Proposed Image Encryption Algorithm Using Block Rotation and Elliptic Curve Cryptography

IMAN QAYS ABDULJALEEL

BASRA UNIVERSITY\SCIENCE COLLAGE\COMPUTER SCIENCE DEPT.

Abstract:

We have presented a low-latency algorithm designed for parallel Computer architectures to compute the scalar multiplication of elliptic curve cryptography (ECC) which an efficient technique of transmitting the image securely.

The image mixing and Encryption techniques were applied to provide the sufficient security and to reduce the risk of any attack during the delivery over the networks.

Our method is based on rotating blocks algorithm (left or right) and XOR operation to mixing all pixels in a color image before encryption it using ECC .

Finally, experimental results and security analysis show that the proposed image encryption scheme can resist exhaustive, statistical and differential attacks.

Keywords: Block cipher, encryption, decryption, color image, ECC, rotation.

خوارزمية مقترحة لتشفير الصور باستخدام تدوير الكتلة وتشفير المنحنى الاهليليجي

الملخص

قدمنا من خلال هذا البحث خوارزمية مبسطة لهياكل محوسبة متوازية لحساب الضرب العددي الخاص بتشفير المنحنى الاهليليجي (ECC) والذي يعتبر من اهم الاساليب الفعالة للنقل الامن.

ومن خلال استخدام اليه خلط بيانات الصورة وبعض من تقنيات التشفير المستخدمة تم الحصول على نسبه كفاءه عاليه من خلال حمايه البيانات المرسلة والمستلمة عبر الشبكة العنكبوتية وبالتالي تقليل المخاطر الناجمة عن اي محاولة تسعى للاستيلاء عليها. واعتمدت الخوارزمية المقترحة على استخدام الية التدوير الكتلي (باتجاه اليمين اوباتجاه اليسار) وعملية XOR لخلط كل البيانات الموجودة في الصورة الملونة قبل تشفيرها باستخدام ECC.

ومن خلال النتائج التجريبية والتحليل الامني بينا امكانية النظام المقترح على صد هجمات شاملة واحصائية وتفاضلية.

الكلمـات المفتاحيـة : التـشفير الكتلـي، التـشفير، فـك التـشفير، الـصورة الملونـة، خوارزميـة المنحنـى الاهليليجي، التدوير.

1. Introduction

With the rapid development of computer science, multimedia technology has become increasingly mature, so image encryption is a more and more important subject[1].

Image encryption techniques tend to convert original image into another image that is hard to be understood to keep the image confidential between users, in other word, it's important that without decryption key no one can access the content. Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. First, the image size is almost always much greater than that of text. Therefore, the old system takes more time for encrypting the image data directly. The second problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data[2].

The main attraction of ECC is that it can provide better performance and security for small key size, in comparison to RSA cryptosystem. In ECC a 160-bit key provides the same security as compared to the traditional crypto system RSA with a 1024-bit key, thus in this way it can reduced computational cost or processing cost [3].

The various ideas used in the existing image encryption techniques can be classified into three major types: position permutation, value transformation and the combination form [4]. A few image encryption techniques suggested recently are discussed in the following paragraph in brief.

Chang-Mok Shin, et al. [5] suggested method which was multilevel form of image encryption using binary phase exclusive OR operation and image dividing technique.

We can see in R. K. Gawande, et al. an algorithm uses two different techniques, Chaotic mapping and ECC to encrypted an image [6]. Kamlesh Gupta, et al. has been proposed an ethical way for image encryption using ECC algorithm [7]. P.G. Shah, et al. have used ECC-based authentication algorithm in which they conclude that elliptic curve scalar multiplication is core operation, but this operation is the most time consuming operation [8].

2. Related Works:

In this paper we used elliptic curves. The study of elliptic curves by algebraists, algebraic geometers and number theorists dates back to the Last of the twentieth century. Elliptic Curve Cryptography (ECC) was discovered in 1985 by Neal Koblitz and Victor Miller[9]. An elliptic curve in its "standard form" is described below:

2.1 Elliptic Curve Cryptography (ECC)

Elliptic curves are curves having a specific base point, these are given by explicit polynomial equations called "Weierstrass equations" [10].

In realistic terms, the performance of ECC can be increased by selecting particular underlying finite fields of particular interest and referred to as the elliptic group mod p, where p is a prime number. This is defined as follows. Choose two nonnegative integers, u and v, less than p that satisfy:[3]

$$4u^3 + 27v^2 (mod\ p) \neq 0 \dots (1)$$

Then Ep(x, y) symbolises the elliptic group mod p whose elements (x, y) are nonnegative integers less than p which satisfies the condition:

$$y^2 = x^3 + ax + b\ (mod\ p) \dots (2)$$

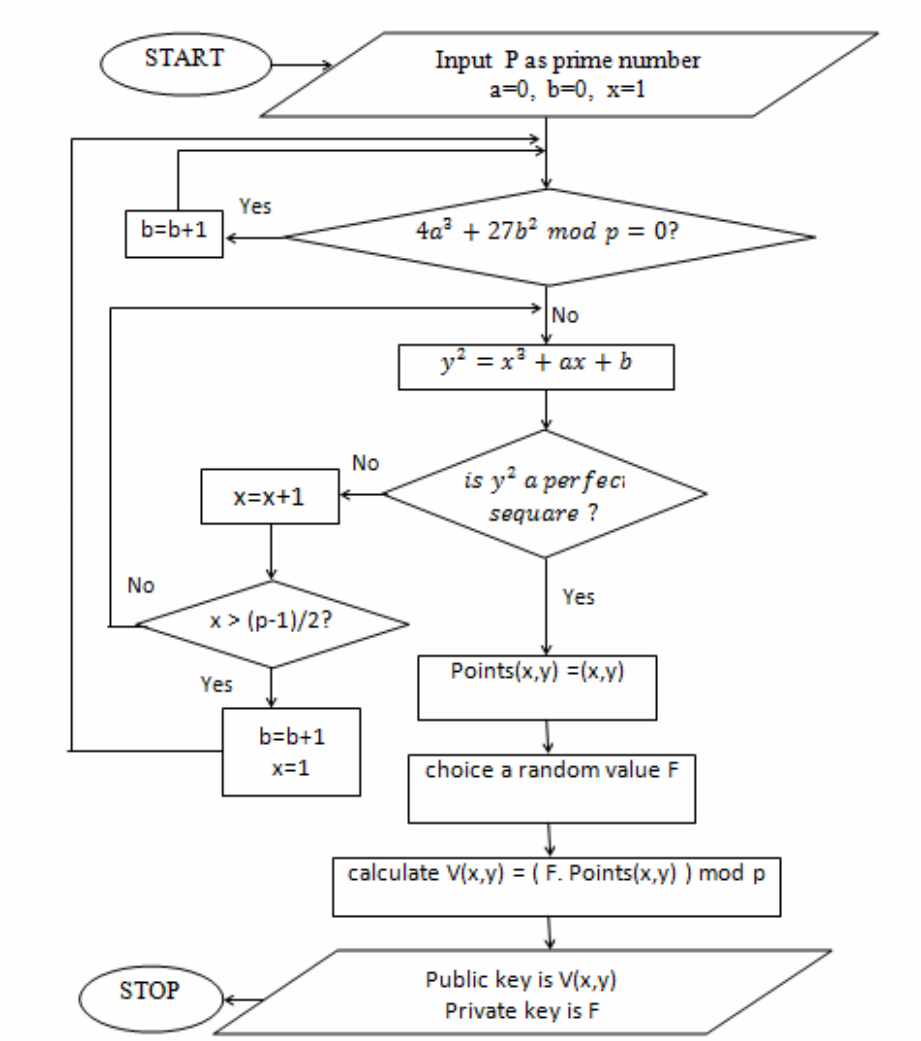


Figure (1): elliptic curve cryptography algorithm

Let P(xp,yp) and Q(xq,yq) be the two points on the curve of Eq.2.Then the point additions P + Q , as well as point doubling P + P are two operations defined on elliptic curve E which can geometrically be represented by tangent and chord operation. By applying the point addition and doubling operation we can multiply a scalar k with a point P, such that kP = Q, where k is a scalar. Given P and Q, it is computationally infeasible to obtain k. If k is sufficiently large, k is the discrete logarithm of Q to the base P. Hence the main operation involved in ECC is related to the point multiplication i.e. multiplication of a scalar k with any point P on the curve to obtain another point Q on the curve[11,12]. The elliptic curve algorithm described in fig (1) [11,12].

3. The Proposed System:

The proposed algorithm has the following features:

1. It is used a recursion Block array partition to the input RGB image.
2. Each output block size is of 64*128 pixels.
3. Each output block contain small blocks array of size 8*8 pixels.
4. We have a 32 random sub-keys , each sub-key have 8 bits , that's mean the total sub-keys size 256 bits.
5. Rotation technique is used .
6. ECC algorithm is used.

3.1 The proposed Rotation technique

In this paper we present a new rotation technique depends on blocking each image into separated blocks. Each block contain 64 pixel(8*8 pixel) .

The algorithm steps are:

- Input a block of 64 pixels and save it as matrix of 8*8 pixel.
- Rotate each vertical line in this matrix as(describe in Figure(2)) :

Rotate row 1 one location to the left.
Rotate row 2 two locations to the left.
Rotate row 3 three locations to the left.
Rotate row 4 four locations to the left.
Rotate row 5 one location to the right.
Rotate row 6 two locations to the right.
Rotate row 7 three locations to the right.
Rotate row 8 four locations to the right.

1	2	3	4	5	6	7	8	←	left rotation one location
9	10	11	12	13	14	15	16	←	left rotation two location
17	18	19	20	21	22	23	24	←	left rotation three locatio
25	26	27	28	29	30	31	32	←	left rotation four location
33	34	35	36	37	38	39	40	→	right rotation one locatior
41	42	43	44	45	46	47	48	→	right rotation two locatior
49	50	51	52	53	54	55	56	→	right rotation three locati
57	58	59	60	61	62	63	64	→	right rotation four locatio

Figure (2): Vertical Rotation step in the proposal rotation algorithm

- Rotate each horizontal line in the results matrix from the above step as (describe in Figure(3)) :

Rotate column 1 one location upward.
Rotate column 2 two locations upward.
Rotate column 3 three locations upward.
Rotate column 4 four locations upward.
Rotate column 5 one locations downward.
Rotate column 6 two locations downward.
Rotate column 7 three locations downward.
Rotate column 8 four locations downward.

2	3	4	5	6	7	8	1
11	12	13	14	15	16	9	10
20	21	22	23	24	17	18	19
29	30	31	32	25	26	27	28
40	33	34	35	36	37	38	39
47	48	41	42	43	44	45	46
54	55	56	49	50	51	52	53
61	62	63	64	57	58	59	60
↑	↑	↑	↑	↓	↓	↓	↓
upper rotation one location	upper rotation two location	upper rotation three location	upper rotation four location	down rotation one location	down rotation two location	down rotation three location	down rotation four location

Figure (3): Horizontal Rotation step in the proposal rotation algorithm

- Save the result matrix as a new block in the mixing image.

11	21	31	35	57	51	45	39
20	30	34	42	6	58	52	46
29	33	41	49	15	7	59	53
40	48	56	64	24	16	8	60
47	55	63	5	25	17	9	1
54	62	4	14	36	26	18	10
61	3	13	23	43	37	27	19
2	12	22	32	50	44	38	28

Figure (4): result step in the proposal rotation algorithm

- Repeat the above steps into all original image blocks to find the new mixing image.

3.2 Encryption algorithm

Encryption algorithm completes in three steps:

1. Input 32 sub-keys each key have 8 bits.
2. Input original image then split up into R G B values. These values denoted the intensity levels of the Red, Green and Blue shades denoted by values ranging from 0 – 255. The algorithm worked upon each of these R G and B values separately.
3. sorting each level pixels(R or G or B) into 8 big blocks array (each block array contain 64*128 pixels) as explain in figure(5)

a. Each block of the 8 big blocks separated into another small blocks array (each small block array contain 8*8 pixels). That mean we have 4 small blocks array. see figure (5)

b. XOR operation between each value in the small blocks (i.e. block array of 8*8 pixels) and 8 keys generation from the 32 keys(see figure(6)).
c. Rotate each horizontal or vertical vector into a small block by using proposed rotation algorithm (see figures (2-4)).
4. After finishing mix and rotation all values in each 8 big blocks, encryption stage can be started Using ECC algorithm to encrypt each block array with the public and private key as describe above.
5. Save the encrypted image.

Figure (7) describe the flowchart of proposed algorithm.

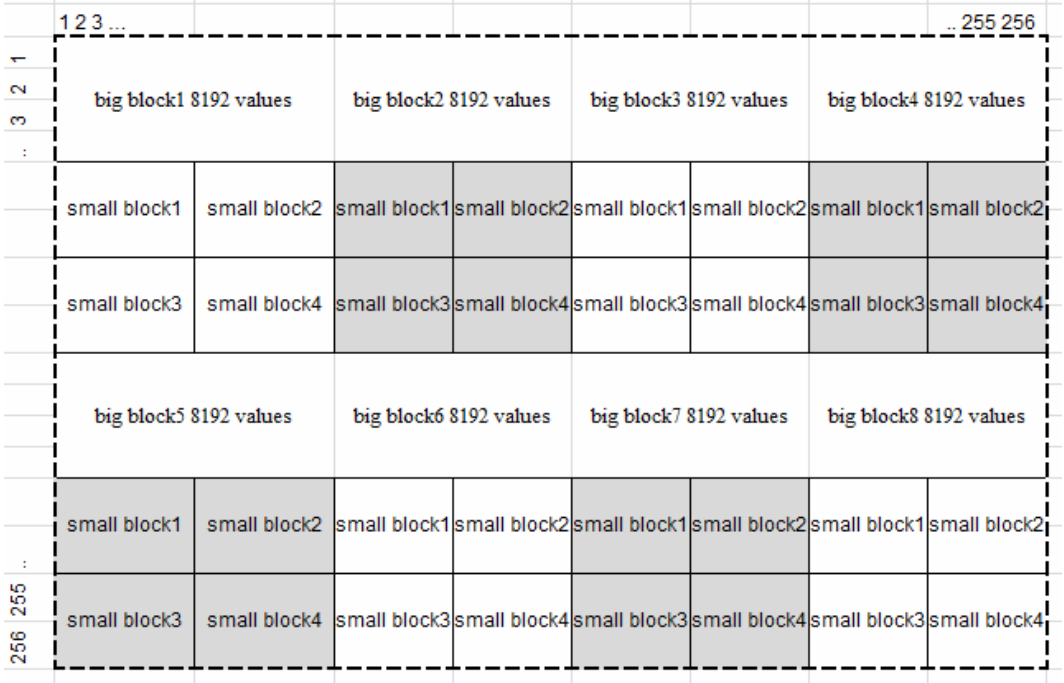


Figure (5): original input image after blocking it into eight big blocks.

v11	v12	v13	v14	v15	v16	v17	v18	→	XOR K1
v21	v22	v23	v24	v25	v26	v27	v28	→	XOR K2
v31	v32	v33	v34	v35	v36	v37	v38	→	XOR K3
v41	v42	v43	v44	v45	v46	v47	v48	→	XOR K4
v51	v52	v53	v54	v55	v56	v57	v58	→	XOR K5
v61	v62	v63	v64	v65	v66	v67	v68	→	XOR K6
v71	v72	v73	v74	v75	v76	v77	v78	→	XOR K7
v81	v82	v83	v84	v85	v86	v87	v88	→	XOR K8

small block 1 in big block 1

v11	v12	v13	v14	v15	v16	v17	v18	→	XOR K9
v21	v22	v23	v24	v25	v26	v27	v28	→	XOR K10
v31	v32	v33	v34	v35	v36	v37	v38	→	XOR K11
v41	v42	v43	v44	v45	v46	v47	v48	→	XOR K12
v51	v52	v53	v54	v55	v56	v57	v58	→	XOR K13
v61	v62	v63	v64	v65	v66	v67	v68	→	XOR K14
v71	v72	v73	v74	v75	v76	v77	v78	→	XOR K15
v81	v82	v83	v84	v85	v86	v87	v88	→	XOR K16

small block 2 in big block 1

v11	v12	v13	v14	v15	v16	v17	v18	→	XOR K17
v21	v22	v23	v24	v25	v26	v27	v28	→	XOR K18
v31	v32	v33	v34	v35	v36	v37	v38	→	XOR K19
v41	v42	v43	v44	v45	v46	v47	v48	→	XOR K20
v51	v52	v53	v54	v55	v56	v57	v58	→	XOR K21
v61	v62	v63	v64	v65	v66	v67	v68	→	XOR K22
v71	v72	v73	v74	v75	v76	v77	v78	→	XOR K23
v81	v82	v83	v84	v85	v86	v87	v88	→	XOR K24

small block 3 in big block 1

v11	v12	v13	v14	v15	v16	v17	v18	→	XOR K25
v21	v22	v23	v24	v25	v26	v27	v28	→	XOR K26
v31	v32	v33	v34	v35	v36	v37	v38	→	XOR K27
v41	v42	v43	v44	v45	v46	v47	v48	→	XOR K28
v51	v52	v53	v54	v55	v56	v57	v58	→	XOR K29
v61	v62	v63	v64	v65	v66	v67	v68	→	XOR K30
v71	v72	v73	v74	v75	v76	v77	v78	→	XOR K31
v81	v82	v83	v84	v85	v86	v87	v88	→	XOR K32

small block 4 in big block 1

Figure (6): explain blocking of big block (1) into 4 small blocks of 8*8 pixels

In the decryption process, we should provide the same 32 sub-keys. The user split encrypted image to 8 big blocks then we take 256 pixels as an input vector to ECC algorithm to be decrypted. After decrypting 256 pixels we split it to 4 small blocks as described in encryption algorithm. Then we try to reverse all the steps of rotation algorithm followed by XOR operation between each pixel in small block and sub-keys before we reconstruct the original image.

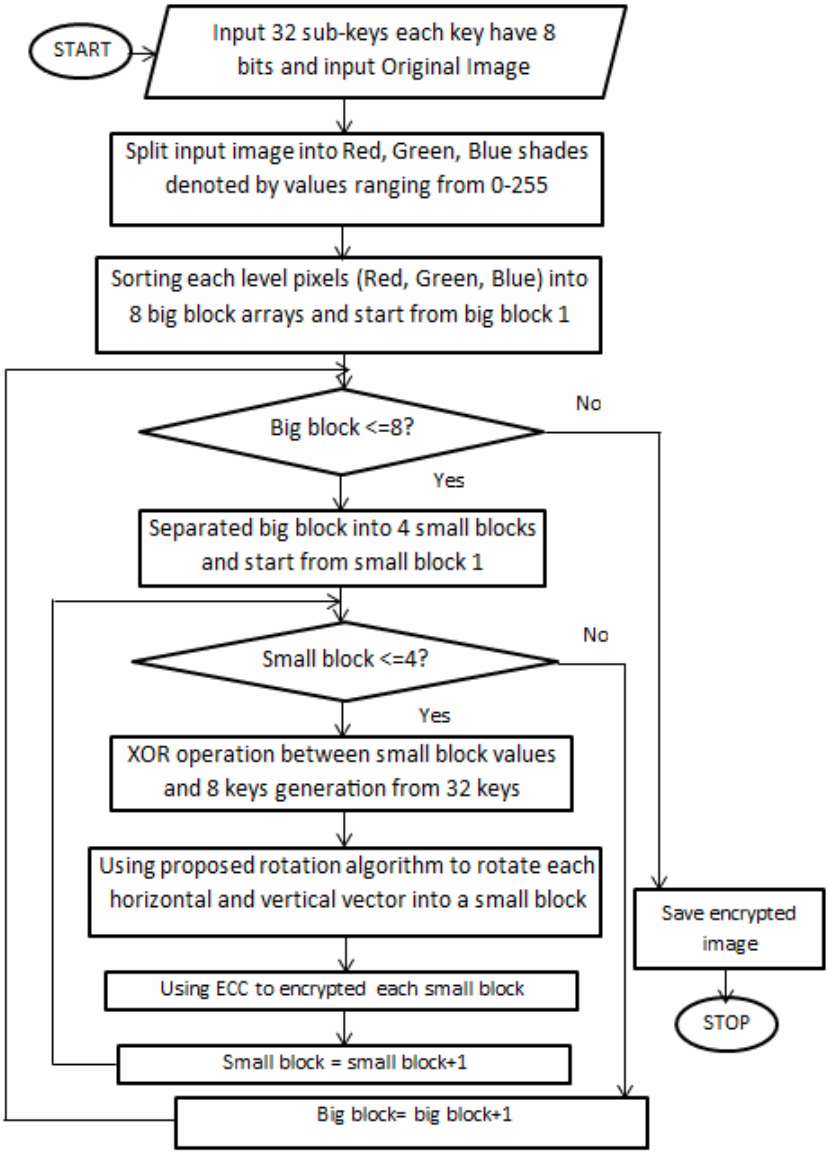
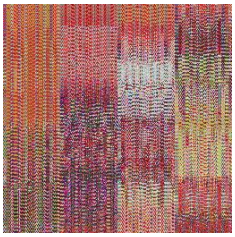


Figure (7): Proposed Encryption algorithm flowchart

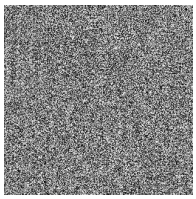
4. Experimental results

The proposed encryption algorithm was applied in a JPEG color image that have the size 256*256 pixels. Four color images are used in this paper (LENA, PEPEAR, BABOON, BARBARA). LENA experiments are given in Figure (8).

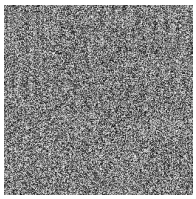
(a)original image



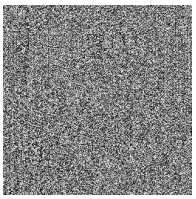
(b) mixing pixel using proposed rotation algorithm



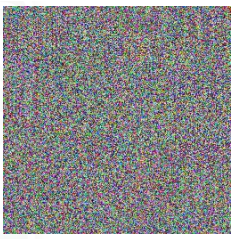
(c) Red channel encryption using proposed algorithm



(d) Green channel encryption using proposed algorithm



(e) Blue channel encryption using proposed algorithm



(f) color image encryption using proposed algorithm

(g) decrypted image

Figure (8): experiment result of LENA after using the proposed encryption algorithm

5. System Performance

We describe below the most important performance of the proposed system:

5.1 Differential attack:

In general, a desirable property for the proposed cipher is its sensitive to small change in the plain-image (single bit change in plain-image). To crack the encryption we can create a small change in the original image to observe changes in the result. By this procedure, a significant relationship between the original image and the encrypted image can simply exist. If one small 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 practically useless. Three common measures have been used for differential analysis: The Number of Pixels Change Rate (NPCR) measures the different pixel numbers between two images and UACI(Unified Average Changing Intensity) measures the average intensity of differences between the original image and the encrypted image [13,14].

Suppose we have two encrypted images, whose corresponding original images have only one pixel difference, be denoted by E1 and E2. Denote a bipolar matrix D, and D have the same size as E1 and E2. Then, D(i,j) can calculated by E1(i,j) and E2(i,j) as describe in equation(3).

$$D(i,j) = \begin{cases} 0, & \text{if } E1(i,j) = E2(i,j) \\ 1, & \text{if } E1(i,j) \neq E2(i,j) \end{cases} \quad \ldots(3)$$

The NPCR of these two images is defined in equation(4)

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad \ldots(4)$$

Where W and H are the width and height of E1 or E2.

The UACI can define as

$$UACI = \frac{1}{W \times H} \times \frac{\sum_{i,j} |E1(i,j) - E2(i,j)|}{255} \times 100 \ldots (5)$$

Tests have been performed on the proposed algorithm on a 256-level grey scale image of size 256×256 pixels. The results are shown in Table (1). The results of NPCR and UACI show that a small change in the original image will result in a significant difference in the encrypted image. Therefore, the proposed method has a good capability to resist the differential attack.

Table(1): result of differential analysis

image	NPCR	UACI
LENA	99.1898	33.3165
BABOON	99.4095	29.0141
PEPEAR	99.5850	31.1193
BARBARA	99.9832	30.1763

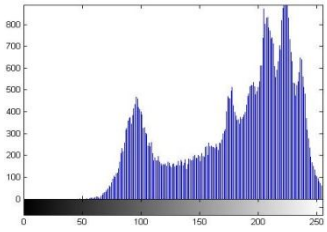
5.2 **Histogram analysis:**

An image-histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level [15]. It is important to

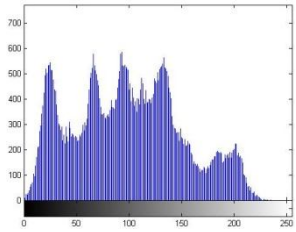
guarantee that the original image and encrypted image at each intensity level (Red, Green and Blue) do not have any statistical similarities.

Figure (9) explains the histogram of the Red, Green and Blue components of the original images and its corresponding Red, Green and Blue components of the encrypted images. We can notice that the histogram of the original color image is very different from the histogram of the encrypted color image. This result shows that statistical attacks based on the histogram analysis can't give any information to break the proposed cryptography algorithm.

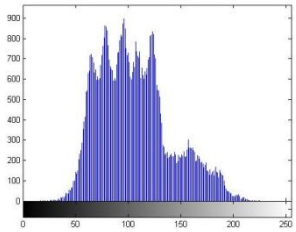
(a) original image



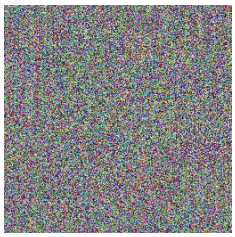
(b) Red channel histogram of original image



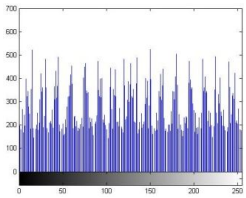
(c) Green channel histogram of original image



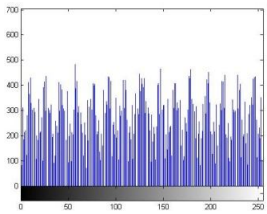
(d) Blue channel histogram of original image



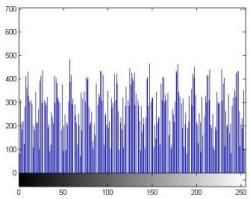
(e) encryption image



(f) Red channel histogram of encrypted image



(g) Green channel histogram of encrypted image



(h) Blue channel histogram of encrypted image

Figure (9): Histogram result of original and encrypted image LENA.

5.3 Correlation analysis:

There is a very good correlation among adjacent pixels in the digital image [14].

To test the correlation properties of the enciphered image, we performed statistical analysis on the encryption algorithm. This is done by testing the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels, respectively.

Equation (6) is used to study the correlation between two adjacent pixels in the horizontal, vertical and diagonal orientations [16].

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \dots (6)$$

$$D(x) = \frac{1}{N}\sum_{j=1}^{N}(x_j \times \frac{1}{N}\sum_{j=1}^{N} x_j)^2 \dots (7)$$

$$cov(x,y) = \frac{1}{N}\sum_{j=1}^{N}(x_j \times \frac{1}{N}\sum_{j=1}^{N} x_j)\left(y_j - \frac{1}{N}\sum_{j=1}^{N} y_j\right) \dots (8)$$

Where x and y are intensity values of two neighboring pixels in the original image and N is the number of adjacent pixels selected. E(x) is the estimation of mathematical expectations of x, D(x) is the estimation of variance of x, and cov(x,y) is the estimation of covariance between x and y. x and y are grey-scale values of two adjacent pixels in the image. Table (2) shows the correlation of two vertical, Horizontal and diagonal adjacent pixel in the original and those in the encrypted image. If the correlation coefficient equals zero, then the encryption image has no features and highly independent on the original image. If the correlation coefficient equal -1, this means encrypted image is a negative of the original image [17].

Table(2): correlation of two pixels

CHOSEN image		**adjacent pixels in correlation analysis**		
Image	**Image type**	**Horizontal correlation**	**Vertical correlation**	**Diagonal correlation**
LENA	Original image	0.9167	0.9053	0.8759
	Encrypted image	-0.0002	-0.0035	-0.0026
BABOON	Original image	0.9460	0.9720	0.9212
	Encrypted image	-0.0015	0.0001	-0.0097
PEPPEAR	Original image	0.9653	0.9768	0.9475
	Encrypted image	0.0052	-0.0018	-0.0013
BARBARA	Original image	0.9451	0.9504	0.9107
	Encrypted image	0.0043	-0.0037	-0.0023

5.4 **Image entropy**

Entropy is a statistical measure of randomness that can be used to characterize the texture of an image [15]. It is well known that the entropy H of a massage source S can be calculated as:

$$H(m) = \sum_{i=1}^{2N-1} P(m_i).log_2(\frac{1}{P(m_i)}) \quad \ldots(9)$$

Where p(mi) represents the probability of message mi and the entropy is expressed in bits. When we encrypted an image, the idealistic value of entropy should be 8. Let us consider the cipher-images in Table (3).We found the output of such a cipher-images emits symbols with entropy of less than 8. This means that information leakage in the proposed encryption process is negligible.

Table (3) entropy value of experiment images

IMAGE	RGB image	Entropy of Original image	Entropy of Encrypted image
LENA	RED image	7.5728	7.8709
	GREEN image	7.3362	7.8567
	BLUE image	7.5931	7.8462
BABOON	RED image	7.2763	7.7894
	GREEN image	7.5834	7.8773
	BLUE image	7.0160	7.8018
PEPEAR	RED image	7.5678	7.8422
	GREEN image	7.3961	7.8437
	BLUE image	7.4999	7.8236
BARBARA	RED image	7.3898	7.8038
	GREEN image	7.6357	7.8328
	BLUE image	7.1222	7.7809

6. Conclusion

In this paper we presented new algorithm for image encryption by using sorting of pixels as per their RGB values and XOR them with random 32 sub-key (each sub-key have 8 bits) then we rotation each pixels left and right which helped to reduce the correlation between pixels and increased entropy value.

We present an elliptic curves public key solution to the traitor tracing problem from the wide variety of possible group structures of points on an elliptic curve, and from the fact that addition on elliptic curves is somewhat complicated. This to attraction of using elliptic curves compared to other is that it appears to offer equal security for a far smaller bit size, thereby reducing processing overhead.

We used Matlab 7 and this is a lossless image encryption algorithm with results.

References

[1] Y. Zhang,P. Sun,L. Yi, Y. Ma and Z. Guo(2012)" Analysis and Improvement of Encryption Algorithm Based on Blocked and Chaotic Image Scrambling", Research Journal of Applied Sciences, ISSN: 2040-7467, Engineering and Technology 4(18): 3440-3447.

[2] A. Srivastava (2012)" A survey report on Different Techniques of Image Encryption", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 6.

[3] V. K. Yadav, A.K. Malviya, D.L. Gupta, S. Singh, and G. Chandra (2012) " Public Key Cryptosystem Technique Elliptic Curve Cryptography with Generator g for Image Encryption", ISSN:2229-6093 , Int.J.Computer Technology & Applications, Vol 3 (1), 298-302.

[4] N. K. Pareek, V. Patidar, and K. K. Sud (2011)" A Symmetric Encryption Scheme for Colour BMP Images", IJCA Special Issue on "Network Security and Cryptography" NSC.

[5] Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim (2003)"Multilevel Image Encryption by Binary Phase XOR Operations ", IEEE.

[6] R. K. Gawande, P. S. Kulkarni and K. A. Ganar (2012)" Multi Level Image Encryption using Chaotic Mapping And Elliptic Curve Cryptography", International Conference On Engineering Innovation and Technology, ISBN : 978-93-81693-77-3, Nagpur.

[7] Gupta, K., Silakari, S. (2010) "Performance Analysis for Image Encryption Using ECC," Computational Intelligence and Communication Networks (CICN), 2010 International Conference on, vol., no., pp.79-82.

[8] P.G. Shah, X. Huang and D. Sharma (2010)"Sliding window method with flexible window size for scalar multiplication on wireless sensor network nodes," proceeding in international conference on wireless communication and sensor computing, pp. 1-6.

[9] V.S. Miller (1986)"Use of Elliptic Curves in Cryptography", Advances in Cryptology- Proceedings of CRYPTO'85, Springer Verlag, pp 417-426.

[10] J. H. Silverman (1986)"The Arithmetic of Elliptic Curves",Graduate Text in Mathematics 106, Springer-Verlag.

[11] D. Hankerson , A. menezes and S. Vanstone (2004) "Guide to Elliptic Curve Cryptography", Springer-Verlag New York, Inc.

[12] D. Aglawe, S. Gajbhiye (2012)"Software Implementation of Cyclic Abelian Elliptic Curve using Matlab.", International Journal of Computer Applications (0975 – 8887) Vol. 42, No.6.

[13]. Xiao Feng, X.T., Shaowei Xia (2011)"A Novel Image Encryption Algorithm Based On Fractional Fourier Transform and Magic Cube Rotation", in IEEE 4th International Congress on Image and Signal Processing., IEEE: China. p. 1008-1011.

[14]. A.N. Pisarchik, M.Z. (2008) "Image Encryption with Chaotically Coupled Chaotic Maps". Physica D., Vol. 237, No. 20: p. 2638-2648.

[15] A. Awad , A. Saadane (2010)" New Chaotic Permutation Methods for Image Encryption", IAENG International Journal of Computer Science,37:4.

[16] K. Faraoun (2010)" Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption", The International Arab Journal of Information Technology, Vol. 7, No. 3.

[17] A. Gautam, M. Panwar, P.R Gupta (2011) " A New Image Encryption Approach Using Block Based Transformation Algorithm", INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES, Vol. 8, Issue No. 1,pp. 090 – 096.