International Journal of Pure and Applied Mathematics
Volume 119 No. 12 2018, 13387-13396
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue
ijpam.eu

Secured Transmission of a compressed image by using ECC

Ponmani E, Nandhini E, Karthika K, Saravanan Palani*

School of Computing, SASTRA Deemed University, India

*Corresponding Author

Abstract:

Security is the main issue concerned with protecting the digital images that are transmitted over the network. By providing the high security, the digital images on the network can be protected from various types of attacks. A Cryptographic technique plays a major role in providing the security goals such as confidentiality and integrity for digital images. Elliptical curve cryptography (ECC) is the asymmetric encryption which is used to apply to the images that result from DWT Compression. Discrete Wavelet Transform (DWT) is an important compression technique which is used to compress the image effectively. It represents the input data in the form of the low pass (approximate) and high pass (detailed) coefficients. These coefficients are entered into the filters. The outputs from these filters are down-sampled for compression. In this paper, the transmitted images via wireless network were secured by encryption using the public key. The sender will generate the private key from the compressed image based on elliptical curve cryptography. The Sender will send the compressed image and private key separately to the receiver. DWT provides high compression ratio and robustness for protecting the digital image integrity. This experiment result provides some performance measures such as Peak Signal to Noise Ratio (PSNR), Bit Error Rate (BER) and Mean Squared Error (MSE). It also provides high integrity for transmitted digital images.

Keywords: Discrete Wavelet Transform (DWT), Elliptical curve cryptography (ECC), Encryption, Security, Integrity.

1. INTRODUCTION

The Image Compression is one of the most important concepts in Image processing. It is used to decrease the storage size of an image without affecting the quality of an image. In image processing, there are various types of methods available for image compression. The minimization of file size will increase the storage capacity. Due to reduced size, the file is easy to transfer. Finding out the less correlated pixels is the main aim of image compression. Redundancy and Irrelevancy are the two important principles used in compression of an image. There are three types of redundancy. They are coding, interpixel and psycho-visual redundancy. The removal of any one or more of the redundancies will achieve the better compression. An algorithm such as DCT and DWT are used for image compression. In that, Wavelet transform is the best technique used for image compression [1]. Compared to DCT, DWT produce effectively high compression ratio, and it takes less time than

DCT [1]. DWT provides robustness for protecting the image integrity. In this paper, DWT produces the performance measures such as Peak Signal to Noise Ratio (PSNR), Bit Error Rate (BER), and Mean Squared Error (MSE).

The Quality of the compressed image was predicted by two error metrics. The Error metrics are PSNR and MSE. The Ratio of maximum strength of the signal to the strength of the corrupted noise is called as PSNR [2]. The Cumulative squared error between the original and compressed image is called as MSE. The Number of bit errors per unit time is known as Bit Error Rate (BER). If the PSNR value is high and the MSE value is low, then the quality of the compressed image is better [2].

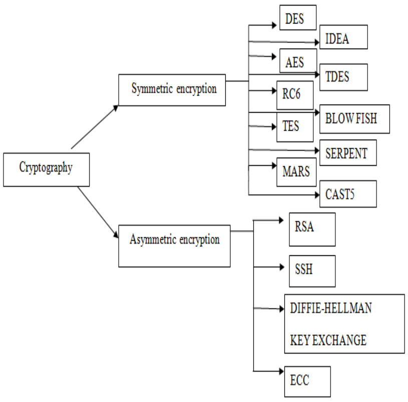

Fig1.Types of Cryptographic techniques

The concept of cryptography plays an important role in protecting the transmitted images on the network from various types of attacks [11-20]. A cryptographic technique protects the user's data. The Security goals such as confidentiality, authenticity, and integrity were provided by encrypting the data [21-30]. The cryptographic algorithm includes both symmetric and asymmetric encryption. In Symmetric encryption, both encryption and decryption were done by a single key (same key) [3]. In Asymmetric encryption, two different keys are used [31-35]. One key is used for encryption, and another key is used for decryption. This encryption is also called as Public key cryptography [3].

Fig1 shows the type of cryptographic techniques. The Symmetric encryption algorithm includes DES, AES, IDEA, TDES, Blowfish, Serpent, RC6, TEA, MARS and CAST5 [3]. The Asymmetric encryption algorithm includes RSA, SSH, Diffie-Hellman key exchange [4] and elliptical curve cryptography. In this paper, elliptical curve cryptography is used for both encryption and decryption. In existing systems, they performed the DCT based encoding for produce the encoded data and symmetric encryption for encrypting the data. This encrypted data was transmitted through the wireless network. This encryption provides the secured transmission. In DCT based encoding, the image was divided into 8×8 blocks, and these blocks are quantized by quantization table to produce 64 coefficients. The first value in the leftmost corners is called as DC coefficient, and other 63 values are collectively called as AC coefficients. Differential Pulse Code Modulation (DPCM) was used to encode the DC coefficients, and Run Length Coding (RLC) was used to encode the AC coefficients. Finally, they performed the symmetric encryption for securing the encoded data. The Sender will send the encoded data after encryption, and the receiver will decrypt the data.

2. RELATED WORKS

Barbhuiya, Laskar, and Hemachandran [1] proposed a new technique for compression. They developed DWT and Inverse DWT for achieving high compression ratio. Mostafa and Fakhr [2] they introduced a technique called compressive sensing to achieve high PSNR values. Amara and Siad [3] used the Elliptical curve cryptography for encryption.

Through ECC, they achieve high security for encrypted data.

Khan and Singh [4] used the ECC for reducing the size of the key. In comparison with RSA, ECC requires smaller key size. Nashat and Hassan [5] they developed the new wavelet transform called Haar wavelet transform to attain the high compression ratio and PSNR values. Tabassum, Islam, and Amin [6] they also developed the Haar wavelet transform to represent the image in terms of frequencies to achieve the high-quality image. Bio medical images are embedded secretly in selected cover images using meta data [7]. Setiadi, Kistijantoro, and Miyaji [8] they used ECC for achieving the high computational power.

3. DISCRETE WAVELET TRANSFORM (DWT):

The Signal Analysis is represented by the Wavelet function. In DWT compression, the Sum of wavelet function represents an image. These Wavelet functions are collectively called as Wavelets. It represents an image in terms of both location and scale [5]. The DWT compressions represent the input data in the form of low pass and high pass coefficients.

The properties of the wavelet functions are:

- $\int_{-\infty}^{0} \varphi(t)dt = 0;$

The above function represents the wavy appearance of the signal.

- $\int_{-\infty}^{0} |\varphi(t)|^2 dt = 0;$

It represents that the energies are confined to a finite duration.

The two important filters are used in DWT [5]. They are low pass and high pass filter. The coefficients are entered into those filters. The Approximate coefficient and detailed coefficient are the output of low pass and high pass filter respectively. These coefficients are also called as subbands [5].These outputs are divided into LL, LH, HL, and HH. The LL is said to be approximate coefficient, and all others are said to be detailed coefficient. All research work uses 2-Dimensional DWT. In DWT, the LL, LH, HL, and HH are the output which comes from the first level of decomposition. After performing the matrix transformation, again the approximate coefficients and detailed coefficients are divided into four parts. A further level of decomposition is done on approximate coefficients.

The Fig 2a and 2b represent the level of decomposition occurs in an image.

After performing DWT, we will find the PSNR and MSE ratio [5]:

$$\text{PSNR} = 10Log_{10}(255^2/MSE)dB$$

$$\text{MSE}=1/MN\sum_{x-1}^{M}\sum_{y-1}^{N}[f(x,y)-f^1(x,y)]^2$$

If the value of PSNR is high and MSE is low, then the compressed image quality is better.

LL_1	HL_1
LH_1	HH_1

Fig2a.First Level of Compression

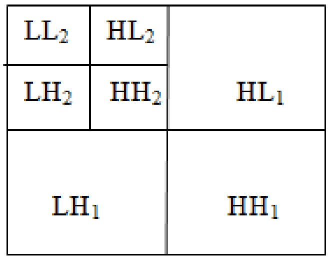

Fig2b.The second level of compression

4. INVERSE DWT:

The Reverse process of DWT is called Inverse DWT. Therefore an original image can be reconstructed from the compressed image.

5. HAAR WAVELET TRANSFORM:

Haar Wavelet Transform is one of the important transformations in the DWT [6]. It is the best method used for compressing the image. In HWT, if the Matrix A has an image with even dimensions M×N, then we have to compute the value of W_MA. Here, the matrix multiplication was done by applying W_M to each column of matrix A. Therefore; the output will be a matrix with M×N dimension. Haar matrix is used to process both columns as well as the row of an image. By the process of Wavelet Matrix Transposition, the coefficients of the filters are placed on the column of Matrix A. The Discrete Haar Wavelet Transform was computed by,

$$B = W_M A W_N^T$$

In HWT, most of the information was conserved in the upper left corner and remaining Blocks contain less information about the image. After compression, the input details are divided into four parts. The upper left-hand corner of the block contains an approximation of an entire image.

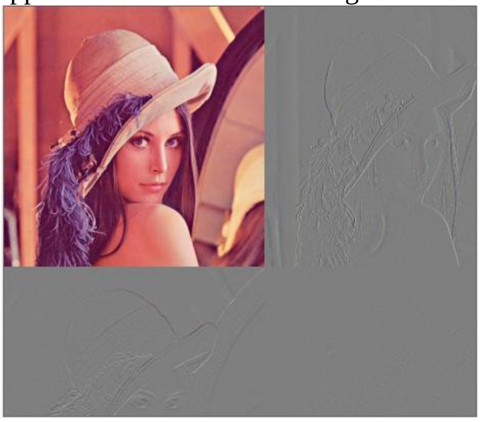

Fig3. DWT Compression

The lower left-hand corner represents the horizontal information of an image. The upper right-hand corner contains vertical information of an image, and the lower right-hand corner is hard to see.

Table 1: Comparison of PSNR values between DCT and DWT

Image Id	**Size of an image**	**DCT**	**DWT**
im1	256×256 (medical image)	31.080dB	50.260dB
im2	256×256	32.732dB	46.207dB
im3	512×512	34.260dB	46.130dB
im4	1024×1024	37.620dB	46.063dB

Table 2: Comparison of MSE values between DCT and DWT

The Compressed or blur portion have higher intensities when compared to other portion. This process is invertible. So, the original image was reconstructed from the blurred image. The Fig3 shows the compression of an image.

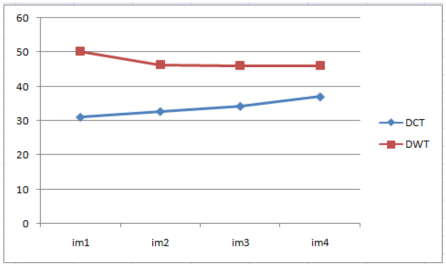

Fig4.The graph on PSNR values between DCT and DWT

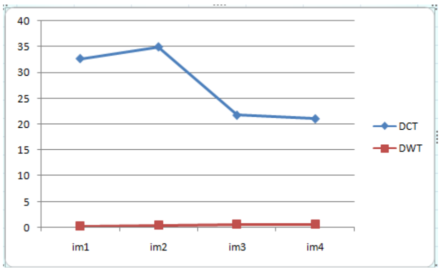

Fig5.The graph on MSE values between DCT and DWT

The above Fig4 and Fig5 show the performance measure of DCT and DWT. In this, DWT produces high values of PSNR than DCT.

6. ELLIPTICAL CURVE CRYPTOGRAPHY

Nowadays, Elliptical Curve Cryptography is the one of the popular cryptographic technique used for encrypting the data. ECC provides high security by encrypting the data [7]. When compared to other public key cryptographic algorithms, ECC use only 160 bits for key size [9] [10]. The other asymmetric algorithms use 1024 bits for exchanging the keys. The Encryption and Decryption process of ECC will be faster when compared to other algorithms. Both Public Key and Private Key can be generated by using this ECC algorithm. The public key is used to encrypt the data by the sender, and the private key is used to decrypt the data by the receiver.

Image Id	**Size of an image**	**DCT**	**DWT**
im1	256×256 (medical image)	32.670	0.246
im2	256×256	34.930	0.514
im3	512×512	21.720	0.616
im4	1024×1024	21.026	0.537

7. ELLIPTIC CURVE

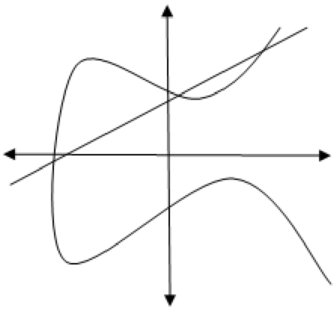

Fig6.Elliptic curve

Consider an elliptic curve E with a particular point L. Consider the curve equation as

$$y^2 = x^3 + ax + b$$

L is a point on the curve and m is the maximum limit. The Fig6 represents the elliptic curve [10].

Key generation is an important part of the elliptical curve cryptography. Here, we can generate the key for both encryption and decryption. The sender will encrypt the image by using the public key, and the receiver will decrypt the image by using the private key. Choose a value ‘e’ within the range of m.

$$P= e*L$$

The e is the private key and P is the public key.

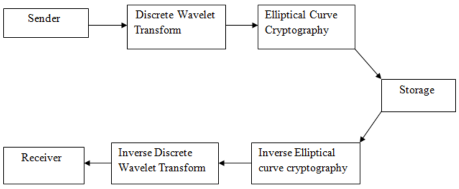
Sender
Discrete Wavelet Transform
Elliptical Curve Cryptography
Storage
Inverse Elliptical curve cryptography
Inverse Discrete Wavelet Transform
Receiver

Fig7.Process Flow Diagram

The Fig7 represents the process flow of secured transmission. In this process, we send the private key and encrypted image separately. The encrypted image will be sent through this process. But the private key will be sent to any other network account (like Mail, Mac address, etc.) of the receiver.

8. CONCLUSION

In this paper, we exploit the secured image transmission via the wireless network by using ECC. Before encryption, we compressed the image by using DWT. DWT avoids the blocking artifacts which cause the loss of valuable information. It produces the image with better quality. It provides higher PSNR values when compared with DCT compression. By using DWT, we are increasing the overall image quality by 32%. Then, we provide integrity to the transferred image by generating the key using ECC.

REFERENCES:

[1]. Barbhuiya, A. J. I., Laskar, T. A., & Hemachandran, K. (2014, November). An approach for color image compression of JPEG and PNG images using DCT and DWT. In Computational Intelligence and Communication Networks (CICN), 2014 International Conference on (pp. 129-133). IEEE.

[2]. Mostafa, M., & Fakhr, M. W. (2017, March). Joint image compression and encryption based on compressed sensing and entropy coding. In Signal Processing & its Applications (CSPA), 2017 IEEE 13th International Colloquium on (pp. 129-134). IEEE.

[3]. Amara, M., & Siad, A. (2011, May). Elliptic Curve Cryptography and its applications. In Systems, Signal Processing and their Applications (WOSSPA), 2011 7th International Workshop on (pp. 247-250). IEEE.

[4]. Singh, S. R., Khan, A. K., & Singh, T. S. (2016, September). A critical review on Elliptic Curve Cryptography. In Automatic Control and Dynamic Optimization Techniques (ICACDOT), International Conference on (pp. 13-18). IEEE.

[5]. Nashat, A. A., & Hassan, N. H. (2016, June). Image compression based upon Wavelet Transform and a statistical threshold. In Optoelectronics and Image Processing (ICOIP), 2016 International Conference on (pp. 20-24). IEEE.

[6]. Tabassum, F., Islam, M. I., & Amin, M. R. (2015, May). A simplified image compression technique based on Haar Wavelet Transform. In Electrical Engineering and Information

Communication Technology (ICEEICT), 2015 International Conference on (pp. 1-9). IEEE.

[7]. Arunkumar, S., Subramaniyaswamy, V., Karthikeyan, B., Saravanan, P., & Logesh, R. (2018). Meta-data based secret image sharing application for different sized biomedical images. Biomedical Research, 29.

[8]. Setiadi, I., Kistijantoro, A. I., & Miyaji, A. (2015, August). Elliptic curve cryptography: Algorithms and implementation analysis over coordinate systems. In Advanced Informatics: Concepts, Theory, and Applications (ICAICTA), 2015 2nd International Conference on (pp. 1-6). IEEE.

[9]. Qiu, Q., & Xiong, Q. (2004, May). Research on elliptic curve cryptography. In Computer Supported Cooperative Work in Design, 2004. Proceedings. The 8th International Conference on (Vol. 2, pp. 698-701). IEEE. [1].

[10]. Singh, L.D., & Debbarma, T. (2014, May). A new approach to Elliptic Curve Cryptography. In Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on (pp. 78-82). IEEE.

[11]. Logesh, R., Subramaniyaswamy, V., Vijayakumar, V., Gao, X. Z., & Indragandhi, V. (2017). A hybrid quantum-induced swarm intelligence clustering for the urban trip recommendation in smart city. Future Generation Computer Systems, 83, 653-673.

[12]. Subramaniyaswamy, V., & Logesh, R. (2017). Adaptive KNN based Recommender System through Mining of User Preferences. Wireless Personal Communications, 97(2), 2229-2247.

[13]. Logesh, R., & Subramaniyaswamy, V. (2017). A Reliable Point of Interest Recommendation based on Trust Relevancy between Users. Wireless Personal Communications, 97(2), 2751-2780.

[14]. Logesh, R., & Subramaniyaswamy, V. (2017). Learning Recency and Inferring Associations in Location Based Social Network for Emotion Induced Point-of-Interest Recommendation. Journal of Information Science & Engineering, 33(6), 1629–1647.

[15]. Subramaniyaswamy, V., Logesh, R., Abejith, M., Umasankar, S., & Umamakeswari, A. (2017). Sentiment Analysis of Tweets for Estimating Criticality and Security of Events. Journal of Organizational and End User Computing (JOEUC), 29(4), 51-71.

[16]. Indragandhi, V., Logesh, R., Subramaniyaswamy, V., Vijayakumar, V., Siarry, P., & Uden, L. (2018). Multi-objective optimization and energy management in renewable based AC/DC microgrid. Computers & Electrical Engineering.

[17]. Subramaniyaswamy, V., Manogaran, G., Logesh, R., Vijayakumar, V., Chilamkurti, N., Malathi, D., & Senthilselvan, N. (2018). An ontology-driven personalized food recommendation in IoT-based healthcare system. The Journal of

Supercomputing, 1-33.

[18]. Arunkumar, S., Subramaniyaswamy, V., & Logesh, R. (2018). Hybrid Transform based Adaptive Steganography Scheme using Support Vector Machine for Cloud Storage. Cluster Computing.

[19]. Indragandhi, V., Subramaniyaswamy, V., & Logesh, R. (2017). Resources, configurations, and soft computing techniques for power management and control of PV/wind hybrid system. Renewable and Sustainable Energy Reviews, 69, 129-143.

[20]. Ravi, L., & Vairavasundaram, S. (2016). A collaborative location based travel recommendation system through enhanced rating prediction for the group of users. Computational intelligence and neuroscience, 2016, Article ID: 1291358.

[21]. Logesh, R., Subramaniyaswamy, V., Malathi, D., Senthilselvan, N., Sasikumar, A., & Saravanan, P. (2017). Dynamic particle swarm optimization for personalized recommender system based on electroencephalography feedback. Biomedical Research, 28(13), 5646-5650.

[22]. Arunkumar, S., Subramaniyaswamy, V., Karthikeyan, B., Saravanan, P., & Logesh, R. (2018). Meta-data based secret image sharing application for different sized biomedical images. Biomedical Research,29.

[23]. Vairavasundaram, S., Varadharajan, V., Vairavasundaram, I., & Ravi, L. (2015). Data mining ‐ based tag recommendation system: an overview. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 5(3), 87-112.

[24]. Logesh, R., Subramaniyaswamy, V., & Vijayakumar, V. (2018). A personalised travel recommender system utilising social network profile and accurate GPS data. Electronic Government, an International Journal, 14(1), 90-113.

[25]. Vijayakumar, V., Subramaniyaswamy, V., Logesh, R., & Sivapathi, A. (2018). Effective Knowledge Based Recommeder System for Tailored Multiple Point of Interest Recommendation. International Journal of Web Portals.

[26]. Subramaniyaswamy, V., Logesh, R., & Indragandhi, V. (2018). Intelligent sports commentary recommendation system for individual cricket players. International Journal of Advanced Intelligence Paradigms, 10(1-2), 103-117.

[27]. Indragandhi, V., Subramaniyaswamy, V., & Logesh, R. (2017). Topological review and analysis of DC-DC boost converters. Journal of Engineering Science and Technology, 12 (6), 1541–1567.

[28]. Saravanan, P., Arunkumar, S., Subramaniyaswamy, V., & Logesh, R. (2017). Enhanced web caching using bloom filter for local area networks. International Journal of Mechanical Engineering and Technology, 8(8), 211-217.

[29]. Arunkumar, S., Subramaniyaswamy, V., Devika, R., & Logesh, R. (2017).

Generating visually meaningful encrypted image using image splitting technique. International Journal of Mechanical Engineering and Technology, 8(8), 361–368.

[30]. Subramaniyaswamy, V., Logesh, R., Chandrashekhar, M., Challa, A., & Vijayakumar, V. (2017). A personalised movie recommendation system based on collaborative filtering. International Journal of High Performance Computing and Networking, 10(1-2), 54-63.

[31]. Senthilselvan, N., Udaya Sree, N., Medini, T., Subhakari Mounika, G., Subramaniyaswamy, V., Sivaramakrishnan, N., & Logesh, R. (2017). Keyword-aware recommender system based on user demographic attributes. International Journal of Mechanical Engineering and Technology, 8(8), 1466-1476.

[32]. Subramaniyaswamy, V., Logesh, R., Vijayakumar, V., & Indragandhi, V. (2015). Automated Message Filtering System in Online Social Network. Procedia Computer Science, 50, 466-475.

[33]. Subramaniyaswamy, V., Vijayakumar, V., Logesh, R., & Indragandhi, V. (2015). Unstructured data analysis on big data using map reduce. Procedia Computer Science, 50, 456-465.

[34]. Subramaniyaswamy, V., Vijayakumar, V., Logesh, R., & Indragandhi, V. (2015). Intelligent travel recommendation system by mining attributes from community contributed photos. Procedia Computer Science, 50, 447-455.

[35]. Vairavasundaram, S., & Logesh, R. (2017). Applying Semantic Relations for Automatic Topic Ontology Construction. Developments and Trends in Intelligent Technologies and Smart Systems, 48.