Grenze International Journal of Engineering and Technology, July 2015

Securing Images using Elliptic Curve Cryptography

[1]Blessy Joy A and [2]Girish R
[1, 2]Department of IT, Nehru College of Engineering and Research Centre, Thrissur, Kerala, India

***Abstract*—The use of multimedia files has been increased drastically. These files may contain sensitive information like military images, medical images, and technical blueprints. This information is passed through open networks which are insecure. This paper proposes a method to encrypt the images according to the required level of security. In the paper, the images are classified into three groups. They are- images having low, intermediate and high security. Different encryption methods are used for these three categories of images. The main contribution of this paper is RGB image encryption using Elliptic Curve cryptography. This paper gives more privilege to the user to select the encryption method and image quality. After the encryption, the images are compressed using JPEG method. Since ECC is used for encryption, this method is highly suitable for mobile environments where the processing power and battery life is limited.**

***Index Terms*— RGB image encryption, bitplanes, Elliptic curve cryptography, Xoring mages.**

I. Introduction

With the growth of the technology, the security of images has become a major concern. To overcome the problem of insecurity of images, encryption is the most popular method used. In the image encryption, the original image is converted to another image which hard to understand the original image can be retrieved only if the correct key is used in the decryption phase. The encryption of images varies from that of text. Up on encrypting the images, the characteristics of multimedia files should be considered. The multimedia files are loss-tolerant, synchronous and power hungry. They also consume large amount of power. These characteristics must be considered while encrypting the multimedia. By considering these characteristics the multimedia encryption in classified in to two. First method is called naïve encryption, in which the entire multimedia frames are encrypted. Obviously this is not an efficient method since it will introduce considerable delay at the receiver's side. This delay interrupts the continuous nature of the multimedia files. So another method called selective encryption is introduced. In this method, only the selected frames or parts of the multimedia files are encrypted. A subgroup of selective encryption is called perceptual encryption, in which encrypted multimedia data are still partially perceptible in order to make a sense about the high-quality version.

The conventional encryption algorithms are used to encrypt the images. The conventional encryption algorithms can be of two types. They are- symmetric and asymmetric key encryption. In symmetric key encryption a shared 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.

Grenze ID: 01.GIJET.1.2.550

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. Elliptic Curve Cryptography (ECC) is one of the asymmetric key cryptosystem which has low computational complexity and low power consumption. In this paper, ECC is used to encrypt the image.

II. Related Works

ECC has a lot of advantages over other encryption algorithms. So recently many methods were proposed on image encryption using ECC. Some of the methods are described below.

A. An ethical way of image encryption using ECC

In this paper, ECC was used to encrypt the message without compression. i.e, each pixel in the image is encoded into a point on the elliptic curve and this point was encrypted and sent to the receiver. No compression method was used in this technique. The resulted encrypted image was of large size. Since a single pixel value was encoded into affine coordinates, the size of the encrypted image will be double that of the original image.

B. Public key cryptosystem technique elliptic curve cryptography with generator g for image encryption

In this paper, 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. In this method also pixel wise encoding is done. And no compression algorithm is used.

C. A Novel Public Key Image Encryption Based on Elliptic Curves over Prime Group Field

In this paper a new mapping method introduced to convert an image pixel value to a point on a predefined elliptic curve over finite field GF(p) using a map table. This mapping technique was very fast with low complexity and computation, easy to implement and for low entropy plain images, mapping will results a high distribution of different points for repetitive intensity values.

III. Elliptic Curve Cryptography

In the proposed system, ECC is used to encrypt the image. After the encryption, the compression is also done. Before moving on to the image encryption, let's discuss the entire process of ECC.ECC is a public key cryptosystem which has two keys- private key and public key. The public key will be distributed among the group of users. ECC works based on elliptic curve theory. The standard equation for the elliptic curve can be written as follows.

$$y^2 = x^3 + ax + b \text{ mod p} \qquad (1)$$

In the above equation p is the prime number based on which the elliptic curve is generated. Not all elliptic curves can be used for cryptography. The condition to be satisfied is the following.

$$(4a^3 + 27b^2) \text{ mod p} \neq 0 \qquad (2)$$

Now we selected the elliptic curve. The next step is to find the points on the elliptic curve. To find the points let's consider the following example. Let the prime number, p=5 and the constant a=1,b=1

First verify that $(4a^3+27b^2) \neq 0$ mod p.
Here $4a^3+27b^2 = 31 \neq 0$ mod 31
Now determine the quadratic residues of 5
$Q_5 = \{1,4\}$
Now $0 \leq x \leq p$ compute $y^2=(x^3+ax+b)$ mod 5

Table I. Finding Points On The Elliptical Curve

X	0	1	2	3	4
Y^2	1	3	1	1	4
$Y^2 \epsilon Q_5$	yes	no	Yes	Yes	yes
Y_1	1	-	1	1	2
Y_2	4	-	4	4	3

The points on the elliptical curve are $E_p(a,b)=\{(0,1),(0,4),(2,1),(2,4),(3,1),(3,4),(4,2),(4,3), \alpha\}$

The next step is to find the generator point (G) from the above set of points. The next step is to convert the binary values or ASCII values to affine coordinates. For this encoding, we have used Koblitz's method. After encoding the data will be the points on elliptic curve. The next phase is to encrypt those points.

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

$$Cm =\{ kG, Pm+ kPB\} \qquad (3)$$

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

$$P_m + kP_B - n_B(kG) = Pm +k(n_BG) - n_B(kG) = P_m \qquad (4)$$

III. Proposes System

A. Image encryption using ECC

In some instances, the complex cryptographic algorithms are not needed to encrypt the images. if the images are shared in a secured environment which is secured by a firewall, the complex encryption algorithms are just a waste of computational complexity. In order to preserve the computational complexity, this paper categorizes the images in to three. They are the images require low, intermediate and high security. Different algorithms are used for these different categories.

If the images are shared in a secured network like intranet, those 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. Xoring of image is a symmetric key encryption. If the image is xored with a key image, only the intended user who knows the key image can only decrypt the image. So this method can also ensure authentication too.

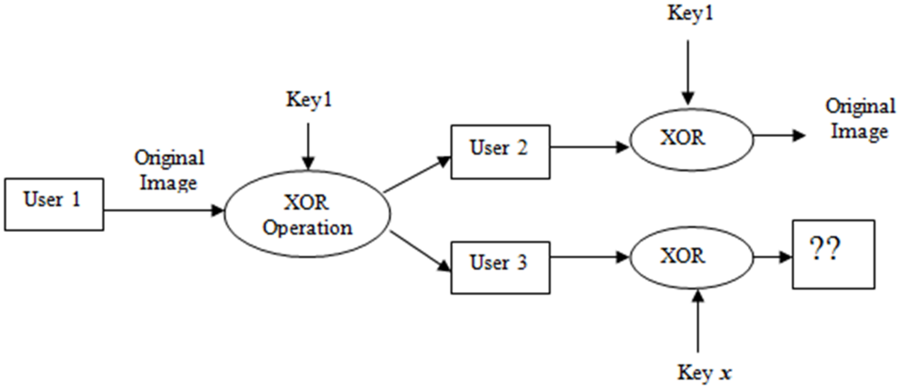

Figure 1. Xoring operation for images having low security

In figure 1, the xoring operation is illustrated. User 1 is the sender. He encrypts the original image using key image 1. The final result is broadcasted in the intranet. User 2 and 3 receives the encrypted image and both try to decrypt the original image by using the keys they have. User 2 only has the same key that of user 1. So only user 2 can only retrieve the original image. Since user 3 does not have the right key, he won't be able to retrieve the original message.

10010101	10101010	11001101	11001100
10100100	11000111	00000110	00101010
10010100	10111100	00000001	11100101
01010101	11001010	10111000	00110001

1111110011010110 —— MSB bitplane/ 8th bitplane

Figure 2. The pixel-wise representation of an image and formation of Bitplanes

For the remaining two categories, the image encryption is done on the basis of bitplanes. A bit plane of an image is a set of bits corresponding to a given bit position. For example, for 8-bit data representation there are 8 bit planes: the first bit plane contains the set of the least significant bit, and the 8th contains the most significant bit. Let the figure 2 represents a 16-pixel image. Each pixel in the image is represented by 8-bits. MSB of each pixel is highlighted in red color. By selecting all the MSBs of the every pixel, we can generate the MSB bitplane of the image. The MSB bitplane is given below to the image representation. The next step is to encrypt those bitplanes. These bitplanes are grouped into 8 bit groups. If the bitplane sequence is not a multiple of 8, then the last field is padded accordingly. Then these 8bit digits are encoded in to elliptic curve and then they are encrypted. After encryption, the image is compressed using JPEG.

For the images require intermediate security, the user is provided with an option to convert the RGB image to greyscale image. First we will discuss about the encryption of 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 b_i of all the pixels in the greyscale image. The higher-order bits usually contain most of the significant visual information, while the lower-order bits contain the subtle details. So by encrypting higher bitplanes we are preserve almost complete information of the image. Even though, the user is provided with an option to choose the number of bitplanes to be encrypted. 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. Then the entire cipher text is compressed using JPEG.

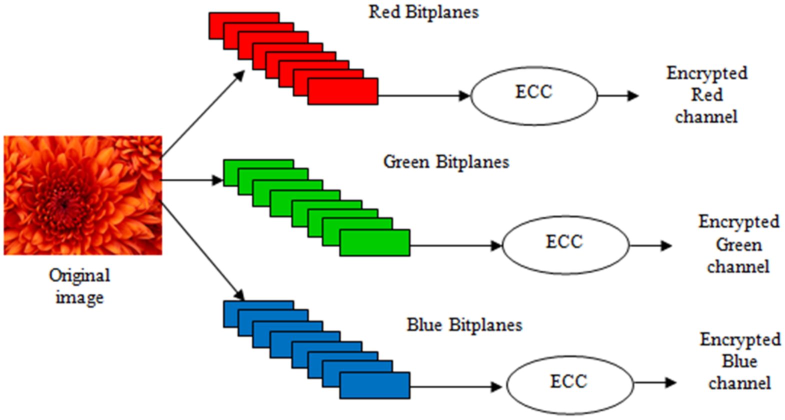

Figure 3. RGB image encryption process

RGB image encryption is different from greyscale image encryption. RGB image have three components which represent red, green and blue channels.8-bits are used to represent each component. Thus total of 24 bits is used to represent a single pixel in rgb image. To perform encryption, first we want to extract three components. That is, we are generating 3 images which represent red, green and blue channel. The result will be three images in which each pixel will be 8 bit in length. And the encryption is performed in each channel separately based on bitplanes. The RGB image encryption is proposed for the images which require high quality and high security. Si it is recommended to encrypt the all bitplanes so that the requirement can be met. Even though the user can select the number of bitplanes to be encrypted. The images in this category include the military images which describe the location of the operation, medical images like scanning reports and blueprints of drawings. After the encryption process, the images are compressed using JPEG.

IV. CONCLUSIONS

In this paper, image encryption techniques are introduced. This paper categorizes the images into three depending upon the required level of security. By proving less complex cryptographic mechanism to the less sensitive image we could preserve the computational complexity. Color image encryption is also proposed in this paper. This paper gives more importance to user privileges too. Since ECC is used to encrypt the images the real time constraints of the multimedia files are maintained. ECC is highly suitable for the environments where the computational power and battery power is limited. By using ECC for image encryption, the image encryption can be easily implemented in mobile devices in an efficient way. This method also can be used for the encryption in sensor networks too. Regarding the security of the system, the strength of the ECC lies on the discrete logarithm problem. It is very difficult to extract the original message if the attacker is provided with the intermediate values of the encryption. Since bitplane encryption is used, the attacker will be able to retrieve the entire image if and only if he retrieves the every bitplanes. This increases the security of the system. After the encryption JPEG compression is also applied. So the resultant image will be of smaller size.

This system can be enhanced to an intelligent system which can analyze the destination address and automatically chooses the encryption mechanism. For ensuring more security, a two phase encryption method also can be used. In this method, first the original image can be xored with a key image and the resultant image can be encrypted based on the bitplanes.

REFERENCES

[1] Lo'ai Tawalbeh et al,(2013) "Use of elliptic curve cryptography for multimedia Encryption", *IET Information. Security*, 7(2), 67–74

[2] Gupta, K., Silakari, S., Gupta, R., Khan, S.A.(2009), *An ethical way of image encryption using ECC in First Int. Conf. on Computational Intelligence, Communication Systems and Networks*, Indore.

[3] Gupta, K., Silakari, S.(2009), "Efficient image encryption using MRF and ECC', *International. Journal Information Technology*,245–248

[4] Yadav, V.K., Malviya, A.K., Gupta, D.L., Singh, S., Chandra, G(2013), "Public key cryptosystem technique elliptic curve cryptography with generator g for image encryption", *International Journal of Computer Technology and Application*, (1), 298–302

[5] Ali Soleymani et al.(2013), "A Novel Public Key Image Encryption Based on Elliptic Curves over Prime Group Field", *Journal of Image and Graphics*, 1(1), 43-49

[6] Chandravathi, D, Roja, P.P(2010), "Encoding and decoding of a message in the implementation of elliptic curve cryptography using Koblitz's method", *International Journal for Computer Science and Engineering*,1904–1907