ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 9 , September 2016

An Inventive Image Security System Based on Massey-Omura Encryption with Group

R.Sivakumar, Dr.K.Thamodaran,

MPhil Research Scholar, Dept. of Computer Science, Marudupandiyar College,

Thanjavur, Tamilnadu, India.

Professor, Dept. of Computer Science, Marudupandiyar College, Thanjavur, Tamilnadu, India.

ABSTRACT: The development of social network and other communication facilities become more advanced as well as security is important in present day communication. Cryptography is a system of storing and transmitting data in a secured form so that only intended user can read and process it. In this paper, an image security system is proposed that provides secured authentication to integrate the image encryption with Elliptic Curve Cryptography and Group concept to provide security. The original image matrix is encrypted with the help of a key sequence which is generated from the elliptic Curve. After performing the decryption process the original image is acquired. The PSNR and IQIM are used to measure the image quality distortion. The correlation coefficients (BCR), key sensitivity analysis, Statistical analysis are used to measure the efficiency of the proposed image security system. The experimental results are offered to exhibit the competence of the proposed system.

KEYWORDS: BCR, Elliptic Curve, Image Encryption, IQIM, PSNR.

I. INTRODUCTION

Image processing[11] is processing of images using mathematical operations by using any form of signal processing for which the input is an image, a series of images, or a video, such as a photograph or video frame; the output of image processing may be either an image or a set of characteristics or parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal processing techniques to it. Images are also processed as three-dimensional signals where the third-dimension being time or the z-axis. Information is a precious resource to individual, organization, government, military and everyone. The security of information is become unavoidable due to fast development and applications of computer networks and internet technology. Security[2],[3] consists of some policies, rules, protocols and standards that help the society or organization to meet the goals. Random number are playing significant role in strengthen the cryptographic primitives and it is represented by cryptographic keys to secure the valuable information. Public key cryptography does not have an extensive a history as symmetric key encryption, being discovered only in the mid 1970s.

Cryptosystems [5] can be classified into two categories namely symmetric key cryptosystem and asymmetric key cryptosystem. In symmetric key cryptosystems, the same key is used for both Encryption as well as decryption. Asymmetric or Public key or shared key cryptosystems use two different keys. One is asymmetric or public-key and another one is private key. The private key is kept by the receiver. The public key is announced to the public. One is used for encryption while the other key is used for decryption. The two keys can be used interchangeably. Symmetric cryptosystem is classified into block cipher and stream cipher. Stream cipher encrypts one bit of plaintext at a time. Block Cipher that encrypts plaintext at once as a group rather than one bit at a time. Stream Cipher executes faster compared to block cipher. Most of the encryption uses Stream Cipher. The figure1 shows the concept of asymmetric key cryptography system.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 9 , September 2016

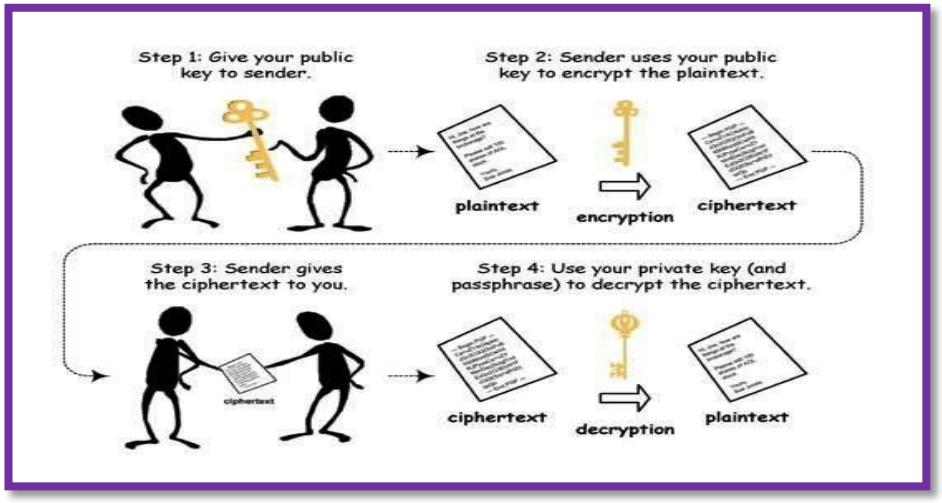


Fig. 1. : Asymmetric key Cryptography

Kuo.C and M. Chen[1] have stated that the task of image encryption system has enlarged the requirement to restrict the illegitimate access of image contents. Scrambling or encryption techniques are used as traditional systems for visual confidentiality. In spatial domain, simple permutation or affine transformation is used for making the contents unintelligent. These techniques have high outstanding intelligibility and hence these low cost scrambling methods become defenseless to attacks with the development of computer and communication media. Philip P. Dang and Paul M. Chau [4] have suggested the image encryption scheme for secure internet multimedia application via the VEA and polynomial inversable function defined on GF (2^m). Feng Huang et al.[6] have recommended the symmetric image encryption method using simple two-dimensional map. The proposed method makes use of image stretch-and-fold and a simple diffusion mechanism. Richard Winton[7] has recommended that Massey-Omura encryption algorithm along with two enrichments offered to improve security. The enhanced Massey-Omura system (EMO-1) replaces the prime modulus with a composite which is the product of two distinct (large) primes. In this manner the system is provided with a level of security similar to that of an RSA public key system. A stronger version of the enhanced Massey-Omura system (EMO-2) adds a digital signature to the EMO-1 system. The digital signature allows the recipient of a message encrypted with EMO-2 protocol to authenticate the identity of the sender, providing an additional aspect of security.

K.Ganesan et al.[8] have tendered an image encryption method using public key system and Chebyshev chaos map to encrypt color images and videos in real time applications. The security method has been enhanced using a non-XORing hash function to secure it against chosen plaintext attack. Q.Gong-bin et al.[9] intended an image encryption scheme using combination of DES and chaotic map to improve the security and expand the key space. This scheme yields better security and anti-attack ability effectively. M.Ahmad et al.[10] have represented an image encryption scheme using three different chaotic maps. The 2D cat map is used to perform shuffling of pixels on blocks, 2D coupled logistic map is used to generate control parameters and 1D logistic map is used to perform encryption on shuffled image. Muneeswaran.K [12] has been offered the simple and strong encryption system for image security. Boolean operations XOR and Rotating system make a satisfactory diffusion and confusion in the bits of the pixels of the image. Furthermore the strong came from the ability of the cryptosystem to use a large number of bits in the secret key.

S.V.Sathyanarayana et.al. [13] have enlighten the properties of finite fields and elliptic curves in the design of a stream cipher system. Additive and Affine encryption key sequences obtained from random elliptic curve points using six schemes are designed and investigated. The encrypted images obtained for the input image and the corresponding histograms are discussed. The histograms are almost flat offering good security for images. The Entropy and the correlation coefficient of the input and encrypted images are computed and analyzed. Vinod Kumar Yadav et. al. [14] have offered the cryptocraphic scheme using Elliptic Curve Cryptography with generator ‘g’ for Image Encryption. ECC is an competent system of transmitting the image securely. It has been shown though the image encryption by ECC to transmits the image secretly and efficiently recovers the same at the receiver end. The scheme comprises of the important algorithms namely encryption algorithm is used to create every 2-D image pixels of the original image into

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 9 , September 2016

the ECC points in a finite abelian group over GF(2^m). Srinivasan Nagaraj and G. S. V. P. Raju[15] have suggested that scrambling method only is insufficient to devise the secure transmission of multimedia contents over internet. It is required to strengthen the secure transmission through some encryption techniques to make it robust against various attacks over communication. As a result Elliptic Curve Cryptography for image data is developed to meet the current security needs.

The rest of this paper is organized as follows. Section II provides the information about Elliptic Curve Cryptography and Group Theory. Section III offers the proposed image security system using Massey-Omura encryption with group. The formulae for measure of performance like PSNR, IQIM and BCR are given in section IV. The experimental results and security analysis are presented in Section V and Section VI concludes this paper.

II. ELLIPTIC CURVE CRYPTOGRAPHY AND GROUP THEORY

Encryption[2],[3] is the process of encoding a message so that its meaning is not understandable; decryption is the reverse process, transforming an encrypted message back into its normal or original form. ECC is an asymmetric cryptography algorithm which involves some high level calculation using mathematical curves to encrypt and decrypt data. Elliptic curves are algebraic curves which have been studied by many mathematicians for a long time. In 1985, Neal Koblitz and Victor Miller independently proposed the public key cryptosystems using elliptic curve. The ECC is a realistic, secured technology to be implemented in constrained applications. Generating curves to work as cryptographic curves must go through numerous algorithms and procedures so as to create a reliable cryptographic curve. The feature of ECC which include the benefits of higher-strength per-bit higher speeds with lower power consumption and bandwidth savings and storage efficiencies.

Abstract algebraic system is called a group. Group theory is well-developed branch of abstract algebra. Group theory is applied not only in mathematics also in various branches of the physical sciences and in computer science especially in Cryptography. Camille Jorden (1838 – 1922) submited J.A. Serret's work and he showed group theory had evolved in to an explicit mathematical construct. He defined a group "to be a system of permutation of a finite set with the condition that the product (Composition) of any two permutations of the system is also a permutation". H. Weber's notion of a group has four axioms, but it turns out that one of his axioms is unnecessary when compared to the modern definition. The modern definition of a group is as follows:

An algebraic structure is a set which is equipped with one or more binary operations. The simplest important structure is called a *group* which has one operation satisfying certain rules, or axioms. A non - empty set G together with the binary operation✸, that is (G,✸) is called *group* [2] if ✸ satisfies the following conditions.

(i) Closure : For every a, b ε G, a ✸ b ε G.

(ii) Associative: For every a,b,c ε G, a✸(b✸c) = (a✸b)✸ c

(iii) Identity : There exists and element e ε G called the identity element such that a ✸ e = e✸a = a for all a ε G

(iv) Inverse : There exists and elements a^{-1} ε to G called the inverse of 'a' such that a ✸ a^{-1} = a^{-1} ✸a for each a ε G.

A group (G, ✸) is said to be an *abelion group* if a ✸ b = b ✸a for all a, b ε G. (commutative group) [16].

Elliptic curve cryptosystems are used to implementing discrete logarithm methods. An elliptic curve is basically a set of points that satisfy the equation $y^2 = x^3 + ax + b$. When considered in finite field of characteristic p (where p must be larger than 3). A slightly different equation is needed for the case of small characteristic, $p = 2$ and $p = 3$. The points on elliptic curves can be added together and they form a structure called a *group* or *abelian group*. This is just a way of saying that you can do arithmetic with them as you can do with integers when using just addition and subtraction. With regard to cryptography, elliptic curves have many theoretical benefits but they also are also very practical.

III. PROPOSED IMAGE SECURITY SYSTEM USING MASSEY-OMURA ENCRYPTION WITH GROUP

In this proposed image encryption system image coefficients are encrypted through Massey-Omura encryption with group. The image coefficients are encrypted by means of EX-OR operation with a secret key. The keys are generated through Elliptic curve points for encryption and decryption processes The encryption method is used to increase the robustness of the proposed encryption scheme. The given image is divided in to number of blocks. Divide the width

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 9 , September 2016

and height of image by width and height of block size 4096 bits (M x N=64 x 64). In this scheme the image size is (512 x 512). So that ((512 x 512 pixels) / (64 x 64 pixels))= 64 blocks. The proposed mechanism is devised with Massey-Omura public key cryptographic algorithm with group. Elliptical curve concept is employed to generate the points. These points are fulfilling the properties of group. The Peak Signal-to-Noise Ratio(PSNR), Image Quality Index Metric (IQIM) based on three factors such as loss of correlation, luminance distortion, and contrast distortion are utilized to assess the image quality distortion and correlation coefficient(BCR) is utilized to assess the correlation among the image pixels.

A. GENERATION OF AN ELLIPTIC CURVE POINTS

The proposed image encryption is based on synchronous cipher using Elliptic curve as a part is discussed. The points on GF(P) over an Elliptic curve is taken with an equation (1).

$$y^2 = (x^3+ax+b) \bmod P \quad (1)$$

by choosing appropriate parameters, a and b, where P is a prime number. The key for the encryption algorithm is generated using the index point. An elliptic group over the Galois Field Ep(a, b) is obtained by computing $x^3 + ax + b \bmod p$ for $0 \le x < p$. The constants a and b are non negative integers smaller than the prime number p and must satisfy the condition.For each value of x, one needs to determine whether or not in it a quadratic residue. If it is the case, then there are two values in the elliptic group. If not, then the point is not in the elliptic group Ep(a, b). Elliptic curve points are generated for encryption and decryption processes. The procedure is as follows:

$$4a^3 + 27b^2 \bmod p \neq 0 \quad (2)$$

Let the prime number p = 23 and let the constants a = 1 and b = 1 as well. Initially, verify that

$4a^3 + 27b^2 \bmod p = 4\times 1^3 + 27\times 1^2 \bmod 23$

$4a^3 + 27b^2 \bmod p = 4+27 \bmod 23 = 31 \bmod 23$

$4a^3 + 27b^2 \bmod p = 8 \neq 0.$

Find out the quadratic residues Q_{23} from the reduced set of residues $Z_{23} = \{1, 2, 3,...,21, 22\}$:

Table 1.: Construction of $(x^2 \bmod P)$ and $(p-x)^2 \bmod P$.

S.No.	$(x^2 \bmod P)$	$(p-x)^2 \bmod P.$	=
1	$1^2 \bmod 23$	$22^2 \bmod 23$	1
2	$2^2 \bmod 23$	$21^2 \bmod 23$	4
3	$3^2 \bmod 23$	$20^2 \bmod 23$	9
4	$4^2 \bmod 23$	$19^2 \bmod 23$	16
5	$5^2 \bmod 23$	$18^2 \bmod 23$	2
6	$6^2 \bmod 23$	$17^2 \bmod 23$	13
7	$7^2 \bmod 23$	$16^2 \bmod 23$	3
8	$8^2 \bmod 23$	$15^2 \bmod 23$	18
9	$9^2 \bmod 23$	$14^2 \bmod 23$	12
10	$10^2 \bmod 23$	$13^2 \bmod 23$	8
11	$11^2 \bmod 23$	$12^2 \bmod 23$	6

Therefore the set of (p-1) / 2 = 11 quadratic residues $Q_{23} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16,18\}$. For $0 = x < p$, calculate $y^2 = (x^3 + x + 1) \bmod 23$ and determine if y^2 is in the set of quadratic residues Q_{23} :

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 9 , September 2016

Table 2. : Construction of $y^2 = (x^3+x+1) \bmod 23$

x.	y^2	$y^2 \in Q_{23}$	y_1	y_2	x.	y^2	$y^2 \in Q_{23}$	y_1	y_2
0	1	Yes	1	22	12	16	Yes	4	19
1	3	Yes	7	16	13	3	Yes	7	16
2	11	No	-	-	14	22	No	-	-
3	8	Yes	10	13	15	10	No	-	-
4	0	No	0	0	16	19	No	-	-
5	16	Yes	4	19	17	9	Yes	3	20
6	16	Yes	4	19	18	9	Yes	3	20
7	6	Yes	11	12	19	2	Yes	5	18
8	15	No	-	-	20	17	No	-	-
9	3	Yes	7	16	21	14	No	-	-
10	22	No	-	-	22	22	No	-	-
11	9	Yes	3	20					

The elliptic group Ep (a,b)=E_{23}(1,1) thus include the points (including also the additional single point (4,0)):

E_{23}(1,1) = { (0,1), (0,22), (1,7), (1,16), (3,10), (3,13), (4,0), (5,4), (5,19), (6,4), (6,19), (7,11), (7,12), (9,7), (9,16), (11,3), (11,20), (12,4), (12,19), (13,7), (13,16), (17,3), (17,20), (18,3),(18,20),19,5), (19,18) }.

In this proposed method Massey-Omura public key cryptographic algorithm is used for image encryption and decryption process based on with group. The following Figure 2.shows the scatter plot of elliptic group Ep (a, b) =E_{23}(1,1).

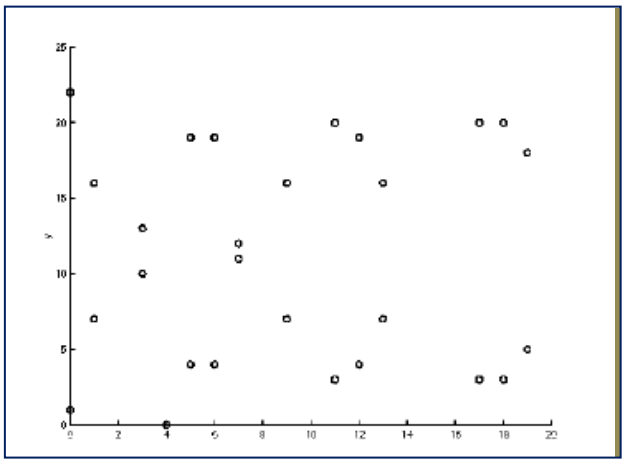


FIG.2 : SCATTERPLOT OF ELLIPTIC GROUP EP (A, B)=E_{23}(1, 1)

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 9 , September 2016

B.KEY GENERATION PROCEDURE

Step 1. Acquire the domain Parameters of ECC, D = (m, *G*, *a*, *b*, x).
Step 2. Plot the chosen Elliptic curve.
Step 3. Attain key pair by means of ECC domain parameters.
Step 4. Encrypt the Image through the keys generated.

C.KEY EXCHANGE PROCEDURE

Step 1. Sender sends his public key to the Receiver and keeps his private key as secret.
Step 2. Receiver sends its public key to Sender and keeps its private key as secret.
Step 3. Sender finds the Key by means of Sender's private key and receiver's public key.
Step 4. Receiver calculates its Key by means of Sender's private key and Sender's public key.
Step 5. At first Sender sends the Image by way of the key calculated at Sender side.
Step 6. Receiver verifies the Key sent by the Sender with the key calculated at Receiver side.
Step 7. If both the keys are matched, Receiver can decrypt the Image with the key pair generated.

D.ENCRYPTION PROCEDURE

Alice wishes to send a message to Bob. They do not need to have a private or public key. The message is encoded as an element m ε G. This protocol is sometimes described as the 'you - to - me' and 'me – to- you' method. It requires Alice and Bob to carry out a conversation rather than just a single transmission of encrypted message.

Step 1. Alice computes a random integer, x_A, coprime to #G, and sends Bob the element
$a = m^x A$.
Step 2. Bob computes a random integer, x_B, co-prime to #G, and sends back to Alice the element
$b = a^x{}_B = m^x A^x{}_B$.
Step 3. Alice can compute x_A^{-1} (mod #G) and so sends back to Bob the element
$a^1 = b^{x-1}{}_A = m^X A^X B^{X-1}{}_A = m^X B$.

E.DECRYPTION PROCEDURE

STEP 1. Verify the generated key pair.
STEP 2. Finally Bob computes $x^{-1}B$ (mod #G) and can decrypt the message as
$(a^1)\, x^{-1}B = m^{xBx-1}B = m$.

IV. Measures of Performance

The performance of the proposed encryption system is determined through Peak Signal-to-Noise Ratio (PSNR), Image Quality Index Metric (IQIM), Correlation Coefficient (BCR) which are illustrated as follows:

A. PEAK SIGNAL-TO-NOISE RATIO (PSNR)

The quality of encrypted image is quantified by means of peak signal-to-noise ratio (PSNR) as mentioned in equation (3).

$$PSNR = 10\log_{10}\left[\frac{MAX^2}{MSE}\right] \quad \text{where} \quad MSE = \left[\frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[X(i,j) - X'(i,j)]^2\right] \qquad (3)$$

where MSE indicates mean square error, X and X' are the original and the partially encrypted images respectively with image size of $M \times N$. The smaller values of PSNR provide good results in encrypted images.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 9 , September 2016

B. IMAGE QUALITY INDEX METRIC (IQIM)

The image quality distortion is evaluated with help of universal image quality index (IQIM), which is mathematically defined and suggested by Zhou Wang, Alan. C. Bovik. The image quality distortion is assessed by the equation (4) based on the three characteristics such as loss of correlation, luminance distortion, and contrast distortion. If two images *f* and *g* are considered as a matrices with *M* column and *N* rows containing pixel values *f*[*i,j*], *g*[*i,j*], respectively ($0 \geq i > M$, $0 \geq j > N$), the universal image quality index *Q* may be appraised as a product of three components:

$$Q = \frac{\sigma_{fg}}{\sigma_f \sigma_g} * \frac{2\bar{f}\bar{g}}{(\bar{f})^2 + (\bar{g})^2} * \frac{2\sigma_f \sigma_g}{\sigma_f^2 + \sigma_g^2} \tag{4}$$

where $\bar{f} = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} f[i,j], \qquad \bar{g} = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} g[i,j]$

$$\sigma fg = \frac{1}{M+N+1} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (f[i,j] - \bar{f}) * (g[i,j] - \bar{g})$$

$$\sigma_f^2 = \frac{1}{M+N-1} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (f[i,j] - \bar{f})^2, \quad \sigma_g^2 = \frac{1}{M+N-1} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (g[i,j] - \bar{g})^2$$

The first component is the correlation coefficient, which appraises the degree of linear correlation between images *f* and *g*. It varies in the range [-1, 1]. The best value 1 is attained when *f* and *g* are linearly related, which means that *g*[*i,j*] = *a***f*[*i,j*]+*b* for all possible values of *i* and *j*. The second component, with a value range of [0, 1], appraises how close the mean luminance is between images. Since σ_f and σ_g can be considered as estimates of the contrast of *f* and *g*, the third component appraises how similar the contrasts of the images are. The value range for this component is also [0, 1]. The range of values for the index *Q* is [-1, 1]. The best value 1 is attained if and only if the images are identical. Quality Index appraises the universal image quality index.

C. CORRELATION COEFFICIENT (BCR)

The correlation value among the neighbouring pixels in encrypted image is evaluated through equation (5).

$$r_{xy} = \frac{COV(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad \text{where} \qquad E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i \quad ,$$

$$D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2 \qquad COV(x,y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \tag{5}$$

Where $E(x)$ is the assessment of mathematical expectations of *x*, $D(x)$ is the assessment of variance of *x* and cov(*x*, *y*) is the assessment of covariance between *x* and *y*, where x and *y* are grey-scale values of two adjacent pixels in the image.

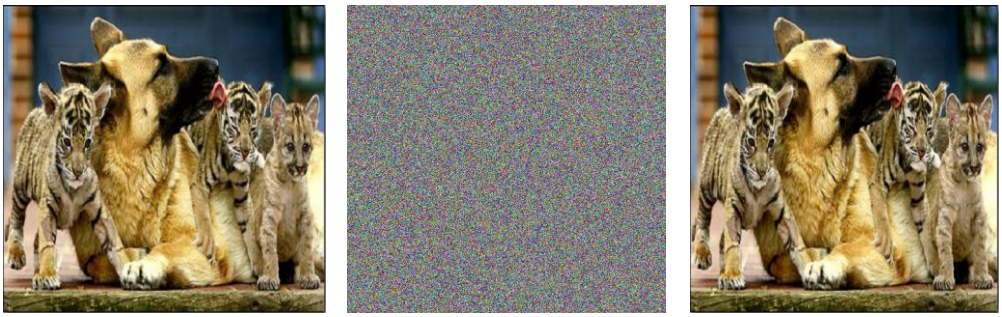
V. EXPERIMENTAL RESULTS AND DISCUSSION

This suggested image security system based on Massey-Omura encryption with group is designed through Elliptic Curve Cryptography. The points on elliptic curves can be added together and they form a group structure. In secret key cryptographic algorithm, the sender uses a key to encrypt plain image, and then sends the encrypted image to the receiver. The receiver applies the same key to decrypt the encrypted image and recovers the original image. In public key cryptography, one of the keys is the public key, and the other key is the private key. To send a message, the sender uses the receiver's public key to encrypt information and the receiver uses his or her private key to decrypt the encrypted image. Experiments are conducted with more than 50 dissimilar images and sample results are offered in this section. The test images are of size (512 x 512) with pixel values in the range 0-255. Experiments are conducted

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 9 , September 2016

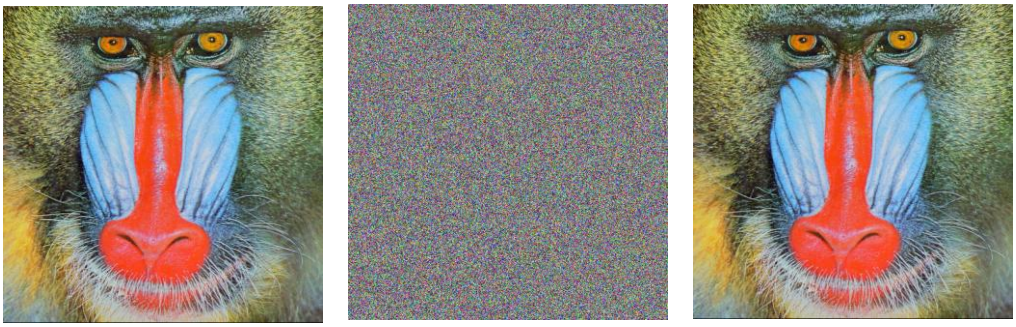
through the proposed scheme repeatedly on different images. The standard test images such as Animals, Barbara, Cheetah, Couple, Hippopotamus, Lake Boat, Lena, Mandrill, Nature and Splash are considered for experiments and reports.

The original images are shown in figure 3(a(i)), (b(i)) and (c(i)) respectively. The encrypted images are shown in figure 3(a(ii)), (b(ii)) and (c(ii)) respectively. The performance of the proposed encryption scheme is appraised by calculating the PSNR, IQIM values between the original and the encrypted images and correlation value (BCR) between the neighboring pixels regarding to equations (3),(4) and (5) respectively as described in Section IV and the derived results are offered in the table 3. The Peak Signal to Noise Ratio (PSNR) value of almost all encrypted images is found to be maximum 9.3725dB. The image quality distortion (IQIM) value of almost all encrypted images is found to be maximum 0.0087. The correlation coefficient (BCR) value of almost all encrypted images is found to be maximum 0.0825. The PSNR, IQIM, BCR results specified that the proposed encryption scheme furnishes competent encryption. Consequently the encrypted images are decrypted by means of given secret key, to obtain the original images and are offered in 3(a(iii)), (b(iii)) and (c(iii)) respectively.



3.(a(i)) 3.(a(ii)) 3.(a(iii))
Fig.3: (a)(i) Original Animals Image , (ii) Encrypted Image, (iii) Decrypted Image

3.(b(i)) 3.(b(ii)) 3.(b(iii))
Fig.3: (b)(i) Original Barbara Image, (ii) Encrypted Image, (iii) Decrypted Image



3.(c(i)) 3.(c(ii)) 3.(c(iii))
Fig.3 : (c)(i) Original Mandrill Image, (ii) Encrypted Image, (iii) Decrypted Image

Fig.3 Encryption and Decryption of Images.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 9 , September 2016

Table 3. PSNR, IQIM, BCR Values Obtained from Encrypted Images through Proposed System

IMAGE	PSNR	IQIM	BCR
Animals	9.021	0.0042	0.0825
Barbara	8.162	0.0067	0.0589
Cheetah	7.168	0.0028	0.0394
Couple	8.106	0.0036	0.0771
Hippopotamus	7.021	0.0047	0.0685
Lake boat	7.849	0.0038	0.0791
Lena	9.372	0.0012	0.0745
Mandrill	8.983	0.0011	0.0766
Nature	7.294	0.0087	0.0147
Splash	8.425	0.0084	0.0792

In order to test the robustness of the encryption scheme, the various analysis such as key sensitivity analysis and statistical analysis are conducted on the test images. The analysis results on test images are presented in subsequent sections.

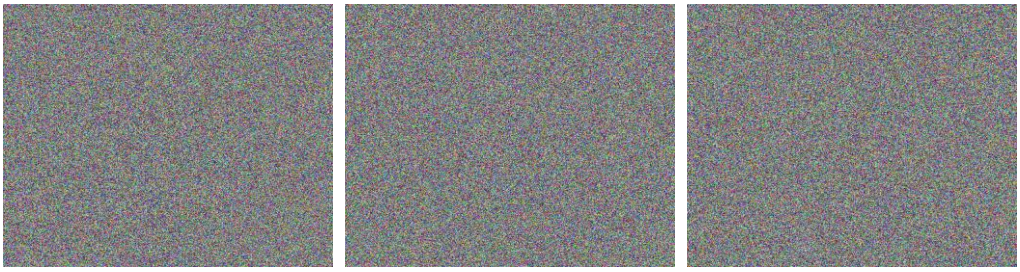
A. KEY SENSITIVITY ANALYSIS

The Three slightly modified secret keys are used to test the sensitivity analysis of key by means of encryption and decryption processes. Initially, the test image Animals is encrypted with help of key-1 of secret key and ciphered image shown in figure 4(a). Next the LSB one element of key-1 is changed to form the key-2 and is utilized to encrypt the same test image to get the encrypted image and the same is shown in figure 4 (b). Similarly MSB one element of key is changed to form the key-3 and is utilized to encrypt the same test image to get the encrypted image and the same is shown in figure 4(c).

Finally the encrypted images via slightly changed keys are compared. It is observed that the image shown in figure 4(a) is varied from the image shown in figure 4(b) and the disparity image is presented in figure 4(d). Similarly the image shown in figure 4(a) is varied from the image existing in figure 4(c) and the disparity image is presented in figure 4(e). It is difficult to match the encrypted images by merely watching these images. From the matching results the correlation between the associated pixels of the three encrypted images is measured via the formula stated in equation (5). The correlation value among the associated pixels of the three encrypted images pertaining to with the aforesaid slightly changed keys, is offered in table 4. The derived results indicate that there is no correlation surviving between the encrypted images although these images have been created through little bit altered secret keys.

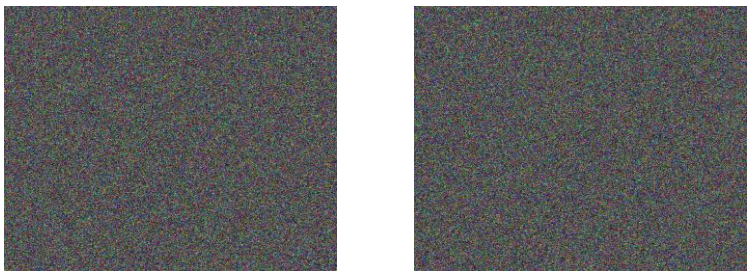
In addition, when a secret key-1 is utilized to encrypt an image and a slightly altered key-2 and key-3 achieved by modifying one element of key-1 are used to decrypt the same ciphered image, both decryptions are unsuccessful as shown in figure 4(f) and figure 4(g).

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 9 , September 2016



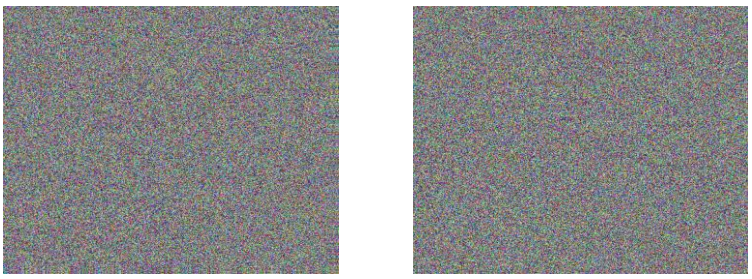
4.(a) 4.(b) 4(c)

Fig.4.(a) Animals Image Encrypted Using Key -1
Fig.4.(b) Animals Image Encrypted Using Key-2
Fig.4.(c) Animals Image Encrypted Using Key-3



4.(d) 4.(e)

Fig.4.(d) : Difference Between Fig.4.(a) & Figure. 4.(b)
Fig.4.(e) : Difference Between Fig.4.(a) & Figure. 4.(c)



4.(f) 4.(g)

Fig.4(f): Unsuccessful Decryption of Fig.4.(a) Using Slightly Modified Key2
Fig.4(g): Unsuccessful Decryption of Fig.4.(a) Using Slightly Modified Key3

Fig.4: Key Sensitivity Test on Animals Image

Table 4.: Correlation Coefficients Between The Related Pixels Of The Two Encrypted Images achieved Through Minor Changed Secret Keys on Animals Image

Image1 obtained using key	Image2 obtained using key	Correlation coefficient
Sk1	Sk2	0.0828
Sk1	Sk3	0.0687
Sk2	Sk3	0.0859

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 9 , September 2016

B. STATISTICAL ANALYSIS

Statistical analysis reveals the relative information between the original and encrypted images. The histogram offers a compact summation of the allocation of data in an image. An Image histogram shows the image pixels are allocated by plotting the number of pixels along with *y*-axis at each intensity level along with *x*-axis. Consequently encrypted image should be absolutely dissimilar from the original image. In order to analyse the level of security of proposed encryption scheme, histogram matching is employed to correlate the original and encrypted images.

In order to demonstrate that the proposed algorithm has more resistance to statistical attacks, an experiment is performed on the histogram of encrypted images. More than 10 colour images of size (512 x 512) are selected for this purpose and their histograms are matched with their corresponding encrypted image. The figure 5 offers the histograms of original and related partially encrypted test images. The histogram of the original images contains large spikes as shown in figure 5.(a(i)), (b(i)) and (c(i)) respectively, however the histogram of the encrypted images are more uniform as shown in figure 5 (a(ii)), (b(ii)) and (c(ii)) respectively. It is observed that the histogram of encrypted images is extremely dissimilar from histogram of their respective original images and encrypted image bears no statistical similarity to the original image. Therefore applying statistical attack on the proposed image encryption scheme is very strong.

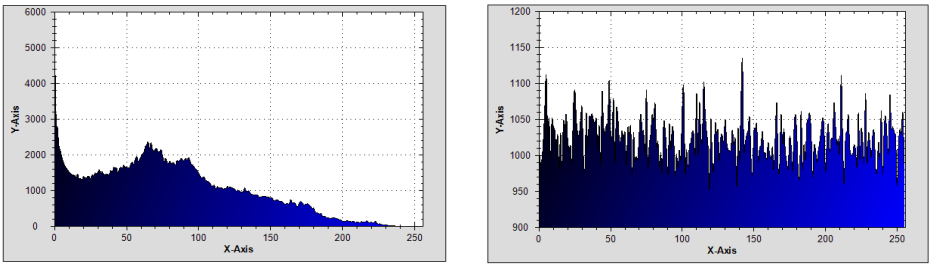


Fig.5a. (i) Histogram of Original Animals Image shown in fig.3(a(i)),
(ii) Histogram of Encrypted Animals Image shown in fig.3(a(ii))

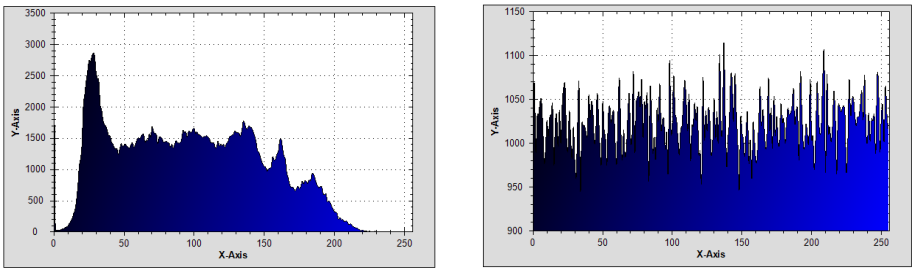


Fig.5.b (i) Histogram of Original Barbara Image shown in fig.3(b(i)),
(ii) Histogram of Encrypted Barbara Image shown in fig.3(b(ii))

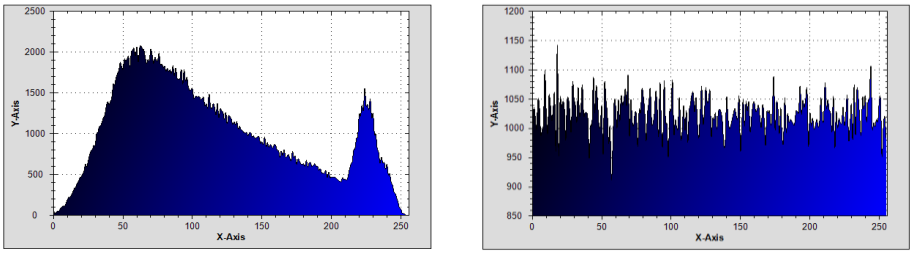


Fig.5.c (i) Histogram of original Mandrill Image shown in fig.3(c(i)),
(ii) Histogram of Encrypted Mandrill Image shown in fig.3(c(ii)),

Fig.5: Histogram of Original and Encrypted Images.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 9 , September 2016

VI. CONCLUSION

Elliptic curves are providing strong security with smaller key sizes and ECC are taking part in many applications. Smaller key sizes may result in faster execution timings for the image encryption. The security of ECC depends on how difficult it is to determine the secret key. Consequently, there is a computational advantage to using ECC with a shorter key length than other security algorithms. The intensity of each pixel is transformed into the elliptic curve and encrypted using ECC. The encrypted image is decrypted by using the key generated from the chosen elliptic curve. The lower values of PSNR, IQIM and BCR of experimental results have confirmed that the proposed security system is offering good security for digital images.

This technique can be further enhanced by making this method compatible to encrypt multimedia data or any other data which has to be transmitted securely. Furthermore this concept may be applied in mobile environment for safe transmission of images. ECC can be used into a security system such as Video Compression, Face recognition, Voice recognition, thumb impression, Sensor network, Industry and Institutions.

REFERENCES

[1] Kuo.C and M. Chen, "A New Signal Encryption Technique and its Attack Study," Proceedings of IEEE Internaional Conference on Carnahan Security Technology, pp. 149, October 1991.
[2] Bruce Schneier, " Applied Cryptography, John wilay sons Pvt. Limited –1996.
[3] Neal Koblitz, 'A course in number Theory and cryptography" 2nd Edition, John Wiley and Sons Pvt Ltd.1996.
[4] Philip P. Dang and Paul M. Chau, "Image Encryption for Secure Internet Multimedia Application", IEEE Transaction on Consumer Electronics, Vol. 46, No.3 pp. 395-403, Aug.2000.
[5] William Stallings, Cryptography and Network Security, Prentice Hall, 4th Edition, 2006.
[6] Feng Huang,Yong Feng and Xinhuo Yu, "A Symmetric Image Encryption Scheme Based on a Simple Novel Two-Dimensional Map", International Journal of Innovative Computing, Information and Control, Vol. 3, No. 6(b), pp 1593-1602, 2007.
[7] R. A. Winton, Enhancing the Massey-Omura Cryptosystem, Journal of Mathematical Sciences and Mathematics Education, Vol. 2, No. 1, (2007), pp. 21-29.
[8] Ganesan.K., I. Singh and M. Narain, "Public Key Encryption of Images and Videos in Real Time Using Chebyshev Maps", Fifth International Conference on Computer Graphics, Imaging and Visualization, 2008.
[9] Gong-bin.Q., J.Qing-feng and Q. Shui-sheng, "A New Image Encryption Scheme Based on DES Algorithm and Chuas Circuit", International Journal of Computer Science and Network Security, vol.8, No.4, April 2008.
[10] Ahmad.M. and M.Shamsher Alam, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", International Journal on Computer Science and Engineering, Vol.2 (1), pp. 46-50, 2009.
[11] Rafael C. Gonzalez, Richard E. Woods, "Digital Image Processing", third Edition, Pearson Prentice Hall, 2009.
[12] Muneeswaran, K.," Elliptic Curve Based Key Generation For Symmetric Encryption", IEEE Computing And Networking, 2011.
[13] S.V.Sathyanarayana,M.Aswatha Kumar and K.N.Hari Bhat , "Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points", International Journal of Network Security, Vol.12, No.3, PP.137-150, May 2011.
[14] Vinod Kumar Yadav et. Al. "Public Key Cryptosystem Technique Elliptic Curve Cryptography with Generator 'g' for Image Encryption", Int.J.Computer Technology & Applications,Vol 3 (1), 2012, 298-302.
[15] Srinivasan Nagaraj and G. S. V.P. Raju , " Image Security using ECC Approach ", Indian Journal of Science and Technology, Vol 8(26), 2015,pp 1-5.
[16] V.Sundaresan, K.S.Ganapathy Subramanian, K.Ganesan, "Discrete Mathematics".

AUTHOR'S BIOGRAPHY

R.SIVAKUMAR is a M.Phil research scholar in the Department of Computer Science Marudupandiyar College, Thanjavur, Tamilnadu, India.. He has received his B.Sc(CS) degree and MCA degree from Bharathidasan University, Trichy, TamilNadu, India. He is having more than 2 years of teaching experience. His area of research interest includes Network Security, Image Security and Software development.

Dr.K.THAMODARAN is working as Professor in the Department of Computer Science Marudupandiyar College, Thanjavur, Tamilnadu, India. He has received his M.Sc(CS) degree and M.Phill(CS) degree from Bharathidasan University, Trichy, TamilNadu, India. He has received his P.hD degree in Computer Science from Alagappa University, Karaikukdi, Tamilnadu, India. He is having more than 23 years of teaching experience. He has published 8 research papers in International Journals and presented 6 papers in the National and International conferences. His area of interest includes Network Security, Image Security and Optimization Techniques.