AL-Qadisiyha Journal For Science Vol.19 No. 3 Year 2014
Mayssa Abd ulkareem ISSN 1997-2490

EFFICIENT HYBIRD (OFKM-ECC) CRYPTOGRAPH SYSTEM USING IN COLOR IMAGE

Received : 23\10\2013 **Accepted : 26\2\2014**

Mayssa Abd ulkareem
Basrah University\Science College\Computer Science Department

ABSTRACT :

The use of image communication has increased in recent years where The rapid development of the communication network through the Internet and development of the electronic trade with spread of the digital media such as (images, audio, video) which can be got easily, copied, and distributed with another persons names. Each type of data has its own features; therefore different techniques should be used to protect confidential image data from unauthorized access. This paper has been proposed new encryption algorithm using in RGB image encryption supported by Elliptic Curve Cryptography (ECC) with forward key mixing (OFKM) process. The main advantage of elliptic curves systems is thus their high cryptographic strength relative to the size of the key. The propose scheme is simple, fast and sensitive to the secret key. The experimental results show that the proposed encryption technique is efficient and has high Security features.

KEYWORDS

ECC, public-key, secret key, encryption, decryption, color image.

1. INTRODUCTION

The widespread use of information exchange across the Internet, and the storage of sensitive data on open networks, cryptography is becoming an increasingly important feature of data security. Many cryptographic algorithms are available for securing information (E.g. RSA, DES, AES etc). Recently, a different approach of generating public key based on elliptic curve cryptography (ECC) [2, 4, 11]. Its security relies on the problem of computing logarithms on the points of an elliptic curve.Study of elliptic curves by the algebraists, algebraic geometers and number theorists dates back to the middle of the nineteenth century there are several criteria that need to be considered when selecting a family of public key schemes for a specific application. The principal ones are: Functionality and Security and Performance. For the desired level of security, do the protocols meet performance? Other factors that may influence a decision include the existence of best-practice standards. Elliptic Curve Cryptography provides an excellent solution not only for the data encryption but also for the secure key transport between two communicating parties [10] and authentic session key establishment protocols [1]. In the method, perfect binary tree was utilized to increase complexity in the encryption algorithm. Designed an encryption algorithm focusing on the application of properties of finite fields' and Elliptic curves. Additive and Affine encryption schemes using six schemes

of key sequences obtained from random elliptic curve points were designed [7, 11]. In this method, 8-bits mask was used for changing the pixel gray level of main image. For changing each pixel gray level, value of each bit of the mask was selected by one of the 256 cellular automat standard rules. One of the 256 cellular automat standard rules was determined by Commotion signal. The main attraction of combining ECC with OFKM algorithm is that it appears to offer equal security for a far smaller key size, thereby saving the processing overhead. To improve the strength of encryption and the speed of processing.

2. PROPOSED ENCRYPTION ALGORITHM

2.1 The Mathematical Overview

Elliptic curves are curves having a specific base point, these are given by explicit polynomial equations called "Weierstrass equations" [12]. Using these explicit equations, we show that the set of points of an elliptic curve forms an A Elian group[10].For fields of various characteristics, the Weierstrass equation can be transformed (and simplified) into different forms by a linear change of variables. We get easier equation for prime field of characteristic $\neq 2, 3$ and binary field [5, 7,10,11]. Definition: An elliptic curve E over the finite field Fp is defined by an equation of the form [4]:

$Y=X^3+AX+B \pmod P$…… ……. (1)

4A3+27B2 ARE NON ZERO. …… (2)

Together with a special point O, called the point at infinity. The set *E* (*Fp*) consists of all points (*x*, y), *x* □ *Fp*, *y* □*Fp*, which satisfy the defining equation (1), together with *O*. An elliptic curve can have many points; any straight line connecting two points of them intersects a third point. The point at infinity O is the third point of intersection of any two points of a vertical line with the elliptic curve. This makes it possible to generate all points out of jest a few [12]. The Arithmetic operations of the Elliptic Curves Group In order to define a cryptosystem on the set of points on an elliptic curve. We need to define an algebraic structure on the points. The easiest algebraic structure, which provides us with all necessary tools, is the group. Therefore we need to define neutral element, inverse elements, and the addition of two elliptic curve points, which needs to be associative [5], and the multiplying the point by integer number:

- The neutral element is O.
- The inverse of point $P=(x, y)$ is $-P=(x, -y)$.
- The addition of two elliptic curve points is:

Let *P=(x1, y1), Q=(x2, y2), R=(x3, y3), P, Q, R €E (Fp),* then *R=P + Q* as follows: *X3 = λ2 - x1 - x2, y3 = λ (x1 - x3) - y1*

Where $\lambda=y2-y1/x2-x1$, *if* $x1 \neq x2$ *and* $\lambda=3x^2_1+a/2y1$, *if* $x1 = x2$

- The multiplying of point by integer refers to computing *Q=KP*, where *P* and *Q* are points on an elliptic curve and *k* is an integer. This really means that we add *P* to itself *k* times. Makes use of the elliptic curve in which the variables and coefficients are all restricted to elements of the finites fields [12].

Two families of elliptic curves are used in cryptographic applications: Prime curves [3, 6] over *p Z* and binary curves (2) *m GF*. For a prime curve over *p Z* , we

use a cubic equation in which the variables and the coefficients all take on values in the set of integers from 0 through p-1 and the calculations are performed with respect to modulo p. (i.e., the inverse of the point (x, y) is the point (X,X The concept of ECC, which was proposed by N. Kobiltz [4,13]and V. Miller [10] in 1985 is that when any two points are selected and added, the point of the sum is generated and is used for cryptosystem. The elliptic curve (EC) over *m F*2is a set of points (x, y) to satisfy the equation $y2+xy=x^3+ax^2+b$. The procedure to generate a public key in ECC is outlined as follows [11, 13]:

(1) [Common] Select any irreducible polynomial f(x).
(2) [Common] Select any vector value a, b for EC such that $y=x^3+ax^2+b$.
(3) [Common] Select randomly an initial point P among points on ECC.
(4) [Sender] Receives p, E, P, k_r P from common.
(5) [Sender] Generates a random integer k_s as a private key.
(6) [Sender] Computes a public key k_sP by multiplying P by k_s and Registers it in the Common directory.
(7) [Sender] Computes a shared secret key k_s (k_rP) by multiplying k_s.
(8) [Receiver] generates a random integer as private key k_r.
(9) [Receiver] Computes a public key k_rP by multiplying P by kr and Registers it in His common directory.
(10) [Receiver] Computes a shared secret key k_s (k_rP) by multiplying k_s.

The algorithm (2) for the stream cipher is shown below to provide an in-depth understanding of the idea.

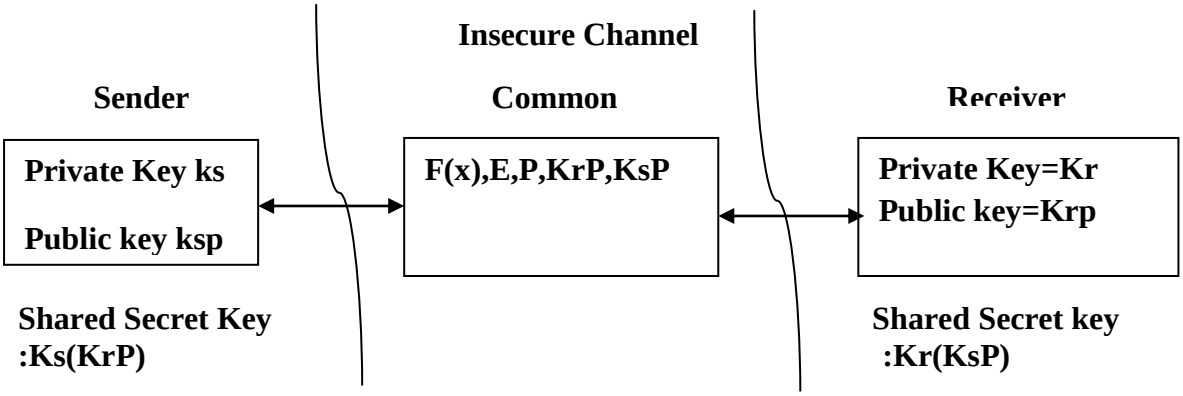


Figure (1) - Concept of ECC public key

2.2 OFKM KEY PROCESS

Image data have strong correlations among adjacent pixels forming intelligible information. To encrypt the image, this intelligible information needs to be reduced by decreasing the correlation among the adjacent pixels. The proposed encryption algorithm does this by modifying the pixel values of the image as well as reshuffling the pixels of the resultant image within itself. In following paragraph, functions of various processes used in the proposed algorithm are discussed. In the FKM used in the proposed algorithm [9]. In both the processes, image block is divided into sub-blocks (*p1, p2...p18*) and each sub-block (*pi*) is modified by using sub-key (*ki*), its previous sub-block (*pi-1*) and sub-block (*pi*) itself.

A similar process is used in the BKM process. In this paper we can use hybrid algorithm (OFKM) ODD forward key mixing used in the proposed algorithm. In this research we did algorithm operates on 64 values and the number of keys 32 and thus we have provided the number of keys less for the larger block. In both into sub-blocks and each sub-block contain 64 value (*p1, p2...p64*).each value in each sub-block (*pi*) is modified by using sub-key (*kJ*). The proposed encryption scheme uses a secret key of 64-bits size. The secret key is divided into 128 equal *parts of 32 bits each referred as sub-keys.*

k=k1k2k3 ……. k32

3. OFKM –ECC BLOCK ENCRYPTION

Encryption following leads to a faster and secure transmission of image data across a channel. Perfect reconstruction is possible with ECC Transform. A digital color image is represented in terms of three color components, namely, Red, Green and Blue (RGB). Each component is like gray scale image. So the three components of an RGB image can be coded separately and concatenated at the end .The proposed method is developed by the following:

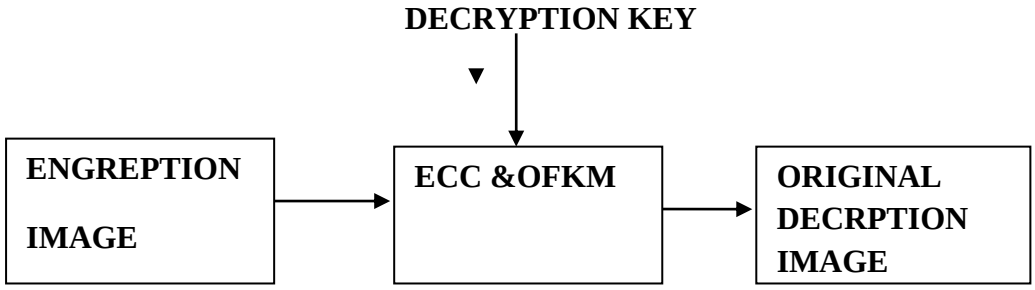


Figure (2) – System Diagram

This sender and receiver side has to do following steps:

step1. Put 32subkey each key length 8 bit that is to say the total length of the key 256 Bit

step2. Read type of color image file (JPG) and size of 256*256 pixels as the color Images divided into three levels B G R and then do the following:

A. Image divided into 16 section size 64*64.

B . Each section from 16 clips does data storage 64*64(4096) in vector Y and then Divided vector into smaller vectors each vector length 128 value as show in fig (3).

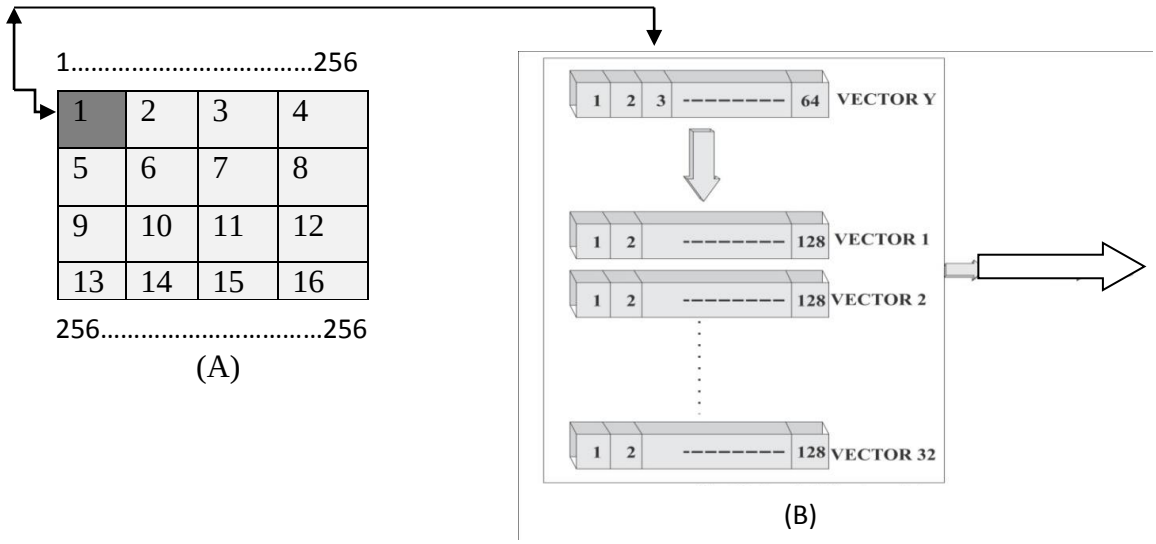


Fig (3) - (A) Image divided into 16 section size 64*64, (B) divided Y into 32 vectors

Then do the following:
1.Use algorithm OFKM to change the original data values from over mix it with 32 sub key as show in fig(4).

Odd Forward key mixing (OFKM) process [Algorithm 1]

p1= p1□□ k_i
FOR I=3 TO 64
IF I MODE 2 < > 0
Pi=Pi□ K_j j=1, 2… 32
ENDIF
ENDFOR

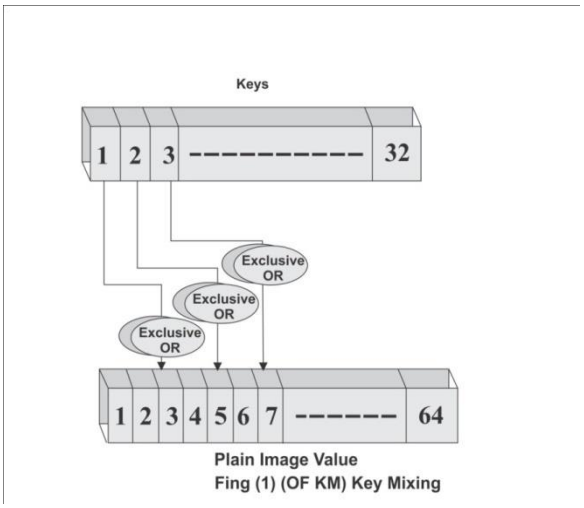


Fig (4) - key mixing (OFKM)

2.Using a key ei (public key),ej (private key)and two soft keys are independent use from ECC algorithm into data from the previous phase and through table has been initialized dimensions (do not have this…) (15*15) we express each constituent value of the image among 0-255.

Elliptic Curves [Algorithm 2]
Image-table= [{0}, {[0 0]} ;{ 1}, {[01]};
{2}, {[0 2]} ;{ 3}, {[0 3]};
•
•
{254}, {[15 14]} ;{ 255}, {[15 15]}];
Ei=elliptic curve point of 4a^3+27b^2+1 equation
G=private key
Ej=bitxor (ei, g)
Input V=input vector of length 128 value
Temph= [ ]
Temp= [ ]
For I=1 to 128
For j=1 to size (imagev-table)
If pvector (I) =imagev-table (j, I) then
Temph= [temph; imagv {j, 2}];
Temp= [temp; imagv {j, 2}];
End if
End for
End for
Tempi=integer Randomize (256);
H=temph (temp1)
Ci=bitxor (bitxor (ei (1), h, ei (2)) ;
Cj=bitxor (bitxor (ej (1), h, ej (2)) ;
Gg=bitxor (bitxor (ci, g), ci);
For I=1 to 128
Encryption vector temp (I) =bitxor (temp (I), Gg);
End for

3. The resulting data are encrypted and we storing them in the section according to the following table (1) in order to add greater security.

Color image decryption, the image decryption is the inverse process of the encryption Get encoded image by performing decryption using Secure Advanced OFKM and ECC to get the transform coded image as show in fig(5) .

Table (1) - (a) Plain image block (b) Encryption image block of OFKM-ECC Algorithms (c) Decryption image blocks

(a)

5	2	7	4
1	6	3	8
13	10	11	16
9	14	15	12

(b)

1	2	4	3
5	6	8	7
9	10	12	11
13	14	16	15

(c)

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

4. HISTOGRAM ANALYSIS

To prevent the access of information to attackers, it is important to ensure that encrypted and original images do not have any statistical similarities. The histogram analysis clarifies that pixel values of image are distributed. A number of images are encrypted by the encryption schemes under study and visual testis performed.
As shown in Fig. (6)

5. CORRELATION ANALYSIS

The correlation coefficient between original and cipher image of horizontal, vertically and diagonally is calculated in the objective is to obtain the value of correlation approach to the one and it is shown in Table 2, Association known as the equation (3) the following[8]: --

$$Corr = \frac{\sum_{r=1}^{N}\sum_{c=1}^{M}(I_1(r,c)-\bar{I}_1)(I_2(r,c)-\bar{I}_2)}{\sqrt{[\sum_{r=1}^{N}\sum_{c=1}^{M}(I_1(r,c)-\bar{I}_1)^2][\sum_{r=1}^{N}\sum_{c=1}^{M}(I_2(r,c)-\bar{I}_2)^2]}} \quad \text{..... (3)}$$

Where:I_1(r,c): is the value of the screen points in the (r, c) of the image described. While I_1(r, c) is a valuable component of the image in (r, c) of the original image is defined as follows:

$$\bar{I}_1 = \frac{1}{M \times N}\sum_{r=1}^{N}\sum_{c=1}^{M} I_1(r,c) \quad \text{... ... . (4)}$$

Where: I_2 (r, c): is the value of the screen points in the (r, c) of the image described.

$$\bar{I}_2 = \frac{1}{M \times N}\sum_{r=1}^{N}\sum_{c=1}^{M} I_2(r,c) \quad \text{..... (5)}$$

Where: I_2: is the rate of the retrieved image as:

M: Height the Image, N: width the image, r: the number of rows and the number of columns. For the color image must be retrieved for the three-color images taken in the calculation of the correlation. And the correlation calculated for each of the color

image is due to the re-installation. The rate of these three correlations is used to generate the image associated with the re-installation of RGB. That the equation of the link to the image color is:

$$Corr_{RGB} = \frac{Corr_{red} + Corr_{green} + Corr_{blue}}{3} \quad \text{..... ... (6)}$$

Where Corr red and Corr green and Corr blue (red link and link and link green blue), respectively, are the correlations for each color layer and the correlation calculated by equation (3) above**.**

Table (2) Correlation table (CR) for two adjacent pixels in the plain and its cipher image

Image	Horizontal correlation	Vertical correlation	Diagonal correlation
Baboon	**0.9167**	**0.9053**	**0.8759**
Baboon encrypted	**-0.0025**	**-0.0086**	**-0.0013**
Pepper	**0.9451**	**0.9504**	**0.9107**
Pepper encrypted	**0.0017**	**-0.0059**	**0.0036**
Lena	**0.9460**	**0.9720**	**0.9212**
Lena encrypted	**-0.0055**	**-0.0043**	**0.0017**
Monliza	**0.9856**	**0.9848**	**0.9731**
Monliza Encrypted	**0.0001**	**-0.0041**	**0.0028**
Lake	**0.9454**	**0.9719**	**0.9282**
Lake encrypted	**0.0123**	**-0.0276**	**0.0006**

6. INFORMATION ENTROPY

The proposed algorithm is secure against the entropy attack. The test result on different image for different round is defined in and show in table (3)**.**

$$H(m)=\sum_{i=1}^{2^N-1} P(m_i).\log_2\left(\frac{1}{P(m_i)}\right) \quad \text{.....(7)}$$

Table (3). Entropy for different images

EBinc	E Ginc	E Rinc	E Bimage	E Gimage	E Rimage	Pic name
7.8748	**7.8614**	**7.8649**	**7.5931**	**7.3362**	**7.5728**	**Baboon**
7.7985	**7.8654**	**7.8829**	**7.1222**	**7.6357**	**7.3898**	**Pepper**
7.8615	**7.8819**	**7.8393**	**7.0160**	**7.5834**	**7.2763**	**Lena**
7.7430	**7.8595**	**7.8566**	**6.5173**	**7.4368**	**7.5644**	**Monliza**
7.8255	**7.8161**	**7.8645**	**7.3502**	**7.4106**	**7.5930**	**Lake**

7. DIFFERENTIAL ANALYSIS

In general, a desirable characteristic of an encrypted image is being sensitive to the little changes in a Plain - image (e.g. modifying only one pixel). Adversary can create a small change in the input image to observe changes in the result. By this method, the meaningful relationship between original image and cipher image can be found [11]. If one little change in the plain image can cause a significant change in the cipher-image, with respect to diffusion and confusion, then the differential attack actually loses its efficiency and becomes almost useless. Tests have been performed on the encryption schemes on a 256-Level color image of size 256×256. The NPCR and UACI experiment result is shown in Table(4) According to the UACI estimation result, the rate influence due to one pixel change is very low. The results demonstrate that a swift change in the original image will result in a negligible change in the ciphered image.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \qquad \text{..... (8)}$$

Where *W* and *H* are the width and height of E1 or E2.We can define D(i,j) as :

$$D(i,j) = \begin{cases} 0, & \text{IF } E1(I,J)=E2(I,J) \\ 1, & \text{if } E1(i,j) \neq E2(i,j) \end{cases}$$

The UACI can define as

$$UACI = \frac{1}{W.H} * \frac{\sum_{i,j} |E1(i,j) - E2(i,j)|}{255} * 100 \qquad \text{..... (9)}$$

Table (4).NPCR&UACI

Image	NPCR	UACI
Baboon	**99.5087**	**32.9417**
Pepper	**100**	**29.4729**
Lena	**98.4100**	**26.5134**
monliza	**99.2722**	**30.6541**
Lake	**98.9471**	**22.5532**

8. CONCLUSIONS

In this paper, we have presented an application of ECC with odd forward key mixing in image encryption. ECC points and OFKM convert into cipher image pixels at sender side and Decryption algorithm is used to get original image within a very short time with a high level of security at the receiver side. Elliptic curves are believed to provide good security with smaller key sizes, something that is very useful in many applications. Smaller key sizes may result in faster execution timings for the image encryption. The propose scheme is simple, fast and sensitive to the secret key. We have carried out an extensive study of security and performance analysis of the proposed image encryption technique using various statistical analysis, key sensitivity analysis, differential analysis, speed performance, etc. Based on the results of our analysis, it conclude that the proposed image encryption technique is perfectly suitable for the secure image storing and transmission, the method of encryption proposed here provides sufficient security against cryptanalysis at relatively low computational overhead.

9. REFERENES

[1] Alfred J. Menezes and Scott A. Vanstone, ,(2012) , Elliptic Curve Cryptosystems and their implementations, International Journal of Distributed and Parallel Systems (IJDPS) Journal of Cryptology, Volume-6, Number-4, pages 209-224.

[2] A. ChandrasekhAR3 D. Sravana Kumar CH. Suneeth, (2012), ENCRYPTION OF DATA USING ELLIPTIC CURVE OVER FINITE FIELDS, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, pages 301-308.

[3] B. Santhi, K.S. Ravichandran, A.P. Arun and L. Chakkarapani, (2012), A Novel Cryptographic Key Generation Method Using Image Features, Department of ICT, School of Computing, SASTRA University, Thanjavur.

[4] Ch.Suneetha, D. Sravana Kumar and A. Chandrasekhar, (2011), secure key transport in symmetric photographic protocols using elliptic curves over finite fields, International Journal of Computer Application, Vol. 36, No. 1.

[5] Dr Kavya N , P Kiran P, S Sathish Kumar,(2012) , A Novel Framework using Elliptic Curve Cryptography for Extremely Secure Transmission in Distributed Privacy Preserving Data Mining, Advanced Computing: An International Journal (ACIJ), Vol.3, No.2

[6]Dr.K.V.Durgaprasad,S.Vasundhara,(2012),ELLIPTICCURVE RYPTOGRAPHY, International Journal of Engineering Research and Applications (IJERA), Vol. 2, no 5, page.1810-1816 .

[7]Mohsen Machhout eat.al. (2010), coupled FPGA/ASIC implementation of elliptic curve crypto-processor, International Journal of Network Security & its Applications Vol. 2 No. 2.

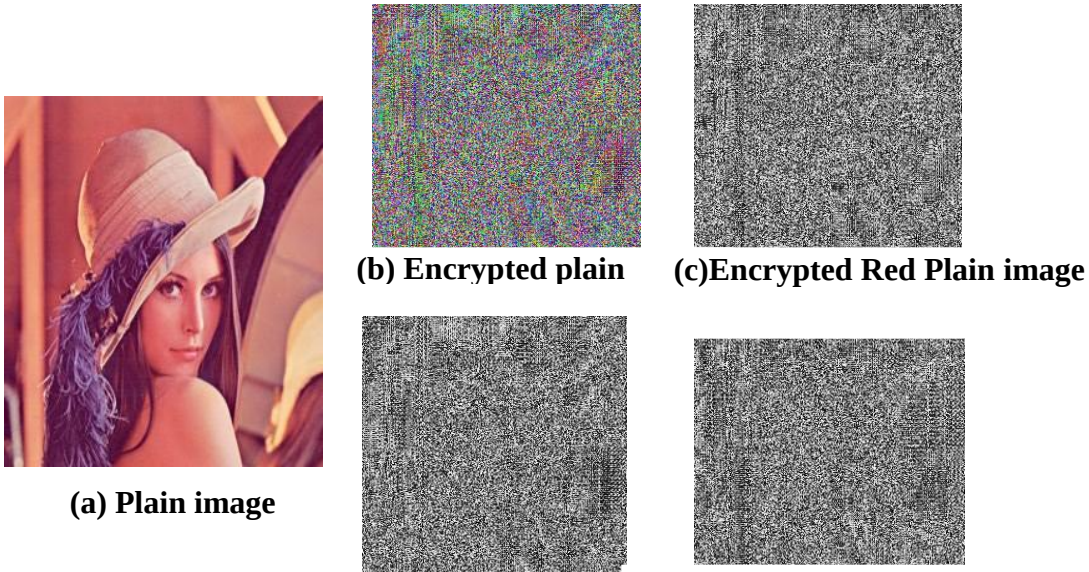
[8]Mays'a Abdul Karim Nasir , Sahera Obaid Sead ,(2010) Anew algorithm for Encryption based on Application the Chaotic Key (EACK),journal al-qadisiyah for pure science,vol.15,No.2,page 163-188.

[9]Narendra K Pareek, (2012), Design and analysis of novel digital image encryption schema, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2.

[10]Pareek, N.K., Patidar, Vinod, &Sud, K.K., (2006), Image encryption using chaotic logistic map Image and Vision Computing, 24, page 926-934.

[11]Patidar, Vinod, Pareek, N.K., &Sud, K.K.., (2010), Modified substitution–diffusion image cipher using chaotic standard and logistic maps.

[12]Vinod Kumar Yadav, Dr. A.K. Malviya, D.L. Gupta ,(2012), Public Key Cryptosystem Technique Elliptic Curve Cryptography with Generator g for Image Encryption in Nonlinear Science and Numerical Simulation, Computer Technology & Applications ,Vol. 3,No (1), page298-302.
[13] Yunpeng Zhang, Peng Sun, Liang Yi, Yongqiang Ma and Ziyi Guo,(2012), Analysis and Improvement of Encryption Algorithm Based on Blocked and Chaotic Image Scrambling, Engineering and Technology, 4(18), page 3440-3447



(a) Plain image

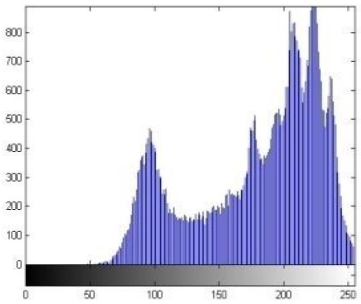
(b) Encrypted plain

(c)Encrypted Red Plain image

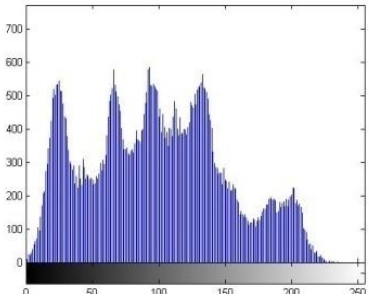
(d)Encrypted Green Pla image

(e)Encrypted *Blue Plain* image

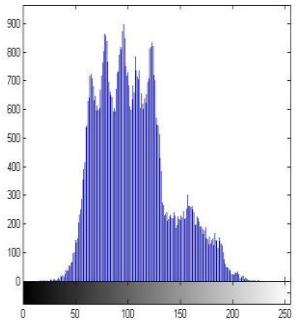
Figure (5) - result of encryption image LENA using OFKM_ECC algorithm



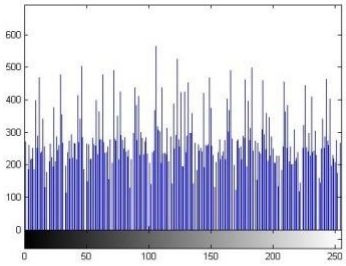
Histogram Red plain Image



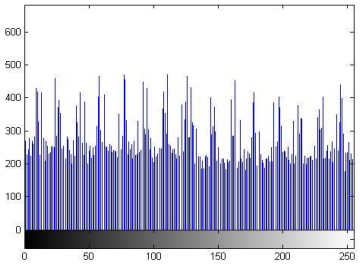
Histogram Green plain Image



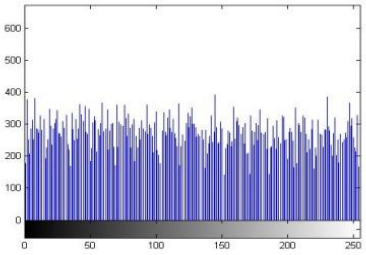
Histogram Blue plain Image



Histogram encrypted Red plain



Histogram encrypted Green plain Image



Histogram encrypted Blue plain Image

Figure (6) - result of Histogram image LENA

AL-Qadisiyha Journal For Science Vol.19 No. 3 Year 2014
Maysa Abd ulkareem ISSN 1997-2490

هجين كفوء(OFKM-ECC) لتشفير النظام باستخدام الصور الملونة

تاريخ الاستلام:23\10\2013 تاريخ القبول:26\2\2014

ميساء عبد الكريم ناصر
قسم علوم الحاسبات \ كلية العلوم \ جامعة البصرة

الخلاصة:

ازداد الاهتمام في اتصالات الصور في السنوات الاخيره حيث النمو السريع لشبكات الاتصال عبر الإنترنت وتطور التجارة الالكترونية وانتشار الأوساط الرقمية المختلفة مثل (الصور، الصوت، الفيديو) والتي أصبح من السهل الحصول عليها ونسخها وتوزيعها بأسماء أشخاص آخرين كل هذا أدى إلى خلق حاجة ملحة لحماية حقوق النشر واثبات الملكية وغيرها. تختلف خوارزميات التشفير باختلاف نوع البيانات لما لكل نوع من البيانات خواصه المختلفة.في هذا البحث تم اقتراح طريقة جديدة لتشفير الصور الملونة باستخدام خوارزمية المنحنيات الاهليجية ومفتاح خلط لمعالجه الصور.ان الفائده الرئيسية لأنظمة المنحنيات الإهليليجية هو ان قوة التشفير بها عالية مقارنة بحجم المفتاح.كما ان الخوارزمية المقترحة تمتاز بالسهولة والسرعة والسرية.

الكلمات المفتاحية
ECC, public-key, secret key, encryption, decryption, color image.