International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 1148–1157

A Study of Image Encryption / Decryption by Using Elliptic Curve Cryptography "ECC"

Hamad Said Hamad AlDerai
Modern College of business and Science (MCBS)
Muscat,Oman
said9998@gmail.com

Basant Kumar
Modern College of business and Science (MCBS)
Muscat,Oman
basant@mcbs.edu.om

Abstract

Millions of images transferred every day on the world via online networks. Some of these images are private and wish to be transferred securely. Where encryption way an important part in maintaining the security of the image and its transmission over the network in a secure manner. The current difficult problem of solving the logarithm problem of the Elliptic Curve is a major Elliptic Curve that helps provide the size of key security with a top level of security compared to other encryption techniques that are dependent on valid factors or a separate logarithmic technique. This paper will review the analysis of the Elliptic Curve technique for encryption and decryption Performances.

Keywords — Elliptic Curve Cryptography; Authenticity; Integrity; Digital Signature;

1.0 INTRODUCTION

A lot of attention has been gained the image encryptions in recent years. And interest in this field, as many different methods have been proposed to encryption the images, and the most recent method is the Elliptic Curve Cryptography (ECC) technique. To use of sending and receiving the images through online in our daily life continues, and the exploitation of cybercrime attackers is to sabotage and know the content of images from data that are completely dangerous, for example, military graphs, which are dangerous to access army sites and sensitive data, as well as maps of banks buildings and their movements therein. Seriously, the computer attacker is likely to be exploited to learn moves to reach the desired goal. So that there is protection for transferred images over the internet networks to hide sensitive data and to maintain the protection of real images [1].

There is a lot of information that realizes when notice the image, and the images have become a source of information. However, still constantly observing different images from different sources. So, to secret images that are transferred safely, from here encryption methods are using tools and techniques to encryption the images. This paper will focus on analyzing the study of Elliptic Curve Cryptography (ECC). The study concluded that there is difficulty in a separate logarithmic problem for the elliptic curve, which relates to the size of the key used. The Elliptic Curve Cryptography (ECC) technology is the most suitable option for encryption/decryption, compared to other encryption/decryption technologies that are either linearly difficult or more difficult. Where Neil Koblitz and Victor S Miller developed the ECC in 1985. This technique gained wide acceptance in its use in 2004 [2].

2.0 LITERATURE SURVEY

Koblitz and Miller introduced elliptical curves to encryption in the middle of 1980 [3]. And, Lenstra's success showed to use of elliptical curves for coordinated value integers. it is the best of the main benefits of using elliptic curve cryptography and provided a security level similar to the classic with system encryption which using a large size of the key [3].

For example, Blake et al. [4] estimated the traditional system to be 4096 bits of the key size and efficiently replaced by 313 elliptic curves without losing accuracy and increase high clarity. This result provided to reducing hardware requirements and saving hardware implementation, causes by the smaller size of key requirements.

ISSN: 2233-7857 IJFGCN

Vanstone, Alfred Menezes, and Darrel Hankerson explained the types of elliptic curve algorithms, and exactly issues through the implementation and protocol of cryptography [5]. Jouko Teeriaho provided to show the implementation of various ECC using the Mathematics equation. so, to secure images transferred over the network by different techniques using ECC which recent years [6].

Abd El-Latif, Ahmed A, and Xiamu provided the technique of image encryption using the chaotic system with the cycle of ECC. They decided this technique to generate the key of random by using the encryption from the original image [7].

Yanbing Liu and Hong Liu made an analysis proposal for encryption of images built on the chaotic system and the elliptic curve that works periodically. The result of this analysis is that the attacker cannot attack the plain text and choose any normal image to determine the pixel value "0" and then create the encrypted image [8].

K. Muneeswaran and S. Maria Celestin Vigila presented an algorithm that uses this algorithm to encrypted images using ECC technology. They used a double line to extract a private key and an integer randomly "k". Also, they used the multiplication method on the bitmap on the cipher image for each pixel value on the elliptical curve coordinates [9].

A. Akhavan, A. Samsudin, Behnia, and A.Akhshani proposed algorithm of image encryption using the map of a Jacobian elliptic curve. So, the matrix of plain image data will be transferred into one matrix of dimension after operating with the key initiate. Then, elements which encrypted using the formula and matrix return back to the original dimension [10].

Xiamu Niu, Li Li, A.Abdl El-Latif suggested the encrypted image scheme using Elliptic Curve ElGamal technology, which in turn plays a homogeneous image together to share secret images. However, they chose a different parameter for the elliptic curve for similar attack resistance from the theory of both Pohling Hellman and Rho Pollard. The result which got it better than the encryption technique using ElGamal and RSA [11].

Scott Vanstone, Alfred Menezes, and Don Johnson described the implementation phase relate to interoperability and the part of security of the Elliptic curve algorithm of the digital signature [12]. While Walid Aljoby, Moad Mowafi, and Lo'ai Tawalbeh provided two ECC based on encryption images, such as selective bit plane and selective quantized DCT coefficients [13]. And Dr.Mamfred Lochter presented set parameters of elliptic curve cryptography across a finite prime field [14].

3.0 DIFFERENT IMAGE ENCRYPTION & DECRYPTION TECHNIQUES

3.1. Encrypt the images by using digital signature:

Kehar Singh and Aloka Sinha [15] [21] have proposed image encryption technology using the digital signature mechanism adapted from the original encrypted image. One of the best possible solutions is to follow the error code in the encrypted image. For example: (BCH) code stand to Bose-Chaudhuri Hochquenghem. Finally, the image receiver before decrypting validates the digital signature available in the encrypted image.

3.2. Encrypt the images by using image technique of multilevel and dividing:

Dong-Hoan Seo, SmJmng Kim, kyu-Bo Chol, Chang-Mok Shin and Ha Wmn Lee [16] [21] have proposed a new algorithm for image encryption, using a dividing image to binary levels, meaning that the gray level to divided the image into several levels, through which the encrypted image is renewed. [27].

3.3. Encrypt the images by using 1D chaotic map technique:

Uvais Qidwai and Fethi Belkhouche [17][21] proposed the method to encryption the images by using possibly several keys such as iterations' number, the external parameters, and the initial state.

ISSN: 2233-7857 IJFGCN

3.4. Image Encryption using chaos technique:

Guoqiang Han and Guosheng Gu [18][21] proposed for image encryption using arrangement and replacement methods. They have made a highly optimized to enhance a cross sampling disposal is used in image encrypted.

3.5. Encrypt the color images by using random of double phase encoding:

Muhammad Abdul Karim and Shikun Zhang [19] [21] have a solution to encryption the color image using the optical image coding system of grayscale, where the color image will be converted and formatted into an indexed image before encoding it in two random stages, the first stage is based on the input level and the other stage On a Fourier level. To decrypt the color image, convert the indexed image to RGB (blue, green, red) color format. Therefore, the methods for encrypted a monochrome channel are more powerful and smaller than encrypted the image to multicolored and channels.

3.6. Image Encryption Using Genetic Algorithm:

Abdul Hanan and Rasul Enayatifar [20][21] proposed the method based composed of a chaotic function image and genetic algorithm. So, the first technically calculate the numbers of image encrypted by chaotic function. Then, the first start of the operation the genetic algorithm, one of its priorities is to encrypt the image. Therefore, to optimize the encrypted and used images, this is the best solution for cipher images that are chosen as the best-encrypted image.

3.7. Algorithm for encryption images by using Elliptic Curve Public Cryptosystem:

Xiaoqiang Zhang and Xuesong wang [22] proposed to encrypt the digital image-based algorithm (Elliptic Curve Public) ECC. It depends on the encoded key transmission and management comparatively simply. The result and analyzes of the algorithm are secure to resist the known plaintext, the differential attack, and the brute force attack. this proposal is the fastest that depends on the encryption speed.

4.0 MATHEMATICAL REVIEW

There some mathematical formulas will use to encryption\decryption the images by using the Elliptic Curve Cryptography technique [2].

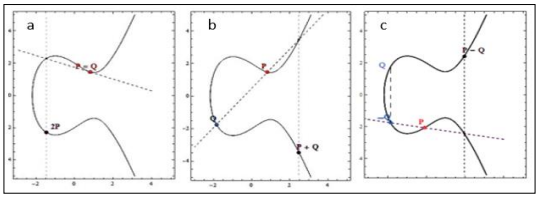


Figure 1. a) doubling Point b) addition Point c) subtraction Point [2]

4.1 Addition Point

The mathematical operations are performed to coordinate the points algorithm using elliptic curve cryptography (ECC). The calculation will be the distinction between addition points present in the elliptic curve as shown above in the figure (1.a) [2].

$$P(x_1,y_1) + Q(x_2,y_2) = R(x_3,y_3)$$

$$x_3 = (\lambda^2 - x_1 - x_2) \bmod P$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \bmod P$$

$$\text{Where } \lambda = (y2-y1) / (x2-x1) \bmod P$$

ISSN: 2233-7857 IJFGCN

4.2 Subtraction Point

To the procedure of the subtraction point, get the result of the point subtracted on the coordinate x-axis, and add that additional point on the resulting coordinate, as shown above in the figure (1.b) [2].

$$P(x_1,y_1)\text{-}Q(x_2,y_2) = P(x_1,y_1)\text{-}Q(x_2,\text{-}y_2)$$

4.3 Doubling Point

To perform the doubling point to add the same value of the two points in the curve, as shown above in the figure (1.c) [2].

$$P(x_1,y_1) + Q(x_1,y_1) = R(x_3,y_3)$$

$$x_3 = (\lambda^2\text{-}2x_1) \bmod P$$

$$y_3 = (\lambda(x_1\text{-}x_3) - y_1) \bmod P$$

$$\text{Where } \lambda = (3x^{\frac{2}{1}} + a) / (2y_1) \bmod P$$

4.4 Multiplication Point

Multiplication is meaning a repeat the point addition bases the coordinate. It has available many algorithms for developing point multiplication [2].

4.5 Encryption and decryption using ECC

To allow the USER A and USER B to be two communicating parties. And that communicating will agree over the curve and generate the formula as below shown [2].

$$y^2 = \{ x^3 + ax + b\} \bmod [P]$$

FromDigits = [list of pixels, b]

5.0 IMAGE ENCRYPTION REQUIREMENTS

The image encryption requirements depend on when plan designing algorithm cryptography. They include codec compliance, compression efficiency, security level, and encryption efficiency, which will discuss one by one [23].

5.1. Codec Compliance:

Some multimedia applications use codec software to procedure decompression and compression file. Therefore, the encryption algorithm does not require modifications to the codec [23].

5.2. Compression efficiency:

This is a challenge for the user by managing storage so that the rate of data flow in the wide range of the network is available. Therefore, the proposed algorithms for encrypted images must not exceed their size in storage or sent, as three processes help to maintain compression efficiency, as shown below in figure 2 [23].

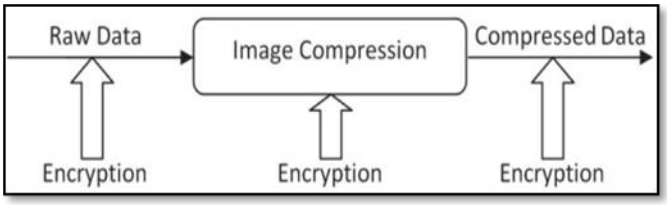


Figure 2, Process of Image Compression and Encryption [23]

ISSN: 2233-7857 IJFGCN

5.3. Security Level:

The security level which requires secure multimedia of applications, such as a stream video request less level of security than other sensitive multimedia from entertainment applications like video call conference [23].

5.4. Encryption Efficiency:

Even the images compressed, it has a big amount of data. So, to apply the images algorithm as a normal way to encrypt the images not enough because of these algorithms are CPU-intensive and designed exactly to encrypt as text data. Therefore, use a specific algorithm to verified, encrypt, and decrypt the images [23].

6.0 ELLIPTIC CURVE CRYPTOGRAPHY (ECC) OPERATIONS

6.1 Collect a group of a pixel inside a single integer:

Images have the list of pixels. If cryptography operation of image happens on a single pixel. So, the cryptography operation is taking more time, because of the number of pixels which available is very large. These problems should be well addressed, such as grouping pixels into one group. However, the number of pixels collected to one group must depend on the parameters of the elliptic curve used. If the available parameters are large for the curve, where the pixels are collected for the image. For example, If the parameter of ECC has 512 bits, it can be grouped 63 pixels in one group. To get the list of multi pixels, that means if 256 digits in the integer (p-1) will convert to a group of the pixel into a single interface, and require mathematical functions as follow,

However, it will take a list of pixels and convert them to the base "b". Then, add the random key to each pixel that avoids happening any error when using a function of mathematically [24].

6.2 Pixels grouping from a big integer:

The pixel value of coordinate will be in the range of bit size which was selected for ECC process. To generate the cipher images, require to bring the image down into the range (0 - 255) of the ECC coordinates, and use the mathematical functions to the Integer Digits [big integer value, 256]. So, insert the value of integer which bigger that chosen the base value will be 256. Then, the output of the function will be valued around between in the range (0-255). Finally, the functions on each which inverse of each other.

FromDigits [ ] and IntegerDigits [ ]

So, the value of pixels is conserved during the ECC procedure. The procedure to encryption the image depends on defining the value of pixel for the image as the first action to the encryption process. The parameters of the elliptic curve cryptography and which agree to distributions between the sender and receiver, it is {G, a, p, b, n}. So, the sender will encrypt the pixel of the plain image to the cipher image is called the public key 'Pb'. but the receiver will decrypt the cipher image and return it to the plain image which called the private key 'nB' [24].

6.3 The image encryption algorithm:

6.3.1. The first select the binary of image (MxN) for input (x).

6.3.2. Each the pixel of the image, which called is a message (m) and will coordinate on each axis as follow (Xm, Ym) that provide the formula of the elliptic curve as follows:

x_m = m x k + J, So, J= 0,1, 2.....

$y_m = \sqrt{x^3 + ax + b}$

ISSN: 2233-7857 IJFGCN

Where ‘k’ is the key of random positive integer, ‘m’ is a message. So, the (Xm, Ym) is modulo for ‘P’, where ‘P’ is the prime number, and should the prime number less than or equal value of (k and m) (P>= (Kxm)) [24].

6.3.3. To encryption of the images want a point on the level ‘G’ and a group of elliptic Ep (a, b). So, User A selects private key ’nA’ to generate a public key ‘nA G’. To encrypt a message and send ‘m’ to User B, User A choose ‘k’ as a random positive integer and produce the cipher image on the following formula, where ‘Pm’ is the public key for User B.

$$C_m = \{kG, P_m + kP_B\}$$

The chart below in figure (3), that explains the encrypted images module using the elliptic curve (ECC) [24].

6.3.4. To decrypt of the images using the method as follow;

$$\{Pm + kP_B - n_B(kG) = Pm + k(n_B G) - n_B(kG)\} = Pm$$

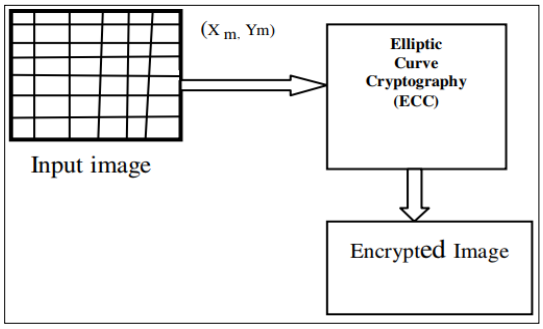


Figure 3, Encryption Image Flow chart [24]

6.4 Simulation and Results:

In the below table the example of points represents elliptic curve ‘E31(1,5)’ as follow:

Table 1, Elliptic Curve E31(1,5) [24]

(0, 6)	(6,14)	(12, 3)	(15, 4)	(21,7)
(0,25)	(6,17)	(12,28)	(15,27)	(21,24)
(1,10)	(7,13)	(13,13)	(16,5)	(25,0)
(1,21)	(7,18)	(13,18)	(16,26)	
(3, 2)	(11,13)	(14, 2)	(19,30)	
(3,29)	(11,18)	(14,29)	(19, 1)	

The guessing Key K = 121, which is resultant from ECC = 2 x (12,3) = 5 x (12,28) = (1,21). To transformation the pixel of image ‘X’ (Xm, Ym) that points of an elliptic curve and then encrypted. Shown below in figure (4), the decrypted image by randomly guessing of the key which equal (123) instead of the correct key (121). So, the original image will be returned back if chosen the correct guessing key [24].

7.0 THE TECHNIQUES OF SECURITY ANALYSIS:

The techniques for security analysis of the cryptography operations is one primary procedure to verify the asset of the cryptographic techniques. So, this part will explain the best technique of analyses [2][25].

ISSN: 2233-7857 IJFGCN

7.1 Analysis of Histogram technique:

The analysis of histogram technique depicts the frequency of each pixel of the image. A perfect cipher image has a frequency distribution of the value of the pixel. The distribution of the pixel in the plain image different than compared with the histogram of the cipher image that distributed equally and got the better of the cipher image, as shown below in the figure (5-6) shown the histogram cipher image and plain image [2][25].

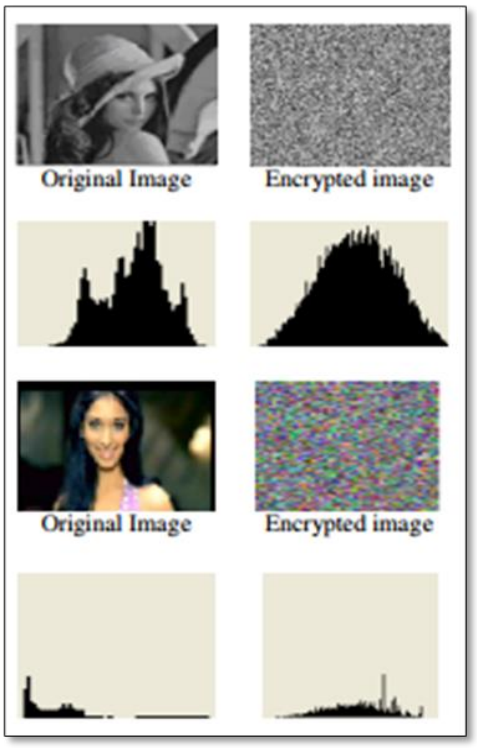


Figure 4, image encryption [24]

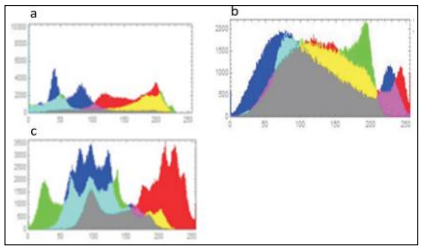
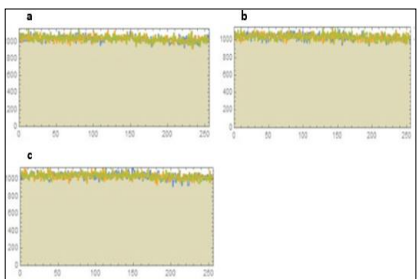


Figure 5, a) Hist of peppers; b) Hist of mandrill;
c) Hist of Lena. [2][25]



ISSN: 2233-7857 IJFGCN

Figure 6, a) Hist of encrypt Lena; b) Hist of encrypt mandrill;
c) Hist of encrypt peppers. [2][25]

7.2 A space of key:

Usually, the security of decryption and encryption depends on the size of the key used. If the key size is bigger, it will be difficult to attack by using a brute force attack. Then, the elliptic curve cryptographic will provide a difficultly Discrete Logarithmic Problem relate to the size of the key [2][25].

7.3 A Sensitivity of key:

The change of the original key should be to change the recovered image from the cipher image. As shown below in figure (7) show the recovered copy of the image using the right key of the receiver and compared with the wrong key which is different from the original key [2][25].

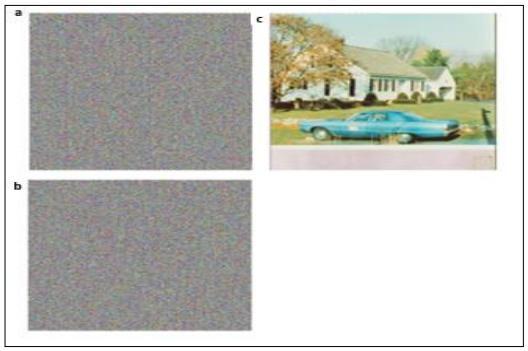


Figure 7, (a) encrypted image of home; (b) Decrypted with wrong key;
(c) Decrypted image with correct key. [2][25]

7.4 Analysis for Entropy Technique:

The entropy technique is a scale of the degree of randomly encryption image. That means the value of pixel for the encrypted image requires to be vastly random. So, a perfect cipher image who has an entropy value with near value = '8', as shown below the table (2) shows the example different values of entropy for the cipher image such as Mandrill, Pepper, and Lena image [2][25].

Cipher Image	Size	Entropy
Mandrill	256*260	7.99884
Pepper	512*520	7.99963
Lena	1024*1040	7.99986

Table 2, Entropy Analysis [2][25]

ISSN: 2233-7857 IJFGCN

7.5 Analysis of Speed:

The encryption and decryption of images depend on the execution time applied to the different algorithms and the size of the images. Even hardware quality and programming skills play important to get the best quality of required. As shown below table (3), shown using the parameters for digital signature verification, encryption, decryption, and digital signature in time execution analysis between images as (Lena, Mandrill, and Peppers) [2][25].

Table 3, Speed Analysis [2][25]

Image	Size	Encryption Time	Decryption Time	Digital Signature	Digital Sign Verification
Lena	1024*1024	2.47 sec	1.58 sec	4.37 sec	4.38 sec
Mandrill	512*512	0.79 sec	0.60 sec	1.39 sec	1.37 sec
Peppers	256*256	0.29 sec	0.30 sec	0.48 sec	0.44 sec

8.0 CONCLUSION

In the digital world today, the security of images is important and becomes more important since when they come to communication is on the world network, and flexibility delivers to the users on each application. In this paper, I surveyed and study the most used encryption and decryption techniques for images. And it can provide the security function and verified the encrypted image before sending it over the internet. Additionally, choose some algorithm of elliptic curve cryptosystem (ECC) that will save the images encrypted and prevent anyone to attack it when transferring it on the open network.

Also, I presented and implement the ethical way for encryption and decryption steps for the cipher image to guarantee the authenticity and integrity of the received image. Additionally, it explained in this paper to define the pixel values, grouping pixel, and change mathematical function which will impact the elliptic curve cryptographic (ECC). Finally, I presented summary types of security analysis tools that will help the cipher image to ensure the strength of encrypted when transferring it over the internet nowadays, to prevent any attack attacking the image to get the information available.

9.0 REFERENCES

[1] Gupta, K., & Silakari, S. (2010, November). Performance Analysis for image Encryption using ECC. In 2010 International Conference on Computational Intelligence and Communication Networks (pp. 79-82). IEEE.

[2] Singh, L. D., & Singh, K. M. (2015). Image encryption using elliptic curve cryptography. Procedia Computer Science, 54, 472-481.

[3] Britto, J., & Roja, M. M. (2017, December). Gaussian noise analysis in elliptic curve encrypted images. In 2017 International Conference on Intelligent Sustainable Systems (ICISS) (pp. 791-794). IEEE.

[4] Blake, I., Seroussi, G., Seroussi, G., & Smart, N. (1999). Elliptic curves in cryptography (Vol. 265). Cambridge university press.

[5] Hankerson, D., Menezes, A. J., & Vanstone, S. (2006). Guide to elliptic curve cryptography. Springer Science & Business Media.

[6] Teeriaho, J. (2011). Cyclic group cryptography with Elliptic Curves. Brasov, May.

[7] El-Latif, A. A. A., & Niu, X. (2013). A hybrid chaotic system and cyclic elliptic curve for image encryption. AEU-International Journal of Electronics and Communications, 67(2), 136-143.

[8] Liu, H., & Liu, Y. (2014). Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve. Optics & Laser Technology, 56, 15-19.

ISSN: 2233-7857 IJFGCN

[9] Vigila, S. M. C., & Muneeswaran, K. (2012). Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications. IJ Network Security, 14(4), 236-242.

[10] Behnia, S., Akhavan, A., Akhshani, A., & Samsudin, A. (2013). Image encryption based on the Jacobian elliptic maps. Journal of Systems and Software, 86(9), 2429-2438.

[11] Li, L., El-Latif, A. A. A., & Niu, X. (2012). Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images. Signal Processing, 92(4), 1069-1078.

[12] Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). International journal of information security, 1(1), 36-63.

[13] Tawalbeh, L. A., Mowafi, M., & Aljoby, W. (2013). Use of elliptic curve cryptography for multimedia encryption. IET Information Security, 7(2), 67-74.

[14] Lochter, D. M. (2005). ECC brainpool standard curves and curve generation v. 1.0.

[15] Sinha, A., & Singh, K. (2003). A technique for image encryption using digital signature. Optics communications, 218(4-6), 229-234.

[16] Shin, C. M., Seo, D. H., Cho, K. B., Lee, H. W., & Kim, S. J. (2003, December). Multilevel image encryption by binary phase XOR operations. In CLEO/Pacific Rim 2003. The 5th Pacific Rim Conference on Lasers and Electro-Optics (IEEE Cat. No. 03TH8671) (Vol. 2, pp. 426-vol). IEEE.

[17] Belkhouche, F., & Qidwai, U. (2003, April). Binary image encoding using 1D chaotic maps. In Annual Technical Conference IEEE Region 5, 2003 (pp. 39-43). IEEE.

[18] Xiao, H. P., & Zhang, G. J. (2006, August). An image encryption scheme based on chaotic systems. In 2006 International Conference on Machine Learning and Cybernetics (pp. 2707-2711). IEEE.

[19] Zhang, S., & Karim, M. A. (1999). Color image encryption using double random phase encoding. Microwave and optical technology letters, 21(5), 318-323.

[20] Enayatifar, R., & Abdullah, A. H. (2011). Image security via genetic algorithm. In International Conference on Computer and Software Modeling (Vol. 14, pp. 198-203).

[21] Pakshwar, R., Trivedi, V. K., & Richhariya, V. (2013). A survey on different image encryption and decryption techniques. International journal of computer science and information technologies, 4(1), 113-116.

[22] Zhang, X., & Wang, X. (2018). Digital image encryption algorithm based on elliptic curve public cryptosystem. IEEE Access, 6, 70025-70034.

[23] Bakhtiari, S., Ibrahim, S., Salleh, M., & Bakhtiari, M. (2014, August). JPEG mage encryption with Elliptic Curve Cryptography. In 2014 International Symposium on Biometrics and Security Technologies (ISBAST) (pp. 144-149). IEEE.

[24] Gupta, K., Silakari, S., Gupta, R., & Khan, S. A. (2009, July). An ethical way of image encryption using ECC. In 2009 First International Conference on Computational Intelligence, Communication Systems and Networks (pp. 342-345). IEEE.

[25] Abdelfatah, R. I. (2019). Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography. IEEE Access.

[26] Luo, Y., Ouyang, X., Liu, J., & Cao, L. (2019). An image encryption method based on elliptic curve elgamal encryption and chaotic systems. IEEE Access, 7, 38507-38522.

[27] Patel, K. D., & Belani, S. (2011). Image encryption using different techniques: A review. International Journal of Emerging Technology and Advanced Engineering, 1(1), 30-34.

ISSN: 2233-7857 IJFGCN