Random Number Generation for High Security using 3 Level DWT Steganography and ECC Encryption – A Survey

[a]Inusha M M, [b]Y Manjula, [c]M Z Kurian

[a]M.Tech Student, VLSI and Embedded system,Dept. of ECE,SSIT, Tumkur, India, [b]Assistant Professor, Dept. of ECE, SSIT, Tumkur, India, 572105. [c] HOD, Dept. of ECE, SSIT, Tumkur, India, 572105.

Abstract

Two types of data hiding techniques are most popular in today's world, they are cryptography and steganography. Where cryptography is science of writing secret code and steganography is science of hiding the secret code. In cryptography data is converted to unreadable form, so that unauthorized users cannot access the secret data. Where in steganography the secret data is hidden into digital media like image, audio and video. The combination of cryptography and steganography techniques will provide the higher security while communicating on the open channel. In the proposed system Elliptic curve cryptography (ECC) technique is used for data encryption and steganography uses 3 levels Discrete Wavelet Transform (DWT) method to hide the encrypted data. These two techniques will provide higher security and the system yields high quality image, less memory utilization, more complexity and higher embedded capacity.

KEYWORDS: Cryptography, Steganography, ECC, 3 level DWT.

I. Introduction

Data security over a open channel network is one of the most important concept nowadays. Because every single person uses internet for data exchange hence securing data becomes more valuable. So confidential data transmission need some protection from unauthorized users. Combination of cryptography and steganography techniques provides higher security and most used techniques for data transmission over open network. In cryptography the plaintext is encrypted to cipher text to protect the data from unauthorized access. There are three types of cryptographic techniques: Symmetric cipher, Asymmetric ciphers and Key exchanges. A symmetric cipher depends on key size and same key is used for both encryption and decryption. Asymmetric cipher consists of two different keys, public key and private key. Where in steganography digital data like image, audio and video is used as a cover image for hiding information and cover image with hidden information is called stego image which looks similar and unsuspicious.

In the proposed system Elliptic Curve Cryptography (ECC) is used for data encryption and decryption. ECC is a public key encryption technique. Where same key is used for data encryption and decryption. This technique is most widely used in video conferencing, social medias etc,. Efficiently deals with the confidentiality of information over open channel. Steganography uses 3 level DWT method to hide the encrypted data. Discrete wavelet transforms are used to convert the image in spatial domain to frequency

domain and then secret message is embedded into the transformed cover image. Thus, the DWT technique describes the decomposition of the image in four non overlapping sub-bands with multi-resolution.

The goal of this work is to combine both steganography and cryptography techniques, which will enhance the security of the data embedded. This combination will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. Many researchers have invented different methods to encrypt and hide information. Cryptography fails if hacker accesses the content of the cipher message; while steganography fails if hacker detects that there is a secret message present in the steganographic medium. Since simple techniques are easily detectable by steganalysis, which is an integral field of defeating steganogrphic techniques. Hence new techniques are developed for higher data security.

II. Literature Survey

Hayfaa Abdulzahra Atee et al,[1] proposed the combination of cryptography and steganography techniques. A dynamic encryption method is used for cryptography and simple LSB and Color Image Based Data Hiding (CIBDH) are the steganograpic methods used. To hide the secret messages into image, the sequential concealment technique is used by simple LSB and the concealment technique is used by CIBDH. Parameters such as PSNR, capacity and MSE values for robustness are considered.

Pye Pye Aung et al, [2] 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. Steganography technique used here is Discrete Cosine Transform (DCT) which uses a part of encrypted message as a key to hide in an image. Parameters such as security and robustness, image quality are considered.

Harleen Kour et al, [3] proposed the cryptography and steganography techniques in which Multiple Least Significant bit (MLSB) is the steganography method used for data hiding. In order to provide security over unauthorized access Digital Signature Scheme Algorithm (DSA) is used for encryption of data and provides data security over the network.

Dipti Kapoor Sarmah et al, [4] proposed the cryptography technique in which Advanced Encryption Standard (AES) is used for data encryption and Discrete Cosine Transform (DCT) is used to hide a part of message in an image and secret key is generated using remaining part of message to make secure system. Parameters like image quality and security over network are considered.

Blessy Joy A et al, [5] proposed the cryptographic technique, ECC technique is used to encrypt the RGB image to protect the data from unauthorized access. The image undergoes pixel wise xor operation and encrypted by ECC. Required number of bit planes is encrypted to achieve different levels of security. Parameters like processing

power, energy, bandwidth limited for ECC are considered. It is used in multimedia communication.

G. A. Sathishkumar et al [6] proposed the multiple chaotic based circular mapping methods which is used for image encryption and data security. Chaotic logistic maps gives pair of sub keys and logistic map sub key is used to encrypt the image. To decrypt the encrypted image the receiver uses the same sub keys. Parameter such as PSNR, loss-less encryption, symmetric key encryption, huge secrete key, less cross correlation are considered.

Aayushi Verma et al, [7] proposed steganography technique that is Discrete Wavelet Transform (DWT). The complexity of hidden image has been decreased through DWT technique. The DWT algorithm is used for embedding and extracting the secret image embedded behind the cover gray scale image. Parameters such as Peak signal to noise ratio (PSNR) and Mean square error (MSE), secure, robust and embedding capacity, less distortion are considered.

A. Anto Steffi et al, [8] proposed the cryptographic technique which uses chaotic baker map and chaotic Lorenz map for image encryption in order to secure the image transformation. Two chaotic maps are employed with 128 bit of eternal secrete key. Different weight age has been provided for all the bits in the external secrete key. Parameters such as high sensitivity towards the secrete key and very large key space are considered.

Pallavi H. Dixit et al, [9] proposed the cryptography and steganography techniques for data security on open network. BLOWFISH method is used for data encryption and Steganography uses List significant Bit (LSB) for hiding the encrypted data. Iris image of authorized person is used to hide encrypted data for the security purpose. The secret key is generated from same iris image which is required for encryption using BLOWFISH algorithm. On 32 bit ARM 7 the algorithms are implemented. Parameters such as memory utilization, processing time for encryption and decryption, security for embedded systems are considered. it is used in mobile, smart card, ATM etc.

Melad J. Saeed et al, [10] proposed the cryptography and steganography techniques in which chaotic method is used for data encryption and Discrete Cosine Transform (DCT) domain to hide encrypted color image. The original image in spatial domain is transformed to frequency domain using DCT. The cover image is embedded in DCT. Parameters such as MSE, PSNR and normalized correlation (NC), to phase and capacity are considered.

Pratibha Sharma et al [11] proposed the steganographic technique, in which 3 level discrete wavelet transform (DWT) is a steganographic method uses for digital image watermarking is presented and it is compared with 1 and 2 levels DWT. In the low frequency sub-band of a cover image multi-bit watermark is embedded by using alpha blending technique. During embedding, depending upon the scaling factor of alpha blending technique watermark image is dispersed within the original image. The

watermark image is extracted by same scaling factor as for embedding. Parameters such as peak-signal-to-noise-ratio (PSNR) and mean square error (MSE) are considered.

Chandra Prakash Shukla et al, [12] proposed the combination of cryptography and steganography to protect the confidential messages on any network. Where Rivest Shamir Adleman (RSA) algorithm is used to secure the message from the hacker. The RSA algorithm converts the text message to cipher text. It is used in FBI, RAW and in security agencies to transfer the secret message.

K.S.Abitha et al, [13] proposed the cryptographic technique in which Elliptic Curve Cryptography (ECC) used to secured data transmission, which increases network security using Ad Hoc on Demand Distance Vector Routing (AODV) algorithm for transfer of data and also increment the efficiency of AODV algorithm using ECC. Parameters such as efficiency and reliability are considered. ECC algorithm is used to encrypt and decrypt the data that is to be transferred

Lei Lei, Chao Wang et al, [14] proposed the steganographic technique in which Discrete wavelet transform (DWT) technique is used for data hiding. Selecting a suitable Decomposition Level (DL) in DWT is of paramount importance to its performance. Sparseness of the transformed signals will determine the appropriate DL. The sparseness of transformed signals after DWT increases with the increasing DLs. it is effective, and widely adopted in biomedical signal processing for denoising, compression and so on.

Mahmoud F. Abd Elzaher et al [15] proposed the cryptographic technique, which is used for communication of voice on secure channel. The voice samples undergo permutation and substitution using transform domains and secret keys in time. To increase the security chaotic maps are used. For permutation of the samples Arnold cat map is applied, in the substitution process Henon map is used for key generation to generate mask keys. Parameters considered are key sensitivity and high quality recovered signal, larger key space.

Ms. Nikita N Chintawar et al, [16] proposed cloud computing technique for data security. ECC is the public key encryption technique. ECC provides protection for authentication, key generation and encryption of data and secure communication. ECC also provides cloud security and data security of cloud in cloud computing by creating digital signature and encryption with elliptical curve cryptography.

R.Nivedhitha et al, [17] proposed the combination of cryptography and steganography techniques for data encryption and hide the data in another medium through image processing. The data is secured using Data Encryption Standard (DES) algorithm for key image generation. The LSB technique is used to hide the encrypted image. By using the same key image the decryption is done using DES algorithm. Parameters considered are imperceptibility and higher similarity between the cover and stego image.

Kimmo J¨arvinen et al [18] proposed the Elliptic Curve Digital Signature Algorithm (ECDSA) in which Altera Cyclone II EP2C20F484C7 FPGA is implemented using a

DE1 development and education board. Digital signatures are digital counter parts of handwritten signatures. Signature is proof of authorship and authenticity and data is unforgeable. The document provided has not been altered after signing. Nios II Integrated Development Environment (IDE) is used to demonstrating the design.

Andrea Miele et al [19] proposed elliptic curve cryptography algorithm for encryption. ECC technique is implemented on constrained devices such as smart phones, allowing to generate ephemeral parameters that are unique to any single cryptographic application such as symmetric key agreement.

Saleh Saraireh et al, [20] proposed a secure communication system using cryptographic algorithm together 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 encryptedmessage in the cover image by modifying the wavelet coefficients. Parameters such as peak signal to noise ratio (PSNR), histogram analysis, security, scalability and speed are considered.

III. Proposed System

ECC is the public key encryption technique. Which generates the key using elliptic curve equation on finite field instead of prime numbers. ECC provides higher security with smaller key size, with the limited storage and smaller key size ECC provides speedier data transmission. ECC yields security with 164 bit key where the other system need 1024 bit key to access the data. Using ECC technique equivalent security have been estimated with low computation power and battery usage. ECC method nowadays used in wide variety of applications such as mobile phones, internal communication, also used to encrypt DNS information.

The cover image is decomposed using 3level DWT method. Frequency and spatial description of an image is provided by wavelet transform. Higher frequency component of the cover image is selected to hide the secret image efficiently. Signal is spitted into higher and lower frequency parts by DWT. Coarse information of signal is present in the low frequency part and edge components information is present in the high frequency part. At each level of decomposition two dimensional applications is obtained. The vertical direction DWT is performed first followed by horizontal direction DWT. At the 1st level of decomposition LL1, LH1, HL1, HH1 4 sub-bands are obtained. At the 2nd level of decomposition LL sub-band of the 1st level is considered as input. The same technique is continued up to 3level to obtain 4 sub-bands i.e., LL3, LH3, HL3, HH3.

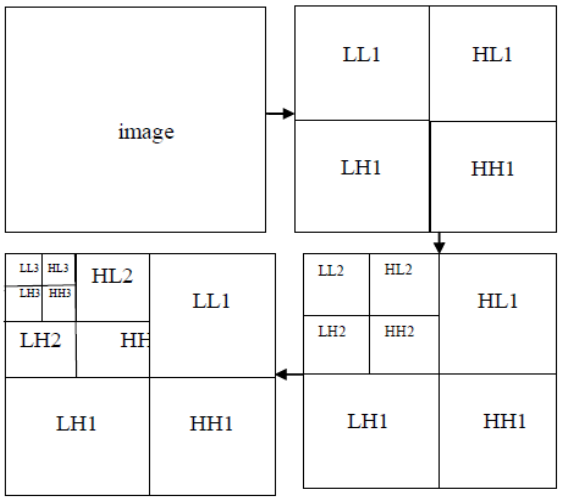

Figure 3.1: 3 level Discrete Wavelet Transform (DWT)

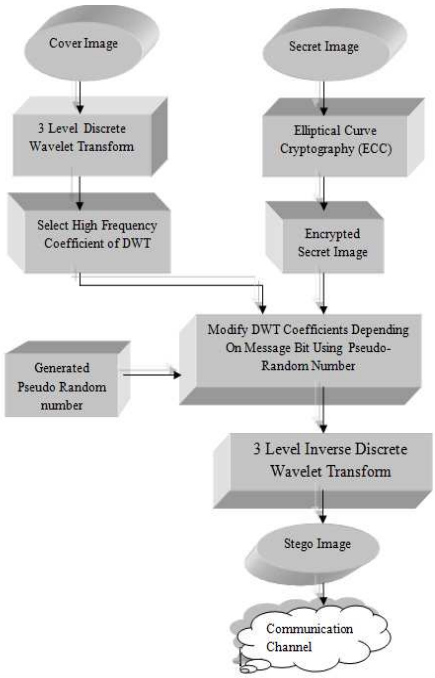

Figure 3.2: Block diagram for secret message embedding

Different sizes of images are converted into uniform size (256x256). To reduce the design complexity color image is converted into gray image is converted into gray image. In the encryption technique secret message is encrypted using ECC. 3 levels DWT steganography is applied on cover image and high frequency coefficients are selected to embed secret encryption message using pseudo random numbers and 3 level inverses DWT is performed to obtain stego image.

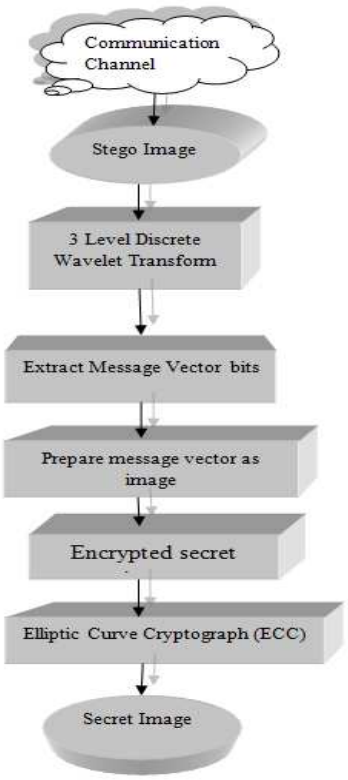

Figure 3.3: Block diagram for secret message recovery

The cover image is available for receiver and the stego image is decrypted to obtain secret image, comparing the mean correlation value of DWT coefficients of both image the encrypted secret image is reconstructed. By using ECC on encrypted data, the secret image has been recovered.

IV. Conclusion

The combined cryptography and steganography features, which provides satisfying factors for better performance. ECC method is used for encryption of the data and steganography uses 3 levels DWT to hide the encrypted data and the data is secured during transmission over the open channel. The proposed system provides high complexity, higher security and the system yields high quality image, less memory utilization and higher embedded capacity. Hence hackers face difficulty while accessing the secret data.

References

[1] Hayfaa Abdulzahra Atee, Robiah Ahma and Norliza Mohd Noor, Cryptography and image Steganography usin dynamic encryption on LSB and color image based data hiding, publication 2015.

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

[3]. Harleen Kour, Surinder Kaur, Data Hiding Using MLSB Steganography, Volume 5, Issue 1, January 2015.

[4]. Dipti Kapoor Sarmah, Neha BajpaiProposed System for data hiding using Cryptography and Steganography

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

[6]. G. A. Sathishkumar, Dr. K. Bhoopathy bagan and Dr. N. Sriraam, Image encryption based on diffusion and multiple Chaotic maps, Vol. 3, No. 2, March 2011.

[7]. Aayushi Verma, Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal , Implementation of Image Steganography Using 2-Level DWT Technique.

[8]. A. Anto Steffi, Dipesh Sharma, Modified algorithm of encryption and decryption of image using Chaotic mapping.

[9]. Pallavi H. Dixit, Kamalesh B. Waskar, Uttam L. Bombale, Multilevel Network Security Combining Cryptography and Steganography on ARM Platform,Vol. 3, No. 1, 2015

[10]. Melad J. Saeed, A new technique based on Chaotic Steganography and Encryption text in DCT domain for color image, Vol. 8, No. 5, 2013.

[11]. Pratibha Sharma, Shanti Swami, Digital Image Watermarking Using 3 level Discrete Wavelet Transform, 2013

[12]. Chandra Prakash Shukla, Ramneet S Chadha, Abhishek Kumar, Enhance security in stegnography with cryptography, Vol. 3, Issue 3, March 2014.

[13]. K.S.Abitha, Anjalipandey, DR.K.P.Kaliyamurthie, Secured Data Transmission Using Elliptic Curve Cryptography,Vol. 3, Issue 3, March 2015.

[14] Lei Lei, Chao Wang, and Xin Liu, Discrete Wavelet Transform Decomposition Level Determination Exploiting Sparseness Measurement, Vol:7, No:9, 2013.

[15]. Mahmoud F. Abd Elzaher, Mohamed Shalaby, Salwa H. El Ramly, Securing Modern Voice Communication Systems using Multilevel Chaotic Approach, Volume 135 – No.9, February 2016.

[16]. Ms. Nikita N Chintawar, Ms. Sonali J Gajare, Ms. Shruti V Fatak, Ms. Sayali S Shinde, Prof. Gauri Virkar Enhancing Cloud Data Security Using Elliptical Curve Cryptography Vol. 5, Issue 3, March 2016.

[17]. R.Nivedhitha, Dr.T.Meyyappan,M.sc.,M.Phil.,M.BA.,Ph.D, Image Security Using Steganography And Cryptographic Techniques, Volume3Issue3- 2012.

[18]. Kimmo J¨arvinen, Prof. Jorma Skytt¨a, Cryptoprocessor for Elliptic Curve Digital Signature Algorithm (ECDSA), August 7, 2007

[19]. Andrea Miele, Arjen K. Lenstra, Efficient ephemeral elliptic curve cryptographic keys

[20].Saleh Saraireh, A Secure Data Communication System Using Cryptography And Steganography, Vol.5, No.3, May 2013