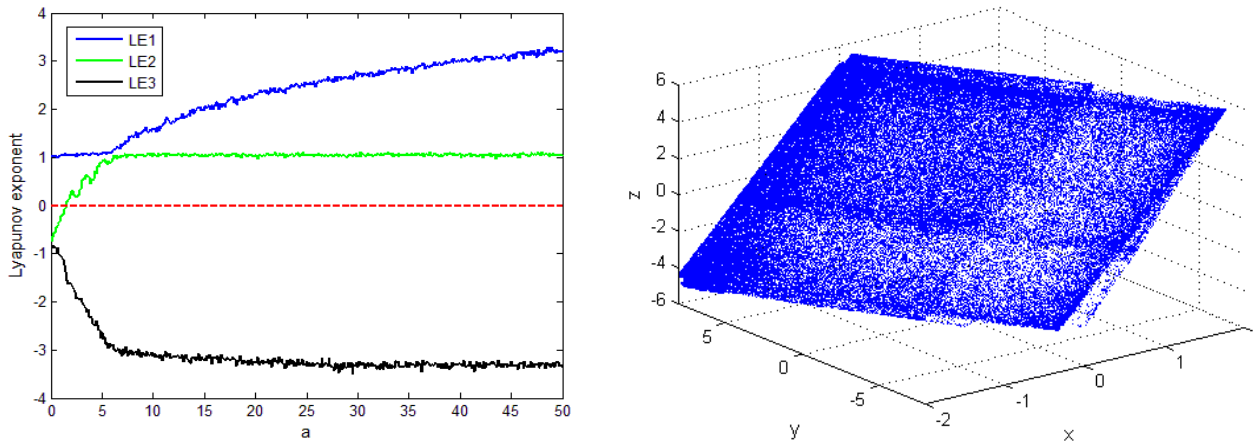

Fig 2. (a) Lyapunov exponent diagram versus parameter a, **(b)** Spatiotemporal diagram with initial values

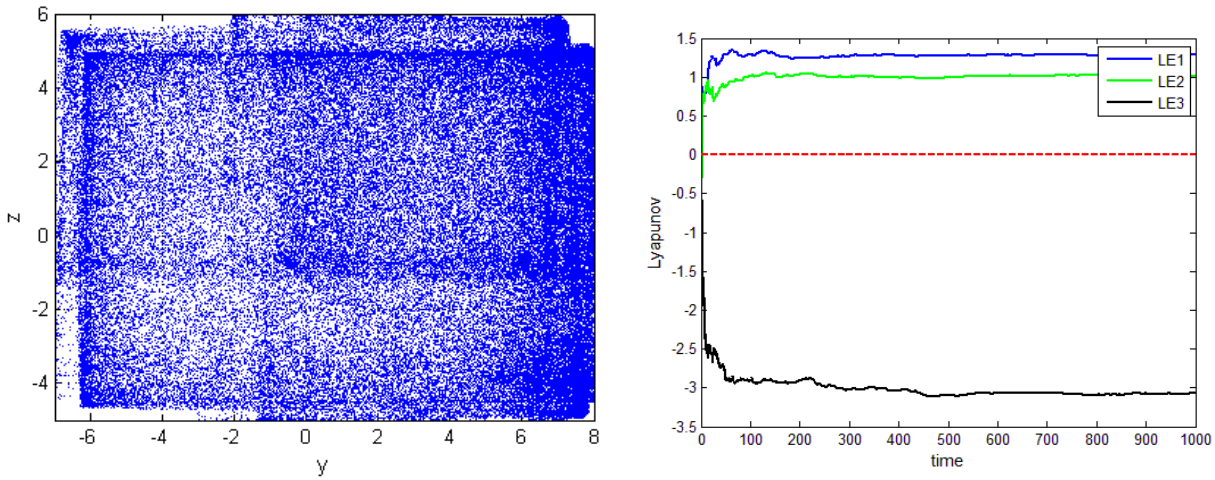

Fig 3. (a) Bifurcation plot, (b) Lyapunov exponent diagram versus parameter time

4. Proposed Method

In this part, we describe the steps of proposed method. Firstly, the watermark image encrypted using the encryption process before the embedding the watermark.

The block diagram of the encryption algorithm shown in fig 6(a).In the encryption process, first, we generate a hash value of the input watermark. Then apply the RSA encryption algorithm on the generated hash content to obtain the digital signature (DS).We append some information parameter to the watermark image with DS. Then Arnold transform has applied to obtain encrypted watermark image (EWI) as shown in fig 6(a). The information parameter includes m, n is the dimension of source image, p, q is the dimension of watermark image and 'a' is the rotational angle of the source image. The angle is calculated by using the corner pixel coordinate of the image [27].

At the received end, inverse Arnold transform has applied to the EWI image. After that, we extract watermark, DS, and information parameters from the resultant image, as shown in fig 6(b).We checked the extracted parameter value from source image characteristics. Let extracted parameter are m', n,' p,' q,' and a.' If the dimension has differed, then the image is altered by the unauthorized person. The angle has calculated by the value of corner pixel of received image. If the amount of the angle is zero, then there is rotation attack on received image otherwise image has rotation attack.

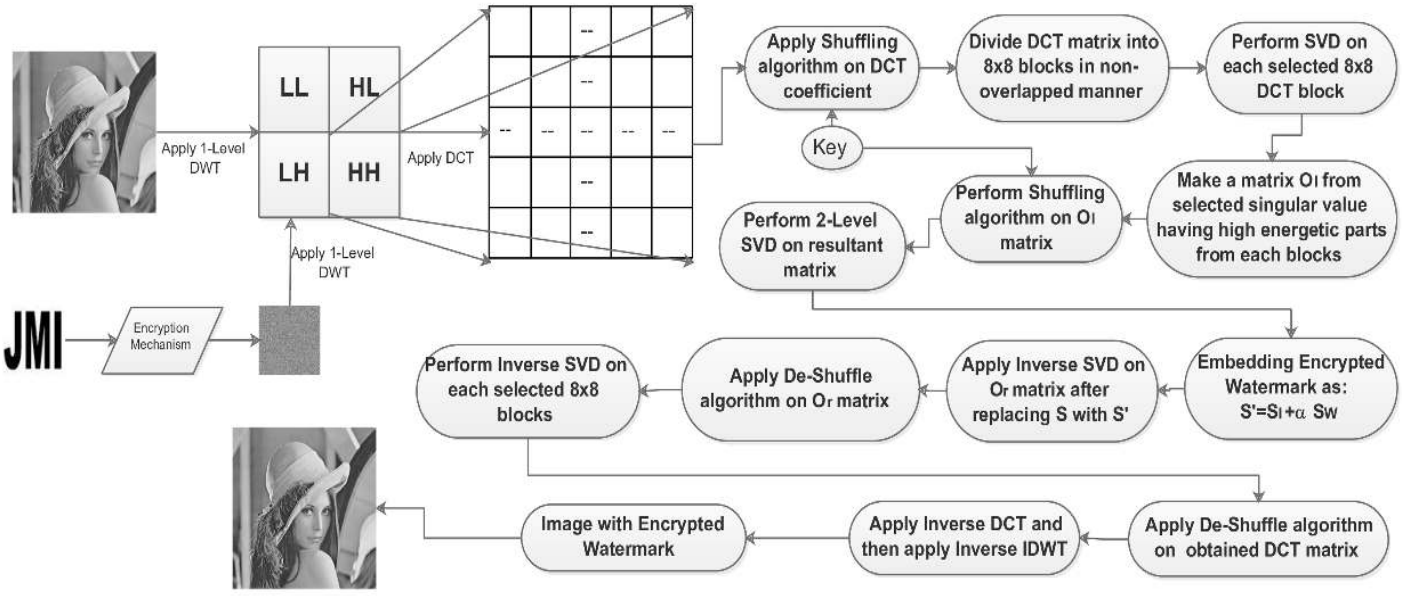

Fig 4. The block diagram of embedding process

In the encryption process of the JMI logo, number of pixel of change rate (NPCR) value is 99.455, the unified averaged changed intensity (UACI) is 33.451 and entropy is 7.939. The adjacent pixels correlation in encrypted images is 0.00549. For copyright logo encrypted image NPCR, UACI, entropy and adjacent pixels correlation are 99.639, 36.48, 7.986 and 0.00637 respectively.

Here, we explain the proposed algorithm for image watermarking technique. We take image I as input image and the size of image is 'm x n' and W notation is used for watermark image. The dimension of the watermark is 'p x q'. The proposed embedding and extraction watermark scheme methodology have shown in the block diagram in Fig 4 and Fig 5, respectively.

4.1 The steps of the proposed embedding scheme

A.1: Convert the source image into the frequency domain using DWT to obtain sub bands

A.2: Select bands of High High (HH) for inserting the watermark image bits

A.3: Apply DCT on HH frequency sub bands and apply Algorithm C named as shuffling algorithm on the DCT coefficient.

A.4: After shuffling DCT coefficient, divide the DCT matrix into 8x8 blocks in non-overlapping manner.

A.5: Now apply SVD on each selected 8x8 DCT block. And make a matrix O_I from selected singular value having high energetic parts from each 8x8 blocks.

A.6: Apply the shuffling algorithm on resultant matrix

A.7: Now apply 2-Level SVD on matrix obtain after step A.6 to get singular value as S_I. $(SVD_{O_I} = U_{O_I} S_{O_I} V'_{O_I})$

A.8: The encrypted watermark image (EWI) produced by the encryption mechanism then apply 1-Level DWT on EWI.

A.9: Apply the A.3 step to A.5 step on the EWI to obtain O_w matrix.

A.10: Apply the shuffling algorithm on resultant matrix O_w.

A.11: Perform 2-Level SVD on matrix O_w to get singular value as S_w. $(SVD_{O_w} = U_{O_w} S_{O_w} V'_{O_w})$

A.12: Calculate $S' = S_I + \alpha * S_w$. Then Obtain O_r matrix as: where α is smoothing factor.

A.13: Perform the inverse SVD on O_r matrix. Then De-shuffle the O_r matrix.

A.14: Replace the singular value in O_I matrix and Perform ISVD on each selected 8x8 blocks as indicate in A.5 step.

A.15: Then finally perform inverse DCT, de-shuffling algorithm, inverse DWT to obtained final watermarked image.

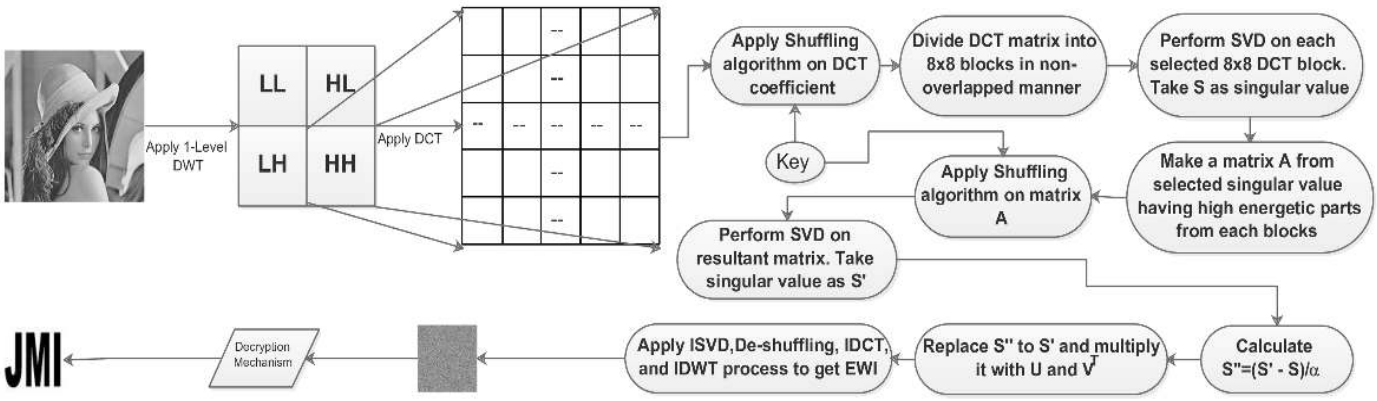

Fig. 5. The extracting process block diagram

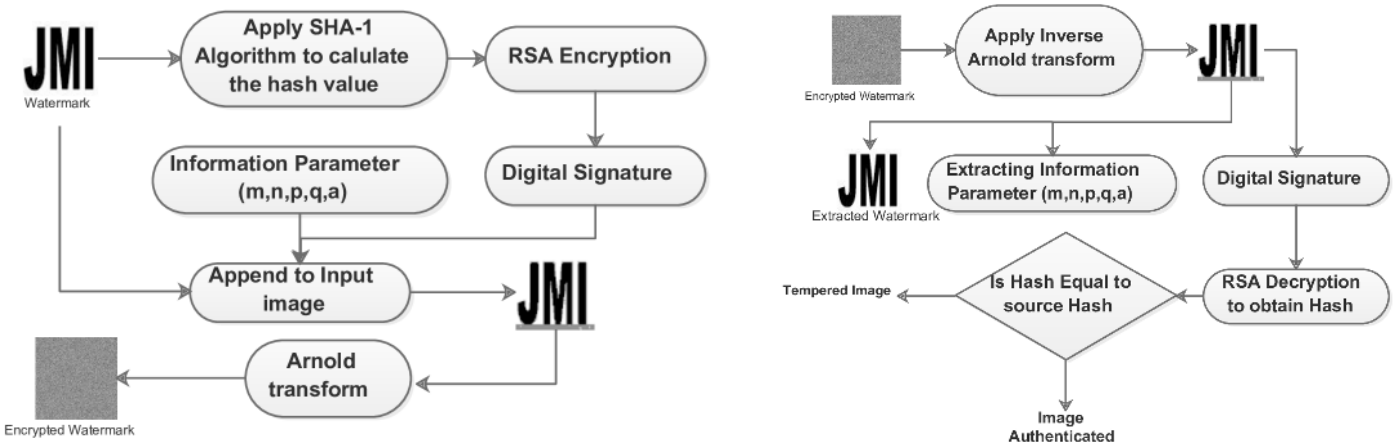

Fig 6. The block diagram of (a) Encryption process, (b) Decryption process

4.2 The steps of the extracting watermarking scheme

B.1: Divide the received image into frequency sub bands using DWT transform and, after that, operate DCT on HH frequency sub band.

B.2: Apply Algorithm C named as shuffling algorithm on the DCT coefficient and divide DCT matrix into 8x8 blocks in non-overlapping manner.

B.3: Perform SVD on each selected 8x8 DCT block. Take S as singular value. Make a matrix form selected singular value having high energetic parts from each block. Then apply shuffling algorithm on the resultant matrix.

B.4: Now apply 2-Level SVD on matrix obtain after step B.3.

B.5: Calculate the $S'' = (S' - S)/\alpha$. Then replace S'' to S' and multiply it as U(S'') V^T.

B.6: Apply the Inverse SVD, De-shuffling algorithm IDCT, and IDWT in order on matrix obtained in step B.5 to retrieve the EWI.

B.7: Now EWI is passed through decryption process to check the authenticity of the image as shown in fig 6(b).

4.3 The Proposed steps of the shuffling algorithm

The shuffle algorithm takes matrix as input and shuffle the matrix using HCM map. The initial value used in HCM map is mentioned in 3.7 section. The fig 7. show the steps of the shuffling algorithm.

Algorithm C : *Shuffling Algorithm*

Input: *Matrix A of size m,n*
Output: *Shuffle A Matrix*

1. *Initialize an 1D array O with size mxn with initial value from 1 to size of matrix mxn*
2. *Set itr←0, B array*
   Initialize x_i y_i and z_i(key)
3. *S←Sizeof(O)*
4. *While(iter< S) do*
5. *Select random pixel using HCM map*
6. $C_1 \leftarrow \lfloor x_i \times 10^{15} \rfloor \bmod(m - iter) + 1$ }
7. $C_2 \leftarrow \lfloor (y_i + z_i) \times 10^{15} \rfloor \bmod(n - iter) + 1$ }
8. $p \leftarrow (C_1 - 1) \times m + C_2$
9. *swap O[p] with O[S-iter]*
   increment iter by one
10. end //while loop end
11. While(iter< S) do
12. *calculate r,c value from B[iter]*
    B[i][j]←A[r][c]
13. *end*
14. *replace A with B*
15. *end*

Fig 7. The Steps of Shuffling algorithm

5. Experimental Results and Discussion

We test our technique under various common image processing attacks to check the robustness. The original image 'Lena' have dimension of 512 x 512 and watermark 'JMI' and copyright logo of 64 x 64 are used as shown in Fig 8.

(a)

(b)

(c)

Fig 8. (a) Lena image, (b) and (c) watermark

The use of PSNR (Peak Signal to noise ratio) is to check the quality of the human vision of the test image in comparison with the original input image. The following equation governs it.

$$PSNR = 20\log_{10}\left(\frac{255}{\sqrt{MSD}}\right)dB \quad (7)$$

Where MSD is the mean squared deviation or mean squared error which is govern by the following equation:

$$MSD = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[I(i,j) - I^{'}(i,j)\right]^2 \quad (8)$$

Hence, lower the MSD, higher the quality. To know whether the embedded logo and extracted logo are similar or not, normalized correlation (NC) is used and governs by the following equation:

$$NC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} W_{i,j} \oplus W^{''}{}_{i,j}}{m \times n} \quad (9)$$

Where $W_{i,j}$ is pixel value of embedded watermark and Wi, j″ is the pixel value of extracted watermark respectively; $m \times n$ is image size. The cumulative NC value is calculated by taking the maximum of NC values of Red, Blue and Green components. The effectiveness of the technique is tested under different common image processing attacks like rotation, blurring, noise addition, compression etc. The 'Lena' image is gone under different common image processing attacks and the visual results are shown in table 1.

The Structure Similarity Index Method (SSIM) is used to quantify image quality caused by various common image processing attacks. It is measure the similarity between the images. For calculating the performance evaluation of the proposed technique, we compare the result with the present scheme proposed by Lin and Lin at al.[4]. Table 2 shows the comparison result with the existing scheme. The NC value is high in most of the cases. Table 3 shows the PSNR result of JMI logo watermark. In table 4 we have shown the result of copyright logo watermark result. The outcomes show that the proposed technique of watermarking is robust and has a strong capability to the different attacks. It also checks the authenticity of the image at the receiver side.

Table 1. Attacked images and extracted robust JMI watermarks after various attacks

Type of attack	Attacked Image	Extracted Watermark
Histogram Equalization		
Median Filter		
Salt & Pepper Noise		
Gaussian Blurring		
Rotated Image by 10 degree clockwise		
Image Flipping		
Cropping 25%		

Table 2. The Comparison result of common image processing attacks on Lena Image of size '512x512' with JMI logo watermark and their NC value

Attacks	Proposed Method	Lin at al. scheme
	NC	NC
Without Attack	1	1
Resizing	0.9879	0.9892
JPEG Compression (10%)	0.9926	0.9921

Salt & Pepper Noise	0.9878	0.8828
Blurring	0.9917	0.9980
Rotation	0.9081	0.8076
Cropping	0.8767	0.8544
Sharpening	0.9945	0.9941

Table 3. The result of common image processing attacks on Lena Image size '512x512' with JMI logo watermark and their PSNR value

	Proposed Method
Attacks	**PSNR**
Without Attack	74.4037
Histogram Equalization	66.2782
Median Filter	80.3524
Salt & Pepper Noise	65.9858
Gaussian Blurring	67.3386
Resize	76.1513
Rotation	27.2838
Image Flipping	27.6713

Table 4. The result of common image processing attacks on Lena Image size '512x512' with copyright logo watermark

Attacks	**PSNR**	**NC**	**SSIM**
Without Attack	Infinity	1	1
Resizing	0.9889	0.9897	0.994
JPEG Compression (10%)	0.9956	0.9978	0.989
Salt & Pepper Noise	0.9897	0.9028	0.918
Blurring	0.9947	0.9987	0.989
Rotation	0.9367	0.9068	0.915
Cropping	0.9067	0.8956	0.909
Sharpening	0.9895	0.9949	0.997

6. Conclusion

In this paper, the image authenticated at receiver end by using information parameter and digital signature. To add more security in the watermarking scheme, the feature of the DCT, DWT, HCM map, and 2 Level SVD has effectively used. The experimental outcomes confirmed that not only the recommended scheme attained higher robustness and imperceptibility in comparison to our earlier scheme. The Watermark image also recovered successfully with the known secret key. Without the information of the private key, the embedded watermark cannot be retrieved.

References

[1] Loan NA, Hurrah NN, Parah SA, Lee JW, Sheikh JA, Bhat GM., "Secure and robust digital image watermarking using coefficient differencing and chaotic encryption", IEEE Access. 2018 Mar 16;6:19876-97.

[2] N. Nikolaidis, I. Pitas,"Robust image watermarking in the spatial domain",Signal Processing,Volume 66, Issue 3,1998,Pages 385-403,ISSN 0165-1684,https://doi.org/10.1016/S0165-1684(98)00017-6.

[3] Sanjay Rawat, Balasubramanian Raman,"A publicly verifiable lossless watermarking scheme for copyright protection and ownership assertion", International Journal of Electronics and Communications, Volume 66, Issue 11, 2012, Pages 955-962, ISSN 1434-8411, https://doi.org/10.1016/j.aeue.2012.04.004.

[4] Lin, Tzu-Chao & Lin, Chao-Ming., "Wavelet-based copyright-protection scheme for digital images based on local features", 2009, Information Sciences. 179. 3349-3358. 10.1016/j.ins.2009.05.022.

[5] Abdelhakim AM, Abdelhakim M., "A time-efficient optimization for robust image watermarking using machine learning", Expert Systems with Applications. 2018 Jun 15;100:197-210.

[6] H. Chen and W. Xu, "Secure and Robust Color Image Watermarking for Copyright Protection Based on Lifting Wavelet Transform," 2018 25th International Conference on Mechatronics and Machine Vision in Practice (M2VIP), Stuttgart, 2018, pp. 1-5.

[7] Stankovic, Srdjan & Djurovic et al., "Watermarking in the space/spatial-frequency domain using two-dimensional Radon Wigner Distribution ", IEEE Transactions on Image Processing. 10. 650-658. 2001

[8] Chang JC, Lu YZ, Wu HL, "A separable reversible data hiding scheme for encrypted JPEG bitstreams", Signal Processing. 2017 Apr 1;133:135-43.

[9] Tanya Koohpayeh Araghi, Azizah Abd Manaf, "An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD", Future Generation Computer Systems, Volume 101, 2019, Pages 1223-1246, ISSN 0167-739X

[10] Loan NA, Hurrah NN, Parah SA, Lee JW, Sheikh JA, Bhat GM," Secure and robust digital image watermarking using coefficient differencing and chaotic encryption", IEEE Access. 2018 Mar 16;6:19876-97.

[11] Singh S, Singh R, Singh AK, Siddiqui , " SVD-DCT based medical image watermarking in NSCT domain", In Quantum Computing: An Environment for Intelligent Large Scale Real Application 2018 (pp. 467-488). Springer, Cham.

[12] Yahya AN, Jalab HA, Wahid A, Noor RM, " Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network", Journal of King saud university-Computer and Information sciences. 2015 Oct 1;27(4):393-401.

[13] Chang, Chin-Chen & Chuang, Jun-Chou, "An image intellectual property protection scheme for gray-level images using visual secret sharing strategy", 2002, Pattern Recognition Letters. 23. 931-94. 10.1016/S0167-8655(02)00023-5.

[14] X.M. Niu, Z.M. Lu, S.H. Sun, "Digital watermarking of still images with gray level digital watermarks", IEEE Trans Consumer Electron, 46 (1) (2000), pp. 137–145

[15] T.H. Chen, G. Horng, W.B. Lee, "A publicly verifiable copyright-proving scheme resistant to malicious attacks", IEEE Trans Ind Electron, 52 (1) (2005), pp. 327–334

[16] S. Alam, S.M. Zakariya, N. Akhtar, "Analysis of modified Triple-A steganography technique using fisher yates algorithm", in International Conference on

Hybrid Intelligent Systems, (2014). ISBN 978-1-4799-7633-1/14/2014
[17] Parah SA, Ahad F, Sheikh JA, Loan NA, Bhat GM, " A New Reversible and high capacity data hiding technique for E-healthcare applications", Multimedia Tools and Applications. 2017 Feb 1;76(3):3943-75.
[18] Khayam SA at al., "The discrete cosine transform (DCT): theory and application (seminar note)", Michigan State University; 2003.
[19] Ahmad, S.A,T., Doja, M.N., "A novel edge based chaotic steganography method using neural network", In: Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications, pp. 467–475
[20] Sharif, A., Mollaeefar, M. & Nazari, M., " A novel method for digital image steganography based on a new three-dimensional chaotic map", Multimed Tools Appl 76, 7849–7867 (2017). https://doi.org/10.1007/s11042-016-3398-y
[21] Anees, A., Siddiqui, A.M., Ahmed, J. et al.,"A technique for digital steganography using chaotic maps", Nonlinear Dyn 75, 807–816 (2014). https://doi.org/10.1007/s11071-013-1105-3
[22] Rawat, S., Raman, B., "A chaos-based robust watermarking algorithm for rightful ownership protection", (2011) International Journal of Image and Graphics, 11 (4), pp. 471-493.DOI: 10.1142/S0219467811004263
[23] Rawat, S., & Raman, B., "A chaotic system based fragile watermarking scheme for image tamper detection", 2011, AEU - International Journal of Electronics and Communications, 65(10), 840-847. doi:10.1016/j.aeue.2011.01.016
[24] Himanshu, Rawat, S., Raman, B.et al, "DCT and SVD based new watermarking scheme", Proceedings - 3rd International Conference on Emerging Trends in Engineering and Technology, ICETET 2010, art. no. 5698309, pp. 146-151.
[25] Rawat, S., Raman, B.at al, "A new robust watermarking scheme for color images", IEEE 2nd International Advance Computing Conference, IACC 2010, art. no. 5423010, pp. 206-209.
[26] S. Alam et al., "Digital Image Authentication and Encryption using Digital Signature", International Conference on Advances in Computer Engineering and Applications (ICACEA), 2015.
[27] Ratnakirti Roy, Tauheed Ahmed, Suvamoy Changder, "Watermarking through image geometry change tracking," Visual Informatics,Volume 2, Issue 2,2018,Pages 125-135,ISSN 2468-502
[28] Alam, Shahzad & Ahmad, Tanvir & Doja, M., "A Chaotic Steganography Method Using Ant Colony Optimization", 2018, doi:10.1007/978-981-10-7566-7_42
[29] Anand, et al., "An improved DWT-SVD domain watermarking for medical information security", 2020, Computer Communications, 152, 72-80. doi:10.1016/ j.comcom. 2020.01.038
[30] Ye, et al., " Image encryption and hiding algorithm based on compressive sensing and random numbers insertion", Signal Processing, 172 doi:10.1016/ j.sigpro.2020.107563
[31] Ramasamy, et al., "An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic-tent map", 2019, Entropy,21(7), doi:10.3390/e21070656
[32] Mauro Barni at al. "A DCT-domain system for robust image watermarking", Signal Processing 66 (1998) 357—372
[33] Xinghua Li at al., "Recovering quantitative remote sensing products contaminated by thick clouds and shadows using multitemporal dictionary learning", 2015, IEEE transactions on geoscience and remote sensing, vol. 52, no. 11
[34] Aleksandr Shnayderman at al, "An SVD-Based Grayscale Image Quality Measure for Local and Global Assessment", IEEE transactions on image processing, vol. 15, no. 2, february 2006