Volume 5, Issue 2, February 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

RGB Image Encryption Based on Bitplanes Using Elliptic Curve Cryptography

Blessy Joy A*, R. Girish
Department of Information Technology
Nehru College of Engineering and Research Centre
Thrissur, Kerala, India

Abstract*— The recent advancements in Information technology increase the use of multimedia transmission through open networks. This paper proposes a new encryption technique for encrypting RGB images using Elliptic Curve Cryptography (ECC) to protect those files from unauthorized access. The images are classified into two depending upon the required level of security. A pixel wise XOR operation is applied for the images which are shared in a secure network like intranet. For highly confidential images 2 stage encryption method is applied. In the first stage the image is XORed with the key image in order to produce the 1st level encrypted image. This image is again encrypted using ECC to produce the final output. In RGB image encryption, the three components of the image are considered separately and encrypted separately. Different levels of security can be achieved by encrypting required number of bitplanes. Since the higher bitplanes contain more information, they have given higher priority to be encrypted. Since images are encrypted based on the bitplane, it is difficult for the attacker to capture the original image. After the encryption, compression is also applied. ECC is suitable for the environments where processing power, energy, bandwidth are limited. So this encryption method can be adapted in mobile communication. ECC is best suitable for real time requirements of multimedia too.

***Keywords*— ECC, RGB Image, XORing Images**

I. INTRODUCTION

Information technology is the one of the most demanded area today. It is the branch of information technology that deals with the security of the information which is transferred through the open networks and stored in a database. In recent days, the use of multimedia has increased drastically. The major multimedia applications include Pay TV, Video conferencing, video telephony, Internet television etc. These multimedia files are transferred through open networks. The open networks are often unsecured. The main challenges hidden in the open networks are unauthorised access, use, disruption, modification, inspection and recording or destruction. The only way to secure the confidential information from the above mentioned problem is to use an effective cryptographic mechanism. Cryptography is the art of secret writing. The basic service provided by the cryptography is the ability to send information between two parties without allowing an unauthorised third party to access or destroy that particular information. In cryptography, the original message is known as plain text and the mangled information is known as ciphertext. The process of generating the ciphertext is known as encryption and the reverse process is known as decryption.

Digital images are attractive data type with widespread range of use and many users are interesting to implement content protection methods on their images to keep from preview, copyright or manipulation. In many applications like military image databases, confidential video conferencing, medical imaging system, cable TV and online personal photograph album, security is essential. Also wide application of images at industrial process turns it into a resource and asset. So it is important to protect confidential images data from unauthorized access [5].

The cryptographic algorithms are classified in to two. They are symmetric cryptographic algorithms and asymmetric cryptographic algorithms. In symmetric encryption algorithms, a same secret key is used to encrypt and decrypt the data. The problems regarding the symmetric key encryption are the privacy of the secret key and the difficulty of storing the keys for all the users. For e.g. if there are *n* number of users in a network, a user has to store *(n-1)* number of keys. The examples of symmetric key encryption include Advanced Encryption Standard (AES) and Data Encryption Standard (DES). The asymmetric key cryptosystems use two large keys for encryption and decryption processes. These keys are called public and private keys and any of them can be used for encryption or decryption. Examples of asymmetric key cryptosystems are Rivest, Shamir, Adleman (RSA) and El-Gamal cryptosystem. The hardness of the underlying mathematical problem represents the fundamental security of all protocols in the public-key family. Hence, asymmetric key cryptography is slower. The application of symmetric key over multimedia networking applications is not practical because each participating entity requires storing the keys of all other entities [1]. Elliptic Curve Cryptography (ECC) is the one of the public key cryptography which is most suitable for multimedia encryption. It is shown that ECC is suitable for the environments where the processing power, storage, band width and power consumption. In this paper ECC is used to encrypt the multimedia file.

Upon encrypting a multimedia file, the characteristics of multimedia files should be considered. Compared with other data types, multimedia files have larger size. When the entire file content has encrypted it will introduce a large overhead at the sender and the receiver. If the multimedia files are completely encrypted, on the receiver side it will take more time to decrypt the information and there by the streaming of the information will be lost. So in order to overcome this problem the concept of selective encryption was introduced. In selective encryption, only the selected part of the multimedia is encrypted. In this paper, Selective encryption is used to achieve the real time requirements of the multimedia file.

II. RELATED WORKS

There are many techniques which uses ECC to encrypt the multimedia files. . In [2] ECC was used to encrypt image without compression, where every pixel of the uncompressed image was encrypted. Since the image was not compressed, the resultant image was of large size and hence consumed large band width. In [3] ECC was used only to encrypt the secret key hat was used to encrypt images. The image encryption itself was done using permutation and diffusion or code computing. A texture image was formed from the source image using ECC. The texture image and source image are XORed to get the pre output image. This image is encrypted pixel by pixel using ECC. This method does not incorporate any compression technique. In [4] ECC points convert into cipher image pixels at sender side and decryption algorithm is used to get original image within a very short time with a very high level of security at the receiver side. Unlike the above mentioned techniques that uses ECC; in this paper ECC is applied to selectively encrypt the portions of the multimedia data along with compression in order to meet the real time requirements of multimedia encryption.

III. MULTIMEDIA ENCRYPTION AND COMPRESSION

If the files are not compressed, they will consume larger band width. So it is essential that the files must be compressed. The compression algorithm can be implemented in three places. They are- before encrypting the data, along with the encryption and after encrypting the file.

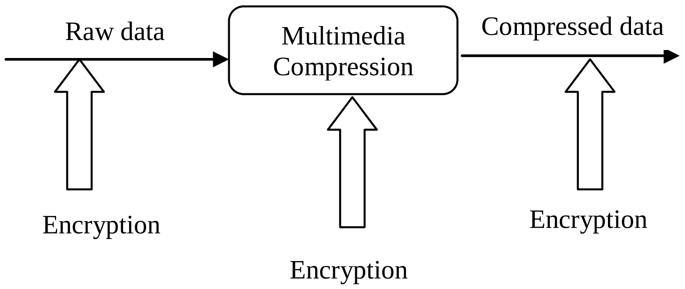

Fig 1. Possible placements of multimedia encryption algorithms

In this paper, the compression is applied after the encryption. i.e., first the image is encrypted using ECC and then the encrypted image is compressed using JPEG algorithm.

IV. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. ECC is a public key cryptosystem, which has a public key and a private key pair. Public key is shared between the group of users participate in the communication, while the private key is kept secret. ECC need a set of predefined parameters. They are the following.

Table 1. Ecc parameters

p	Prime number defines the elliptic curve
a	a and b together forms set of solutions (x,y) to an equation of the form $y^2 = (x^3+ax+b)$ mod p ≠0, where (4a3 + 27b2)mod p ≠ 0
b	
G	Generator point
n	Constant

The operations on the elliptic curve are the following. [1]

1. P + O = P.
2. If P = (x, y), then −P = (x, -y).
3. P + (−P) = O.
4. If P = (x_1, y_1) and Q = (x_2, y_2) with P ≠ Q, then R = P + Q = (x3, y3) is calculated as follows:

$x_3 = (m - x_1 - x_2)$ mod p

$y_3 = (m(x_1 - x_3) - y_1)\bmod p$
where

$$m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}\ mod\ p\ if\ P \neq Q(point\ addition) \\ \dfrac{3x_1^2 + a}{2y_1}\ mod\ p\ if\ P = Q(point\ doubling) \end{cases}$$

5. Scalar multiplication is defined as a series of additions. For example, 3P = P + P + P, where P + P is calculated using point doubling operation and the result is added to point P using point addition.

ECC encryption and decryption methods cannot encrypt and decrypt real plaintext; they only can encrypt and decrypt points on the curve. Thus, plaintext encoding should be done before encryption, and decoding should be done after decryption. Encoding means converting a plaintext message into points defined by the elliptic curve in order to be suitable for encryption, while decoding means converting the points into the original message[6]. In this paper, I used Koblitz method encode and decode the points. After encoding the points, the following method can be used to encrypt and decrypt the messages respectively.

A. *Message Encryption Using ECC*

Let A and B the two communicating entities. m be the message to be encrypted. The first step is to encode the message into a point in the elliptic curve using Koblitz method. P_m is the encoded point. The two parties A and B should select their own private key. Let n_A and n_B the private keys of the entities. To generate the public key, multiply the private keys with the generator point G. For encryption

$$Cm =\{ kG, Pm+ kPB\}\text{------}(1)$$

Where C_m is the cipher text and k is the random positive integer chosen by the entities
For decrypting the data,

$$P_m + kP_B - n_B(kG) = Pm +k(n_BG) - n_B(kG) = P_m \text{--------}(2)$$

V. IMAGE ENCRYPTION USING ECC

In this paper, the images are classified into two depending upon the required level of security. If the images are shared in a secured network like intranet, that images does not need to encrypt by using the complex cryptographic algorithms. So for such images simple pixel wise XORing of images has been performed. The original image is XORed with a key image to produce the final encrypted image as shown in the figure 2. This mechanism can be considered as a symmetric key encryption. Only the user who knows the key image can decrypt the image. So this method ensures confidentiality and authentication required for an intranet.

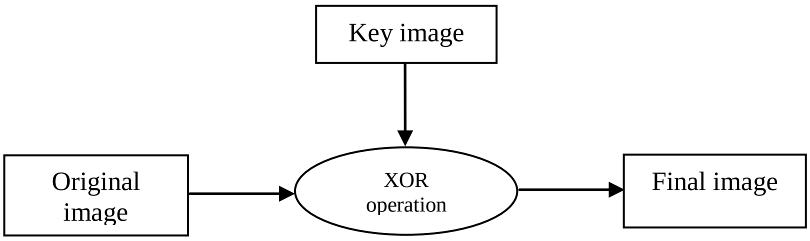

Fig 2 XORing 2 images

For other images, ECC is used to secure them. The user has given with a choice to convert the RGB image to greyscale image. Greyscale images are represented using 8 bits. Let $b_0b_1b_2b_3b_4b_5b_6b_7$ be the single pixel of the greyscale image. And each bit is either 0 or 1. Hence, we can form eight binary images from each bi of all the pixels in the greyscale image in which each binary image is called a bitplane. The binary image formed from the most significant bits (MSB) is called bitplane 8, and the binary image formed from the least significant bits (LSB) is called bitplane 1, and so on. The higher-order bits usually contain most of the significant visual information, while the lower-order bits contain the subtle details [1]. The user can select the number of bitplanes to be encrypted. More number of bitplanes will produce more clear images. If the user needs a high quality image, he should select more number of bitplanes. 8 bits in a bitplane is grouped together and encoded into a point on the elliptic curve and then encrypted into two points of four cipher values, where each value is represented by 32 bits. The cipher values are stored in the LSB bitplane, since it contains only subtle details, and grouped as blocks, each contains 4 cipher values. As a result, each encrypted segment is associated with a block of 128 bits, where the block number is stored in place of the original segment. Since the segment values range from 0 to 255, only 256 blocks at most are required to store the cipher values of all segments. For instance, to encrypt a bitplane of size 256 × 256 bits, only half of the LSB bitplane size (256 × 128 bits) is required to store all the blocks of the cipher values[1].Then the entire cipher text is compressed using JPEG.

RGB images have 3 components which represent red, green and blue colour of the image. RGB images are essential to represent high quality images. For example, medical image, blueprints, technical drawings. All the methods do not give much importance to the quality of the image, while the above mentioned figures should be received with highest quality. This paper proposes a method to encrypt the RGB image. Most of the encryption mechanisms do not provide any chance to the user to determine the level of security needed. In this paper a new mechanism which considers the user privileges are also introduced. The entire encryption process can be explained as follows.

RGB image is represented using 24 bits. Ie, three 8 bit numbers are used to represent the RGB image as follows. $r_0r_1r_2r_3r_4r_5r_6r_7$ $g_0g_1g_2g_3g_4g_5g_6g_7$ $b_0b_1b_2b_3b_4b_5b_6b_7$. Where each r_i represent the red component, each g_i represent the green component and each b_i represents the blue component. Each bit will have a value 1 or 0. While we are encrypting the RGB images, the 3 components should be considered separately. Each components' bitplanes are encrypted using the above mentioned method. Then they are compressed to get the final image. The reverse process is done at the receiver side.

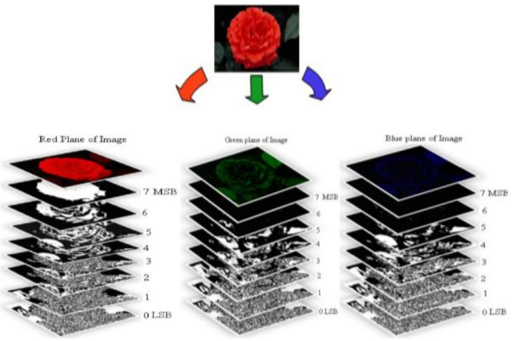

Fig 2 Bitplanes of RGB image

For providing more security, a two level encryption method can be used. In the first stage, the original image is Xored with a key image to produce the intermediate image. then this image will undergo the ECC according to the user requirements.

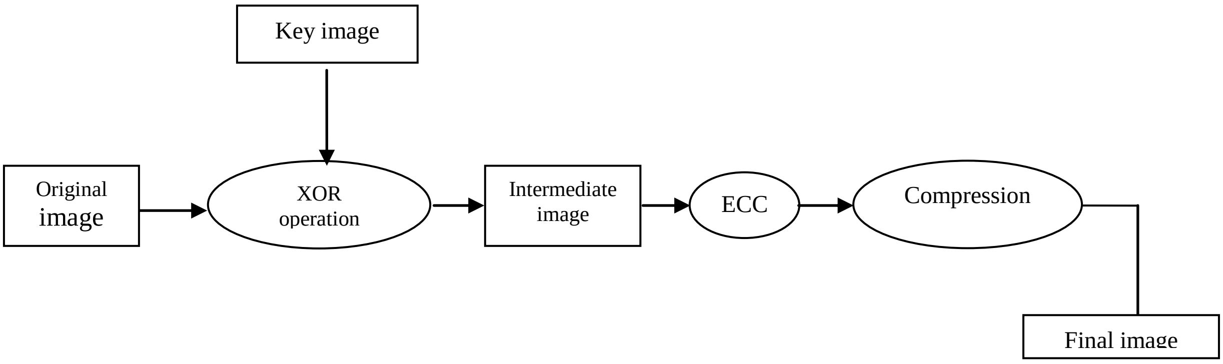

Fig 3. Entire Encryption Process

VI. Results And Conclusions

Bbefore the iamge is encrypted the noise removal is done. It is a process used to remove the unwanted signals from the image. the screen shot for the noise removal is given below.

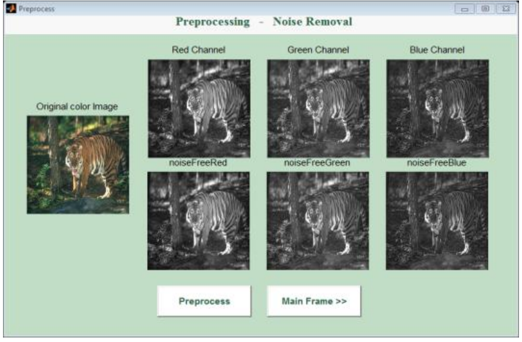

Fig 4. Noise Removal

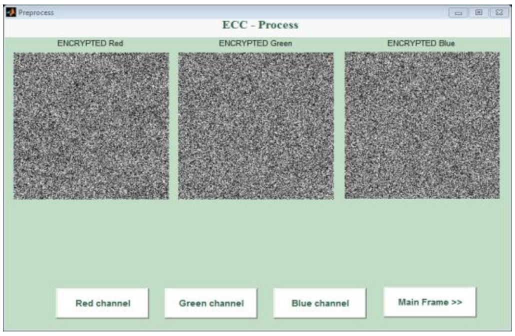

Fig 5 Encrypted Componets of the image

Regarding the encryption efficiency, the ECC operations are generally fast and can meet the deadline of multimedia streams playout at the receiver end. Compared with other public key algorithms, ECC uses addition operations instead of multiplication and uses multiplication operations instead of exponentiation. In regard to the compression efficiency, ECC generates four cipher values for each encrypted DCT coefficient, in case of selective encryption, and similarly for each 8-bit segment of the encrypted bitplane, in case of perceptual encryption. This additional data are stored in place of

In significant information (the high-frequency DCT coefficients or LSB bitplane), which do not increase the size of the compressed data.

Concerning the security level, ECC relies on the discrete logarithm problem in which it is very difficult for the adversary to extract the key given the first point of cipher pair (kG) and the generator point G. Even if a small key is used for the purpose of speedup, the key cryptanalysis may not cause a security threat. For instance, the small key size is preferred if the time that the adversary takes to discover the ECC key is longer than the playout time of the multimedia stream, or if the encryption is oriented for entertainment applications.

ACKNOWLEDGMENT

Achievement cannot be made by the individuals of a project alone. Even though our efforts were immense, the constant guidance and help from people outside the group played an important role in successfully finishing the project. I would like to take this opportunity to thank all those people who helped me out. First and foremost I would like to thank the **God Almighty** for blessing us with his grace and taking our endeavour to a successful culmination. I express my heartfelt thanks to my guide and inspiration **Mr. R. Girish,** Asst.Professor, NCERC, for his valuable support, guidance and constructive ideas throughout our projects. I thank all the assistant professors and supporting staff for their help and I would like to thank my friends who helped me for the successful completion of my project.

.

REFERENCES

[1] Lo’ai Tawalbeh et al, ‘Use of elliptic curve cryptography for multimedia Encryption’ IET Information. Security, Vol. 7, Iss. 2, pp. 67–74, Nov 2013

[2] Gupta, K., Silakari, S., Gupta, R., Khan, S.A.: ‘An ethical way of image encryption using ECC’. Proc. First Int. Conf. on Computational Intelligence, Communication Systems and Networks, Indore, pp. 342–345, July 2009

[3] Gupta, K., Silakari, S., ‘Efficient image encryption using MRF and ECC’, International. Journal. Information. Technology. Know. Manage, pp. 245–248, 2009

[4] Yadav, V.K., Malviya, A.K., Gupta, D.L., Singh, S., Chandra, G,: ‘Public key cryptosystem technique elliptic curve cryptography with generator g for image encryption’, Int. J. Comput. Technol. Appl., (1), pp. 298–302, 2013

[5] Ali Soleymani et al., “A Novel Public Key Image Encryption Based on Elliptic Curves over Prime Group Field”, Journal of Image and Graphics, Volume 1, No.1, pp 43-49, March, 2013

[6] Bh, P., Chandravathi, D., Roja, P.P.: ‘Encoding and decoding of a message in the implementation of elliptic curve cryptography using Koblitz’s method’, Int. J. Comput. Sci. Eng., pp.1904–1907,2010