Indian J.Sci.Res. 17(2): 180-183, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

DIGITAL WATERMARKING FOR ROBUST AND HIGH SECURITY DATA HIDING USING DWT-SVD TRANSFORMS AND ECC ENCRYPTION

[1] Afshan Taj, [2] Y Manjula, [3] Dr M Z Kurian
[1] Digital Electronics ,Dept. of ECE,SSIT, Tumkuru
[2] Dept. of ECE, SSIT, Tumkuru
[3] Dept. of ECE, SSIT, Tumkuru

Abstract: The process of embedding a data or information into exiting data is known as Digital watermarking. This additional data or information are used for embedding called as watermark. With this watermark, if the file or the data gets copied, originality of data is then identified. As, Digital communication facilitates transfer of digital data such as text, audio, video, etc. The un-authorized user can copy this data and can use where ever they want. However, this creates the problem of ownership, copywrite protection and security. To solve this kind of problems, Digital watermarking is used. During transmission of data from one place to other place, intentionally or non-intentionally many attacks occur on digital watermarked image. These results in to decreased image quality and the watermark may get destroyed partially. To provide good security to watermark and to prevent it from damaging, public key encryption and decryption technique such as elliptical curve cryptography (ECC) is used. Further this encrypted watermark used for digital watermarking process using combined DWT-SVD transform.

Keywords- **DWT-SVD transforms, digital image watermarking, ECC.**

INTRODUCTION

In present days the main source to transfer digital data from place to place is through internet. As a result of threats like illegal copying, tampering of data has increased enormously we use a digital watermarking technique to reduce the effects. A technique called as Digital Watermarking which is used to hide the secret information into digital media. It is applicable to many types of multimedia (image, audio and video) to protect copyrights. Due to this water marking many authors and publishers are getting profited and the complaints against copyrights have been minimized.

In watermarking technique the data can be hidden into host signal, then the watermarked object can be distributed all over the host. Here in the proposed method in the host signal the image is hidden by using different frequency domain techniques. In many situations time domain techniques are used, but frequency domain techniques are the best techniques when compared with time domain techniques as time domain techniques are not suitable for heavy long signals as time taken for conversion is more when compared with frequency domain techniques and robustness is more in frequency domain techniques.

In frequency domain techniques different Fourier transforms like DCT(Discrete Cosine Transform), DWT(Discrete Wavelet Transform), LWT(Lifting Wavelet Transform), SVD(Singular Value Decomposition) and combination of four techniques like DCT-SVD, DWT-SVD,DWT-DCT-SVD, LWT-DCT-SVD are applied to the host signal initially.

In DCT-SVD, finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies is expressed in DCT. DCT plays an major role in numerous applications of science and engineering. DCT (Discrete Cosine Transform) is a fourier-related transform similar to the Discrete Fourier transform (DFT), but using only real numbers. In this method DCT primarily the host signal are decomposed into respective coefficients.

Now the obtained coefficients are used to form the matrix in a particular order and then SVD (Singular Value Decomposition) is applied in the matrix to obtain singular values which are also known as Eigen values. According to the watermark data the Eigen values are modified then inverse SVD followed by inverse DCT are applied to obtain the embedded signal and respective SNR is analyzed. By using an embedded signal we will extract the initial audio signal and their appropriate BER and CC are analyzed.

In DWT-SVD method initially Discrete Wavelet Transform is applied to host image signal in which it competes the approximation coefficient vector and detail coefficient vector and then to form the singular values which are known as Eigen values SVD is applied. According to the watermark data the Eigen values are modified and then inverse SVD followed by inverse DWT are applied to obtain the embedded signal and respective SNR is analyzed. By using the embedded signal we will extract the initial audio signal and their appropriate BER and CC are analyzed.

In LWT-DCT-SVD technique initially LWT is applied to host image signal which computes the signal into approximation coefficient vector and detail coefficient vector and then Discrete Cosine Transform is applied to the signal and then to form singular values which are known as Eigen values SVD is applied to the vector. The Eigen values are modified according to

[1]Corresponding Author

watermark data and then inverse SVD succeed by inverse DCT followed by inverse LWT are applied to get the embedded signal and respective SNR is analyzed. By using the embedded signal we will extract the initial audio signal and their appropriate BER and CC are analyzed.

In DWT-DCT-SVD technique initially DWT is applied, which computes the signal into approximation coefficient vector and detail coefficient vector and then Discrete Cosine Transform is applied to the signal and then SVD is applied to the vector to form singular values which are known as Eigen values. The Eigen values are modified according to watermark data and then inverse SVD succeed by inverse DCT succeed by inverse DWT are applied to get the embedded signal and respective SNR is analyzed. By using the above methods, we can increase robustness, security, imperceptibility which in turn satisfies conditions of International Federation of Phonographic Industry (IFPI). The major advantages of these techniques is that they can withstand to different attacks like jittering, resampling, echo addition etc.

LITERATURE SURVEY

Dr Jean-Yves Chouinard et al, [1] proposed basic idea of elliptic curves and its point generation for data encryption. Elliptic curve cryptography (ECC) operations like point addition, point multiplication etc. are disclosed in detail for secure communication.

Moncef Amara and Amar Siad et al, [2] proposed Elliptic curve cryptography (ECC) and its performance in terms of execution speed and security in comparison to the traditional cryptographic algorithms like RSA etc. The ECC points are generated by selecting the Prime number P. Further the author described the application of cryptography on digital signature.

Kamlesh Gupta and Sanjay Silakari et al, [3] proposed Elliptic curve cryptography (ECC) image encryption in which the elliptical points are generated using prime number and its security level comparison with RSA encryption technique.

Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh et al, [4] proposed an Elliptic curve cryptography (ECC) for color image encryption and decryption. Further they include digital signature to the encrypted image to provide authenticity. In order to decrease the computation time they performed operation by grouping the pixels and pairing of the grouped pixels. The algorithm which is proposed yields Entropy of 7.99986 for the Lena image.

Saeid Bakhtiari, Subaraiah Ibrahim et al [5] introduces a new technique which combines both image compression and image encryption techniques. An Elliptic curve cryptography encryption technique is deployed during and before traditional JPEG compression technique for more security and for size reduction. The image pixel values are converted into ECC points by using Koblitz's method.

Pye Pye Aung et al, [6] proposed the combination of cryptography and steganography techniques . To encrypt secrete message cryptographic technique uses advanced encryption standard (AES) algorithm. which have separate keys to hide in cover image. Discrete Cosine Transform (DCT) is the Steganography technique used here. Discrete Cosine Transform (DCT) which uses a part of encrypted message as a key to hide in an image. Parameters such as security, robustness and image quality security are considered.

Shaikh Shoaib et al, [7] proposed the digital video watermarking using 3 level Discrete Wavelet Transform (DWT) algorithm for securing data with a secret key. During the encryption process the key generated with watermarking image is considered and during decryption process the same key is used. The parameters considered are PSNR and MSE.

Mohamed A. Seif At el [8] proposed the ECC based DES algorithm. The DES is a symmetric key Cipher algorithm. The required key is generated using ECC techniques. The ECC based DES method is applied for distinct image files for both encryption and decryption with large key space to resist brute force attack. The parameters considered are correlation, PSNR, MSE , histogram analysis, and key sensitivity analysis.

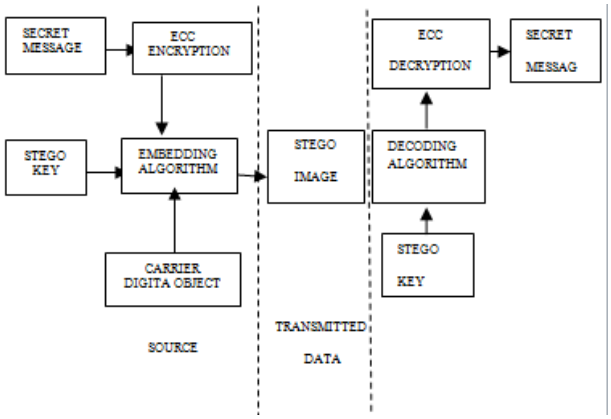
Blessy Joy A et al, [9] proposed the cryptographic technique, Elliptic curve cryptography (ECC) technique is used to encrypt the RGB image to secure the data from unauthorized access. Required number of bit planes are encrypted to achieve different levels of security. The image undergoes pixel wise xor operation and encrypted by ECC. Parameters like bandwidth limited, processing power, energy for ECC are taken into consideration. It is used in multimedia communication.

Saleh Saraireh et al, [10] proposed a secure communication system using cryptographic algorithm along with steganography. The filter bank cipher is used to encrypt the secret text message and steganography uses discrete wavelet transforms (DWT) technique to hide the encrypted messages in the cover image by changing the wavelet coefficients. Parameters such as peak signal to noise ratio (PSNR), speed histogram analysis, security and scalability are considered.

PROPOSED SYSTEM

The basic model of proposed system contains a Carrier, Message encryption and Password. cover-object

is also known as Carrier, in which the message or data is embedded and serves to hide the presence of the message or data. Basically, the model of system is shown on Fig.1. Message is the data that the sender wishes to remain it dern. The message data is an image which encrypted using (Elliptical Curve Cryptography ECC) which is a Public key encryption technique. Stego-key is known as Password, which ensures that message from a cover-object can be extracted only by the recipient who knows the corresponding decoding key. The cover-object with the derned embedded message using DWT-SVD technique is then defined as the stego object. Restoring message from a stego-object needs the cover-object itself and a similar decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message.



Methodology

In this section, the embedding and extraction algorithms of the proposed method is discussed.

a. The Embedding Algorithm

The technique of embedding a watermark in an message signal is as follows and shown in **Fig.1**.

1. Initially message image has been read.

2. The message image is encrypted using Elliptical curve Cryptography.

3. Discrete wavelet transforms (DWT) is applied to Carrier image.

4. DWT coefficients are separated into number of frames.

5. Singular Value Decomposition (SVD) is applied to each frame.

6. 2-dimensional binary watermark image is converted into 1-Dimensional binary data.

7. Singular value of each frame is modified according to following embedding ru

$$\begin{cases} S' = round\left(\frac{s}{Q}\right) * Q; & if\ w(k) = 1 \\ S' = floor\left(\frac{s}{Q}\right) * Q + \left(\frac{Q}{2}\right); & if\ w(k) = 0 \end{cases}$$

$$\begin{cases} w(k) = 0; & if\ \left(\frac{Q}{4}\right) \le mod(S'', Q) < \left(3 * \frac{Q}{4}\right) \\ w(k) = 1; & otherwise \end{cases}$$

Where S' is modified singular value.

8. Inverse Singular Value Decomposition (SVD) is applied to the modified singular value.

9. IDWT and IDCT are applied to get watermarked message.

b. The Extracting Algorithm

The process of extracting watermarked image is as follows.

1. Read the attacked watermarked (Stego) message image.

2. DWT is applied to the Stego message.

4. DWT coefficients are seperated into number of frames.

5. SVD is applied to each frame separately.

6. The watermark bits are sunder out from each frame of singular values by using following rule.

CONCLUSION

A novel approach of watermarking based on ECC and DWT -SVD is suggested. The traditional technique methods are very time consuming and provides less security. DWT-SVD along with ECC method is found to be more secure and fast. The new method was found to satisfy all the requirements of an ideal watermarking scheme such as ,robustness imperceptibility and good capacity. This method is applicable for authentication and data hiding purposes. The future work includes the extension of this technique to other category and formats of images, for example, MRI, CT and DICOM images.

References

[1] Dr Jean-Yves Chouinard: "Design of Secure Computer Systems CSI4138/CEG4394 Notes on Elliptic Curve Cryptography(ECC)", (2002).

[2] Moncef Amara and Amar Siad: "Elliptic Curve Cryptography(ECC) and its Applications", IEEE 7th int.

Workshop on Systems, Signal Processing and their Applications, 2011, pp. 247-250.

[3] Kamlesh Gupta and Sanjay Silakari: "Performance Analysis for image Encryption using ECC", Int. Conference on computational intelligence and Communication Networks, 2010, pp. 79-82.

[4] Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh: "Image Encryption using Elliptic Curve Cryptography", ELSEVIER, Procedia Computer Science, 11th Int. Multi-Conference on Information Processing-2015 (IMCIP-2015), Vol.54, pp. 472-481.

[5] Saeid Bakhtiari, Subaraiah Ibrahim, et. al: "JPEG Image Encryption with Elliptic Curve Cryptography", IEEE Int. Symp. On Biometrics and Security Technologies (ISBAST) 2014, pp. 144-149.

[6]Pye Pye Aung and Tun Min Naing, A novel secure combination technique of Steganography and cryptography, vol. 2, No. 1, February 2014.

[7]Shaikh Shoaib, Prof. R. C. Mahajan Authenticating using secret key in digital video watermarking using 3 level DWT. IEEE Issue 17, January 2015.

[8] Moamed A. Seif Eldeen, Adbellatif A. Elkouny, Salwa Elramly DES algorithm security fortification using elliptic curve cryptography IEEE issue 2 Dec 2015

[9]Blessy Joy A,R. Girish, RGB image encryption based on bitplanes using Elliptic Curve Cryptography, vol. 5, Issue 2, February 2015.

[10]Saleh Saraireh, A Secure Data Communication System Using Cryptography And Steganography, Vol.5, No.3,May20