Partial Cryptography in Digital Media Environment Based on ECC Algebra

Hala B. Abdul Wahab[1]and Rafal Ali Sameer[2]*

[1]Department of Computers, University of Technology,Baghdad,Iraq

[2]Department of Computers, College of Science, University of Baghdad, Baghdad, Iraq

Abstract

In recent years, Elliptic Curve Cryptography (ECC) has attracted the attention of researchers and product developers due to its robust mathematical structure and highest security compared to other existing algorithms like RSA. It is found to give an increased security compared to RSA for the same key-size or same security as RSA with less key size. In this paper a new approach is proposed for encrypting digital image using the arithmetic of elliptic curve algebra. The proposed approach produced a new mask for encrypt the digital image by use a new convolution processes based on ECC algebra operations and work as symmetric cryptographic system instead of asymmetric system. A new approach combined both compression and encryption algorithms, the compression algorithm used here is discrete wavelet transform to decompose the image information into four subbands (LL, LH, HL, and HH), then LL subband will be encrypted. The new approach test by execute encryption and decryption processes was more flexible and efficient.

Keywords: Digital image, DWT, Partial encryption, ECC.

التشفير الجزئي في بيئة الوسائط المتعددة بالاعتماد على رياضيات تشفير المنحني الاهليجي

هالة بهجت عبد الوهاب[1] و رفل علي سمير[2]*

[1]قسم علوم الحاسبات, كلية العلوم، الجامعة التكنولوجية, بغداد, العراق

[2]قسم علوم الحاسبات, كلية العلوم, جامعة بغداد, بغداد, العراق

الخلاصة

ان نظرية التشفير باستخدام المنحني الاهليجي قد لفتت انتباه الباحثين في السنوات الاخيرة, وولدت تطورات بسبب تركيبته الرياضيه المتينه و الامنية العاليه التي يمتلكها مقارنة بالخوارزميات الاخرى الموجودة حاليا على سبيل المثال خوارزمية ال RSA. ان نظرية التشفير باستخدام المنحني الاهليجي وجدت لزيادة الامنية عند استخدام نفس حجم المفتاح RSA اوتوفر نفس الامنية التي توفرها RSA ولكن بحجم اقل للمفتاح. في هذا البحث نطرح طريقة جديدة ومقترحة لتشفير الصور الرقمية باستخدام حساب جبر المنحني

*Email:dady_sniper92@yahoo.com

الاهليجي. الطريقة المقترحة تعمل على انشاء mask جديد يستخدم لتشفير الصورة عن طريق تطبيق هذا الmask على الصورة اعتمادا على جبر تشفير المنحني الاهليجي وتمتاز طريقة التشفير المقترحه كونها تطرح تشفيرالمنحني الاهليجي كنظام تشفير ذات المفتاح الواحد وليس نظام التشفير ذات المفتاحين. كما ان الطريقة الجديدة تجمع بين نظريتي الضغط والتشفير, طريقة الضغط المستخدمة في هذا البحث هي نظرية التحويل الموجي المتقطع المستخدمة لغرض تفكيك بيانات الصورة الى اربع حزم, ثم نشفر الجزء الذي يحمل اهم جزء من البيانات الموجودة في الصورة. تم اختبار الطريقة الجديد ة عن طريق تنفيذ عمليات التشفير وفك التشفير وكانت ذات كفاءة ومرونة ومشجعه.

1. Introduction

With advancements in Digital communication technology the information security takes place as an important role. Nowadays, information security is becoming more important in data storage and transmission. An increasing amount of information is being transmitted over the internet, including not only text but also audio, image, and other multimedia files.

The revolution of multimedia has been a driving force behind fast and secured data transmission techniques. Images are widely used in several processes; therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding. Image hiding or encrypting methods and algorithms range from simple spatial domain methods to more complicated and reliable frequency domain ones [1].

New smaller and faster security algorithms provide part of the solution, the elliptic curve cryptography ECC provide a faster alternative for public key cryptography. Much smaller key lengths are required with ECC to provides a desired level of security, which means faster key exchange, user authentication, signature generation and verification, in addition to smaller key storage needs. The terms elliptic curve cipher and elliptic curve cryptography refer to an existing generic cryptosystem which use numbers generated from an elliptic curve. Empirical evidence suggests that cryptosystems that utilize number derived from elliptic curve can be more secure. The security of ECC has not been proven but it is based on the difficulty of computing elliptic curve discrete logarithm in the elliptic curve group [2].

This paper produces new application for EEC work as symmetric cryptographic system by generate a new mask based on ECC algebra to encrypt the digital image by two proposed algorithms that make transfer process secure, faster and more efficient.

2. Previous researches

Some cryptographic algorithms have gained popularity due to properties that make them suitable for use in constrained environment like mobile information appliances, where computing resources and power availability are limited. One of these cryptosystems is Elliptic curve which requires less computational power, memory and communication bandwidth compared to other cryptosystem. A collection of papers related some of them [2].

1. [2] propose a system for "Proposed New Elliptic Curve Cryptography Protocol Based on Dictionary Techniques",This research proposed a new application for elliptic curve cryptosystem work as symmetric cryptographic system by investigate from dictionary techniques, a new protocol implemented to transfer secret massages between the sender and receiver using dictionary techniques for English text.
2. And in July 2011 [3] Propose a system for "Implementation of Elliptic Curve Cryptography on Text and Image", This research gives a brief background of key exchange and encryption/decryption using ECC. Then explain implementation of these algorithms on text documents.

3. Digital image

Digital images are composed of pixels (short for picture elements). Each pixel represents the color (or gray level for black and white photos) at a single point in the image, so a pixel is like a tiny dot of a particular color. Pixels are a little like grain particles in a conventional photographic image, but arranged in a regular

pattern of rows and columns and store information somewhat differently. A digital image is a rectangular array of pixels sometimes called a bitmap [4].

4. Discrete Wavelet Transform

The Discrete Wavelet Transform (DWT) is a popular tool in the field of image and video compression applications because of its multi-resolution representation capability [5].

The discrete wavelet transform uses filter banks for the construction of the multiresolution time-frequency plane. DWT uses multiresolution filter banks and special wavelet filters for the analysis and reconstruction of signals [6].

The Multiresolution Analysis (MRA) can be implemented with a two channel filter bank using quadrature mirror filters. The algorithm applies a one dimensional highpass and lowpass filtering step to both the rows and columns to the input image. Each filtering step is followed by subsampling which results in change in scale. Transforms in image processing are two-dimensional, so we need to implement a separable transform. When a two dimensional transform is separable, we can calculate it by applying the corresponding one dimensional transform to the column first, and then to the rows. At each decomposition level there are four different output images, an approximation of the input image and three detail images [7]. The information contained in the output subbands of the DWT are:

- LL coefficients which correspond to a lowpass filter to rows, followed by lowpass filter to columns.
- LH coefficients which correspond to a lowpass filter to rows, followed by highpass filter to columns.
- HL coefficients which correspond to a highpass filter to rows, followed by lowpass filter to columns.
- HH coefficients which correspond to a highpass filter to rows, followed by highpass filter to columns [7].

5. Image quantization

As illustrated in section 4, an image can be decomposed into approximate, horizontal, vertical and diagonal details. N levels of decomposition are done. After that, quantization is done on the decomposed image where different quantization may be done on different components [8].

The quantization of the DWT coefficients is done according to uniform scalar quantization characteristics. For the reconstruction, first the quantization is done then an inverse DWT is performed [6].

6. Elliptic Curve Cryptography

The use of Elliptic Curves for cryptography was discovered in 1985 by Victor Miller and Neil Koblitz. ECC is a public key mechanism that provides the same functionality as RSA schemes; their security is based on the hardness of the different problem namely discrete logarithm problem (DLP). This means that the desired security level can be attained with significantly smaller keys in elliptic curve systems than is possible with their RSA counterparts [9].

The mathematics used for ECC are considerably deeper and more difficult than mathematics used for conventional cryptography [10].

Elliptic curves combine number theory and algebraic geometry. These curves can be defined over any field of numbers (i.e., real, integer, complex) although we generally see them used over finite fields for applications in cryptography. An elliptic curve consists of the set of real numbers (x, y) that satisfies the equation:

$$y^2 \bmod p = (x^3 + ax + b) \bmod p \qquad (1)$$

The set of all of the solutions to the equation forms the elliptic curve. Changing *a* and *b* changes the shape of the curve [2]. The parameters *a* and *b* must satisfy the following condition[11].:

$$(4a^3 + 27b^2) \bmod P \neq 0 \bmod P \qquad (2)$$

Small changes in *a* and *b* parameters can result in major changes in the set of (x, y) solutions. Refered as $E_p(a,b)$. figure 1 shows the addition of two points on an elliptic curve. Elliptic curves have the interesting property that adding two points on the elliptic curve yields a third point on the curve [2].

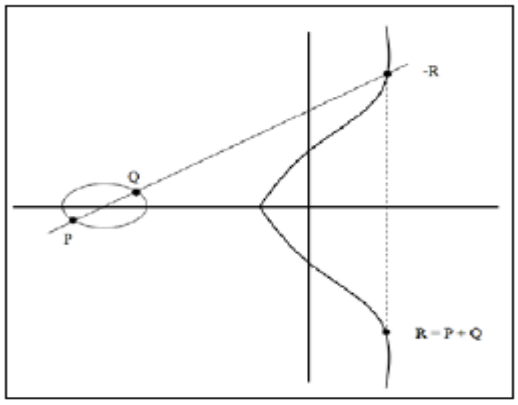


Figure 1- Elliptic curve addition.

6.1 Elliptic Curves over Z_P

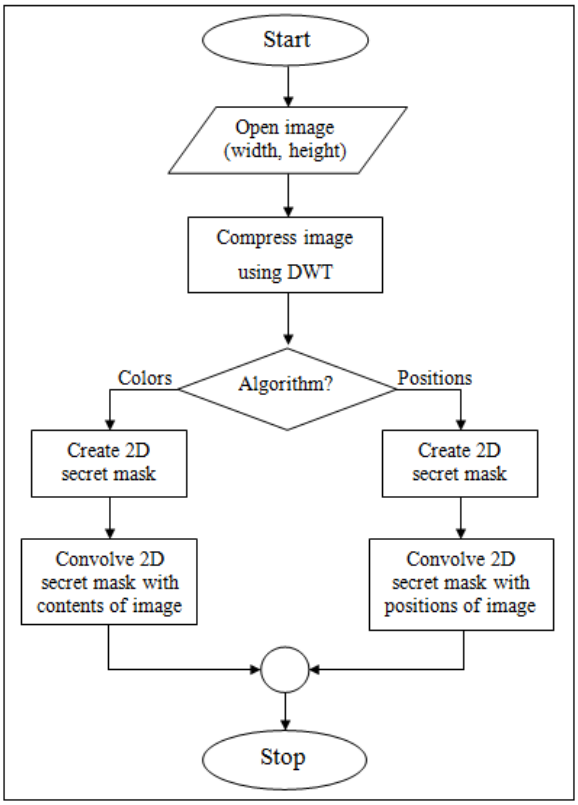
Elliptic curve cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field. Two families of elliptic curves are used in cryptographic applications: prime curves over Z_P (where p is the prime number) and binary curves over $GF(2^m)$. For a prime curve over Z_P, we use a cubic equation in which the variables and coefficients all take on values in the set of integers from 0 through p - 1 and in which calculations are performed modulo p. For a binary curve defined over $GF(2^m)$, the variables and coefficients all take on values in $GF(2^n)$ and in calculations are performed over $GF(2^n)$. Prime curves are best for software applications, because the extended bit-fiddling operations needed by binary curves are not required; and that binary curves are best for hardware applications, where it takes remarkably few logic gates to create a powerful, fast cryptosystem [11].

7. Partial Encryption (Selective Encryption)

The variety of applications for secure multimedia requires either full encryption or selective encryption. The goal of SE is to encrypt a well defined range of parameters or coefficients. Always, when considering image processing applications on such devices we should use minimal resources. However, the classical ciphers are usually too slow to be used for image and video processing in commercial low powered systems. The selective encryption (SE) can fulfill the application requirements without the overhead of the full encryption. In the case of SE, only the minimum necessary data are ciphered [12].

Multimedia communications often requires real-time data transmission, so tremendous image; audio and video data need to be transferred securely. Given that all multimedia data are encrypted, this will consume a great deal of overhead, so that multimedia data is difficult to transmit timely and the quality of communication cannot be guaranteed. Under such circumstances, the design of a selective encryption algorithm with less processing time but with relatively high security level is extremely significant [13].

8. The block diagram of the proposed approach



9. The proposed approach algorithm

The arithmetic of Elliptic curve algebra used in this paper for encrypting pixel's position (x,y) or pixel's value of image. First selecting prime number and apply the EC equation for creating the curve resulting in group of point as ordered pair that will be used as secret key (2D secret mask), then apply the arithmetic of EC algebra between the secret key and the points of image, this operation will done on portion of this points in image after the compression process. The decryption operation is done by applying the

same arithmetic of EC algebra between the encrypted points of image and inverse only the y-coordinate of the points in the secret key as (x,-y). The process of secrete key generation; encryption and decryption will be illustrated more accurately in the following proposed algorithm:

9.1 Generate the 2D secrete mask

The encryption key is 2D secret mask created by using the arithmetic of EC algebra over prime number according to the following conditions:

1. Choose prime number (prime number is an integer number that doesn't accept any division except on itself and 1).
2. Choosing the prime number depending on the type of the encryption process (encrypting image by positions, or encrypting image by colors). When the image encrypting by pixel's positions the prime number (P) will be chooses according to the size of image (width or height), the nearest prime number (the same, smaller or larger) to image's width or height. When the image encrypting by pixel's colors the prime number (P) will be chooses according to the color of the image (gray image, colored image (8-bpp), colored image (24-bpp), etc). While the image using in this work is BMP color image (24-bpp), the color content of each pixel is (Red, Green, and Blue) that is (0 to 255, 0 to 255, 0 to 255), each color to progress by steps to 256 values, so the nearest prime number to every maximum color value is (257).
3. Determine the size of the mask (number of rows and columns).
4. Create the 2D secret mask depending on the EC equation of generating the curve (rule 1), by taking all the numbers (from 0 to P-1), the numbers that satisfied (rule 1) will use to create an ordered pair from (x, y). Create many ordered pairs to fill the 2D secret mask.

9.1.1 Example

To simplify the process of creating the secret key according image encryption by position, assume image size (130 * 130), so the nearest prime number will be (P=131), suppose (a=1 and b=1) or any two numbers that satisfy the equation (2). The set of finite numbers that will be used in key generation (0 to p-1) = (0 to 130): Z_{131}={0,1,2,3,4,5,6,7,8,9,10,……,123,124,125,126,127,128,129,130}

Giving p=131, a=1, b=1 written as E_P (a, b) = E_{131} (1, 1). The result of this formula (y2 mod p = (x^3 + ax + b) mod p) appear in table 1.

Table 1- Create mask.

Z_{131}	Y^2 mod 131	(X^3 + X + 1) mod 131
0	0	1
1	1	3
2	4	11
3	9	31
4	16	69
5	25	0
6	36	92
7	49	89
8	64	128
9	81	84
10	100	94
11	121	33
12	13	38
.	.	
121	100	39
122	81	49
123	64	5
124	49	44
125	36	41
126	25	2
127	16	64
128	9	102
129	4	122
130	1	130

Matching all results of one formula to the results of another, when there is equal results take the original value (in Z_{131}) for each of them to create ordered pair as (x, y).The ordered pairs obtained from (P=131) is 127 pairs, some of the ordered pairs are:

(0,1), (0,130), (1,38), (1,93), (2,50), (2,81), (5,0), (7,58), (7,73), (9,52), (9,79), (10,15), (10,116), …… ,(124,100), (125,33), (125,98), (127,8), (127,123), (128,44), (128,87).

The number of ordered pairs different for every prime. Some of the ordered pairs will be chosen to fill the 2D secret mask, according the size of the 2D secret mask.

9.2 Algorithm One: Encrypt the compressed image by positions

The process of partial image encryption by position will be done after the compression process, then encrypting the LL subband of image. The process of encryption will be done by generating the secret key (2D secret mask) depending on the size of image. Partial encryption is a recent approach to reduce the computational requirements for huge volumes of images (computational requirement described in section 9.2.1). Here partial image encryption scheme will do using DWT with arithmetic of Elliptic Curve algebra. In this method, the approximation matrix (lowest frequency band) is encrypted as it holds most of the image's information. This process of decomposition usually repeated *n* times, and it is repeated just on the LL subband.

The implementation of the algorithm achieves high encryption rates. The steps of encrypt the image are described in figure (2, a), while the steps of reconstruct the original image are described in figure (2, b).

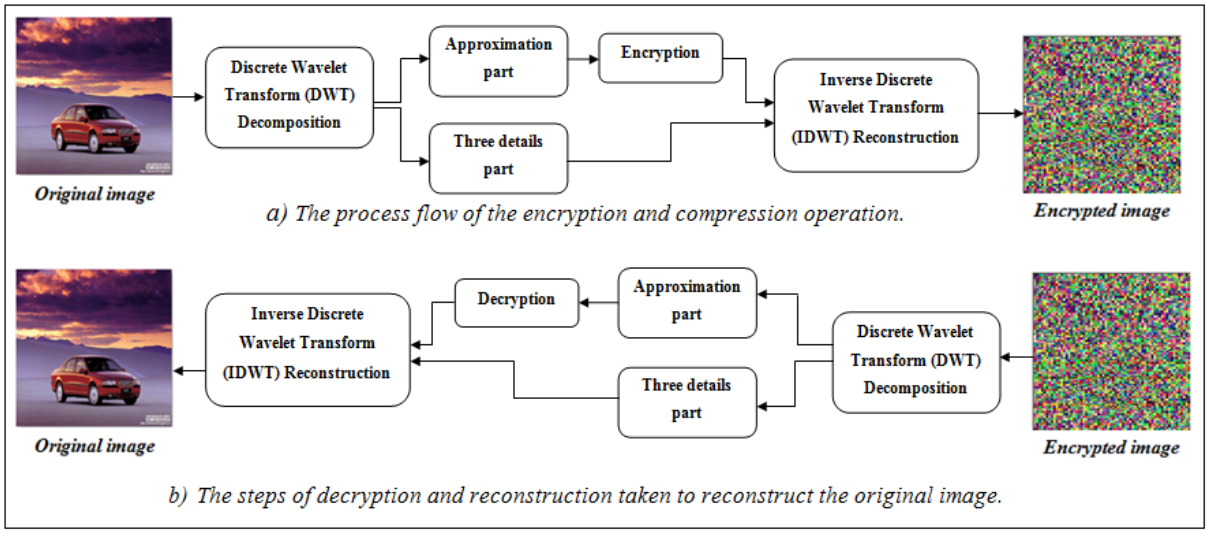


Figure 2- The partial encryption and decryption process.

In this algorithm bitmap image will be compressed using discrete wavelet transform. The compression process done by convolving the Haar filter with the original image to create four sub images (LL: LowLow subband, LH: LowHigh subband, HL: HighLow subband, and HH: HighHigh subband), these subbands created by passing Lowpass and Highpass of Haar filter along the image's rows and columns, and downsampling by 2 after each process, as illustrated in section 4. After the compression operation the process of encryption performed on the LL subband (most significant portion of image). To perform encryption by position first create the secret key by using the arithmetic of EC algebra then passing the 2D secret mask across all pixel's position in the LL subband and apply the EC algebra between the corresponding values (ordered pair from the 2D secret mask and the corresponding position in LL (x, y)). Reconstruct the subbands of image after encrypting the LL subband to get the encrypted image. In the decryption operation the same process will be done but with the inverse of the 2D secret mask values.

figure 3 describe the process of compressed image encryption by position using 2D secret mask (3*2); this mask has ordered pairs generated from prime number (67) using EC equation because the original image size is (257) and after two level of compression the size of LL subband will be (64).

9.2.1 Example

This example illustrates the process of sending and receiving stage for one point will be taken from image. The convolution operation will perform between point from 2D secret mask and point from image (position) based on the arithmetic of EC, these operations performed on all of the positions that will be encrypted.

• **Sending stage**

Suppose the size of image that will be encrypted (256 * 256), where for the second level of compression the size of LL subband will be (64*64), so the prime number will be (67). This example describe the process of encrypting (2, 0) position from image, by the corresponding ordered pair from 2D secret mask (5,8), as follows:

1. Find Lemda (λ),

$$\lambda = \left(\frac{YQ-Yp}{XQ-Xp}\right) \bmod \text{Prime} \quad \text{if} \quad P \neq Q$$

$$\lambda = \left(\frac{8-0}{5-2}\right) \bmod 67$$

$$\lambda = \left(\frac{8}{3}\right) \bmod 67$$

$\lambda = 25$

2. Find the new point using the arithmetic of EC, where $R(x_R, y_R)$ is the new point (encrypted point),

$x_R = (\lambda^2 - x_P - x_Q) \bmod \text{prime}$
$x_R = (25^2 - 2 - 5) \bmod 67$
$x_R = 15$
$y_R = (\lambda (x_P - x_R) - y_P) \bmod \text{prime}$
$y_R = (25*(2 - 15) - 0) \bmod 67$
$y_R = 10$

The convolution process based on arithmetic of EC for the point P=(2,0) and Q=(5,8) give the new point R=(15,10), so the point of image in position (2,0) will replaced by the point in position (15,10), figure 3 illustrate the convolution operation in the sending stage.

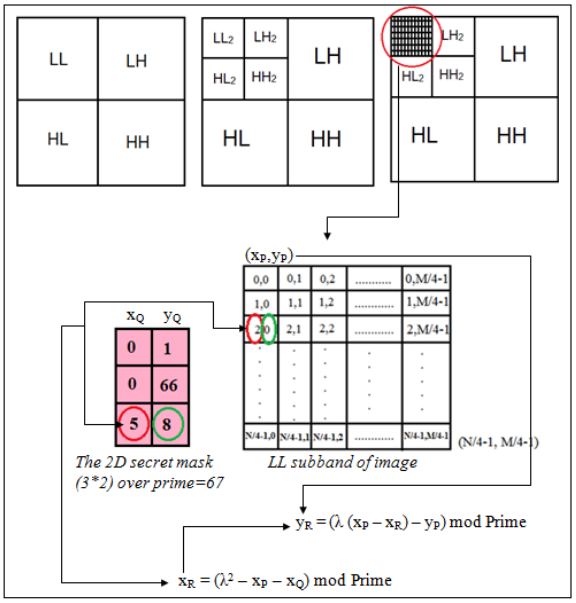


Figure 3- Encrypt compressed image by positions.

• **Receiving stage**

The original point encrypted in sending stage will be reconstructed using the encrypted point (R) and the inverse of the 2D secret mask (-Q) in the decryption process, where the inverse point of (5, 8) in the 2D secret mask is: (5, -8) = (5, -8 + 67) = (5, 59), this operation performed on all the ordered pairs of the 2D secret mask to get the inverse of 2D secret mask.

1. Find Lemda (λ),

$$\lambda = \left(\frac{YQ-Yp}{XQ-Xp}\right) \bmod \text{Prime} \quad \text{if} \quad P \neq Q$$

$$\lambda = \left(\frac{59-10}{5-15}\right) \bmod 67$$

$$\lambda = \left(\frac{49}{-10}\right) \bmod 67$$

$\lambda = 42$

2. Reconstruct the original point using the arithmetic of EC,

$x_P = (\lambda^2 - x_R - x_Q) \bmod \text{prime}$
$x_P = (42^2 - 15 - 5) \bmod 67$
$x_P = 2$
$y_P = (\lambda (x_R - x_P) - y_R) \bmod \text{prime}$
$y_P = (42*(15 - 2) - 10) \bmod 67$
$y_P = 0$

The convolution process based on the arithmetic of EC for the point (15,10) and –Q (5,59) gives the original point (2,0), so the point in the encrypted image in position (15,10) will replaced by the point in the position (2,0).

Algorithm One: Encrypt the compressed image by positions.
Input: Image, Haar filter, Prime number, a, b, size of mask.
Output: Encrypted image

Step 1: Open image and save the image size (width, height).
Step 2: Compress image by discrete wavelet transform method by passing Haar filter over the image to create compressed image with one approximation (LL subband) and three details (LH, HL, HH subbands).
Step 3: Perform the quantization process (multiply all the coefficients with a scalar).
Step 4: Create the 2D secret mask (encryption mask) from prime number based on the size of LL subband using Elliptic curve equation of generating the curve,

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

Step 5: Encrypt image by performing the convolution operation based on the Elliptic Curve arithmetic operation between the 2D secret mask (x_Q, y_Q) and the current pixel's position of LL subband (x_P, y_P),

$$x_R = (\lambda^2 - x_P - x_Q) \bmod p$$

$$y_R = (\lambda (x_P - x_R) - y_p) \bmod p$$

Step 6: Passing the mask to next positions.
Step 7: If Width and Height of LL subband of image larger than the current position the operation performed on then goes to step 5.
Step 8: Reconstruct all subbands of image (encrypted LL, LH, HL, HH).
Step 9: End.

9.3 Algorithm Two: Encrypt the compressed image by colors

The process of partial image encryption by color will be done after the compression process, then encrypting the LL subband of image. The process of encryption will be done by generating the secret key (2D secret mask) depending on the color model of image. Creating the 2D secret mask from prime number using EC equation of generating the curve, the prime number (P) will be chosen according to the color model of image (gray image, colored image (8-bpp), colored image (24-bpp), etc), while the image using in this work is BMP image (24-bpp), the content of each pixel is (Red, Green, and Blue) that is (0 to 255, 0 to 255, 0 to 255) each color to progress by steps to 256 values, so the nearest prime number to each component is (257).
Passing the secret key along the pixel's content of LL subband only two component from the pixel's content must be used because there is only two encryption component for every entity in the 2D secret mask (x, y), therefore the third component will leave as it is, while the image used in this work is bitmap image, so the encrypted color will be Red and Green, Green and Blue, or Red and Blue.
Reconstruct the subbands of image after encryption process of the LL subband to get the encrypted image.
figure 4 describe the process of image encryption by color with 2D secret mask (3*2), the numbers in the 2D secret mask represent ordered pairs generated from the prime number (257) using EC equation.

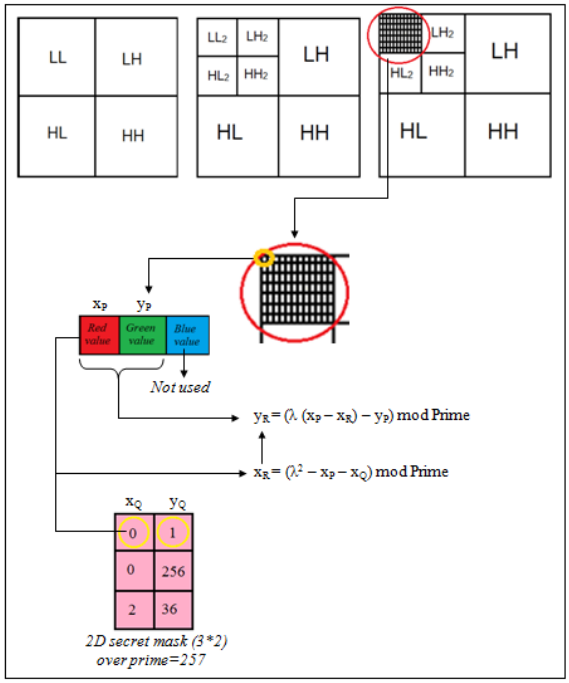


Figure 4- Encrypt compressed image by colors.

Algorithm Two: Encrypt the compressed image by colors.
Input: Image, Haar filter, Prime number, a, b, size of mask.
Output: Encrypted image

Process:
Step 1: Open image and save image size (width, height).
Step 2: Create the 2D secret mask (encryption mask) from the prime number based on Elliptic Curve equation of generating the curve,
$y^2 \bmod p = (x^3 + ax + b) \bmod p$
Step 3: Compress image using discrete wavelet transform method by passing Haar filter over the image to create compressed image with one approximation (LL subband) and three details (LH, HL, HH subbands).
Step 4: Perform the quantization process (multiply all the coefficients by a scalar).
Step 5: Split LL subband of image to three color components (Red, Green, Blue),
pixel = point from image.
Red = pixel mod 256
Green = ((pixel And &HFF00FF00)/256)
Blue =((pixel And &HFF00000)/65536)
Step 6: Encrypt image by performing the convolution process based on the Elliptic Curve arithmetic operation between the 2D secret mask (x_Q, y_Q) and two components from the LL subband of the current pixel's content (Red (x_P), Green (y_P)).
Step 7: Passing the mask to next positions.
Step 8: If Width and Height of LL subband of image larger than the current position the operation performed on then goes to step 6.
Step 9: Reconstruct all subbands of image (encrypted LL, LH, HL, HH).
Step 10: End.

9.4 Implementations the proposed algorithms

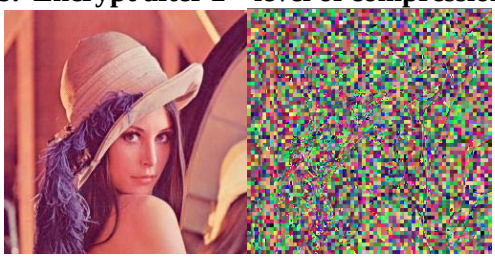
In this section the implementation of the proposed algorithms will be illustrated on the BMP compressed images (first level, second level, third level, fourth level, and fifth level of decomposition) respectively, the compression type used here is discrete wavelet transform (DWT).

1. Encrypt the compressed image by positions

a. Encrypt after 1st level of compression

Original image *Encrypted image*
*Image size 256*256* *prime=131*
*Size of mask =17*2*

b. Encrypt after 2nd level of compression



Original image *Encrypted image*
*Image size 256*256* *prime= 67*
*Size of mask =7*2*

c. Encrypt after 3rd level of compression

Original image *Encrypted image*
*Image size 256*256* *prime= 33*
*Size of mask =23*2*

d. Encrypt after 4th level of compression

Original image *Encrypted image*
*Image size 256*256* *prime= 17*
*Size of mask =7*2*

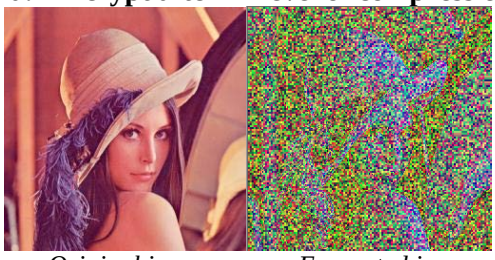
e. Encrypt after 5th level of compression

Original image
*Image size 256*256*

Encrypted image
prime= 13
*Size of mask =17*2*

2. Encrypt the compressed image by colors

a. Encrypt after 1st level of compression



Original image
*Image size 256*256*

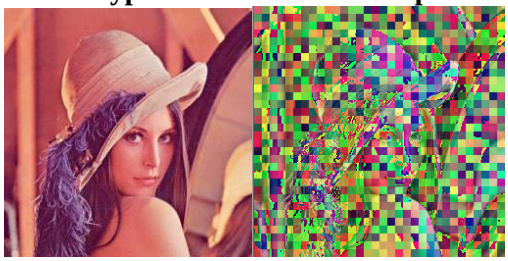
Encrypted image
prime=257
*Size of mask =17*2*

b. Encrypt after 2nd level of compression

Original image
*Image size 256*256*

Encrypted image
prime=257
*Size of mask =17*2*

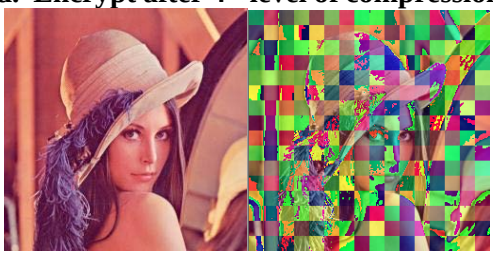
c. Encrypt after 3rd level of compression



Original image
*Image size 256*256*

Encrypted image
prime=257
*Size of mask =17*2*

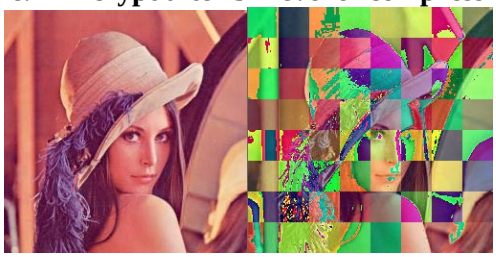
d. Encrypt after 4th level of compression



Original image
*Image size 256*256*

Encrypted image
prime=257
*Size of mask =17*2*

e. Encrypt after 5th level of compression



Original image
*Image size 256*256*

Encrypted image
prime=257
*Size of mask =17*2*

10. Experimental Results Test

In order to determine the proposed approach to generate 2D secret key succeed to conceal pure image information and in the same time the deciphered image can reconstructed the original image without missing any information. The measures use to achieve this test are:-

$$MSE = \frac{1}{H * W} \sum_{y=0}^{H-1} \sum_{x=0}^{W-1} (f(x,y) - f'(x,y))^2 \qquad (3)$$

$$SNR = \frac{\sum_{y=0}^{H-1}\sum_{x=0}^{W-1}(f(x,y))^2}{\sum_{y=0}^{H-1}\sum_{x=0}^{W-1}(f(x,y) - f'(x,y))^2} \text{ dB} \qquad (4)$$

$$PSNR = 10\log_{10}\left(\frac{(255)^2}{MSE}\right) \text{dB} \qquad (5)$$

Where f(x,y) is the value of the original image at row(y) and column(x), f'(x,y) is the corresponding values of ciphered image, and H,

W are height and width of the image respectively. MSE is the mean square error [14]

$$Similarity(A_{ij}, B_{ij}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} a_{ij} b_{ij}}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N} a_{ij}^2}\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N} b_{ij}^2}} \quad (6)$$

Where aij, bij is two images matrices of size (N×N) [15].

From the results of the measures that were used to test the ciphered images that show in tables (2,3,4,5,6,7,8,9,10 and 11) we can obtain the following:-

1. The large results of MSE (Mean Square Error) such as the results in the tables below mean that proposed key is succeeded to conceal pure image information (i.e. there are large errors in ciphered image caused by the use of partial cryptography using EC algebra) [16].
2. The small results of SNR (Signal to Noise Ratio) and PSNR (Peak Signal to Noise Ratio) mean the proposed key caused large noise (i.e. small result implies better image concealment of original image) [17].
3. The similarity measure shows the amount of correlation between the original image and ciphered image and the result from this test is acceptable.

Table 2- The test results for encrypting LL subband of image's positions after first compression level.

Criteria Name	*MSE*			*SNR*			*PSNR*			*Similarity*		
	Red	*Green*	*Blue*	*Red*	*Green*	*Blue*	*Red*	*Green*	*Blue*	*Red*	*Green*	*Blue*
Lina	10337.56	8549.99	3251.97	3.35	1.45	3.29	7.98	8.81	13.009	0.83	0.76	0.86

Table 3- The test results for encrypting LL subband of image's positions after second compression level.

Criteria Name	*MSE*			*SNR*			*PSNR*			*Similarity*		
	Red	*Green*	*Blue*	*Red*	*Green*	*Blue*	*Red*	*Green*	*Blue*	*Red*	*Green*	*Blue*
Lina	9587.93	8111.65	3645.45	3.62	1.53	2.93	8.31	9.03	12.51	0.85	0.77	0.85

Table 4- The test results for encrypting LL subband of image's positions after third compression level.

Criteria Name	*MSE*			*SNR*			*PSNR*			*Similarity*		
	Red	*Green*	*Blue*	*Red*	*Green*	*Blue*	*Red*	*Green*	*Blue*	*Red*	*Green*	*Blue*
Lina	9867.91	8256.14	3152.04	3.518	1.504	3.39	8.18	8.96	13.14	0.84	0.77	0.87

Table 5- The test results for encrypting LL subband of image's positions after fourth compression level.

Criteria Name	*MSE*			*SNR*			*PSNR*			*Similarity*		
	Red	*Green*	*Blue*	*Red*	*Green*	*Blue*	*Red*	*Green*	*Blue*	*Red*	*Green*	*Blue*
Lina	8655.97	7608.61	3496.53	4.011	1.63	3.06	8.75	9.31	12.69	0.86	0.78	0.87

Table 6- The test results for encrypting LL subband of image's positions after fifth compression level.

Criteria Name	*MSE*			*SNR*			*PSNR*			*Similarity*		
	Red	*Green*	*Blue*	*Red*	*Green*	*Blue*	*Red*	*Green*	*Blue*	*Red*	*Green*	*Blue*
Lina	10020.06	7662.37	10655.16	3.46	1.62	1.005	8.12	9.28	7.85	0.84	0.78	0.71

Table 7- The test results for encrypting LL subband of two color component (Red and Green) after first compression level.

Criteria Name	MSE			SNR			PSNR			Similarity		
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Lina	10731.64	9059.68	107.72	3.23	1.37	99.38	7.82	8.55	27.808	0.83	0.76	0.99

Table 8- The test results for encrypting LL subband of two color component (Red and Green) after second compression level.

Criteria Name	MSE			SNR			PSNR			Similarity		
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Lina	10194.84	8995.78	113.93	3.405	1.38	93.97	8.04	8.59	27.56	0.84	0.76	0.99

Table 9- The test results for encrypting LL subband of two color component (Red and Green) after third compression level.

Criteria Name	MSE			SNR			PSNR			Similarity		
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Lina	9937.07	9099.33	119.24	3.49	1.36	89.78	8.15	8.54	27.36	0.84	0.77	0.99

Table 10- The test results for encrypting LL subband of two color component (Red and Green) after fourth compression level.

Criteria Name	MSE			SNR			PSNR			Similarity		
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Lina	10084.12	9670.27	114.22	3.44	1.28	93.73	8.09	8.27	27.55	0.84	0.75	0.99

Table 11- The test results for encrypting LL subband of two color component (Red and Green) after fifth compression level.

Criteria Name	MSE			SNR			PSNR			Similarity		
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Lina	8916.58	8127.02	112	3.89	1.52	95.59	8.62	9.03	27.63	0.86	0.79	0.99

11. Discussion

When comparing the results of each approach for five compression level, the following will be obtained:

a) There are small differences between the results from first level through fifth level compression of the encrypted image by positions, but the best results and tests appear after first level compression
b) The differences between the results from first level through fifth level compression of the encrypted image by colors also small, but the best results and tests appear after first level compression.
c) There is very small effect when changing the size of the mask and this is clear in the above results and images.

12. Conclusions

From the new partial cryptography of digital image using the arithmetic of EC algebra, we reached to the following conclusions:-

a. Encrypt small portion of the digital image after the compression process will reduce the computational overhead and reduce consuming time for encryption.
b. Using the arithmetic of EC to create 2D secret mask.

c. Using the arithmetic of EC algebra to perform the encryption process.
d. The proposed approach succeeds to produce EC as one key cryptosystem instead of two key cryptosystem.
e. The proposed approach be more efficient when the prime number nearby the image dimensions (width and height), and color components.
f. The proposed approach be more secure with different values for a, b.
g. Increasing the level of compression will decrease the encryption rate (decrease the number of encrypted pixels in image) because only LL subband of image will encrypted, this is produce less security, so the first level is the best level for creating encrypted image with high security level.

References

.

1. Sasidharan S., Philip D.S., **2011.** A Fast Partial Image Encryption Scheme with Wavelet Transform and RC4. *International Journal of Advances in Engineering & Technology*, India. Vol. 77 No 2.
2. Abdul Wahab H. B., Rahma A.M. S., **2012.** Proposed New Elliptic Curve Cryptography Protocol Based on Dictionary Techniques. *European Journal of Scientific Research Publishing*,. Vol. 1, Issue 4.
3. Kolhekar M., Jadhav A., **2011.** Implementation of Elliptic Curve Cryptography on Text and Image. *International Journal of Enterprise Computing and Business Systems.*V:1,Issue 2.
4. Jonathan Sachs, **1999.** Digital Image Basics. [online] Available http:// www.dl-c.com/basics.pdf,p:1.
5. Islam A., **2010.** *Hardware Implementation of Daubechies Wavelet Transforms using Folded AIQ Mapping.* Thesis, M.Sc, University of Saskatchewan, Canada.
6. Merry R.J.E., **2005.** *Wavelet Theory and Applications a literature study*. Eindhoven University of Technology. pages 22.
7. Mohammad Ayache, Mohamad Khalil and Francois Tranquart, **2011.** Artificial Neural Network for Transfer Function Placental Development: DCT and DWT Approach. *International Journal of Computer Science Issues*, Vol. 8. Issue 5, No 3, pages 22.
8. Myung-Sin Song, **1991.** Wavelet Image Compression, *Mathematics Subject Classification.*,p:2.
9. Samant Khajuria, Henrik Tang, **2009.** Implementation of Diffie-Hellman Key Exchange on Wireless Sensor Using Elliptic Curve Cryptography. *IEEE*, Copenhagen University College of Engineering & Aalborg University, Denmark.,p:772.
10. Kimmo Järvinen, **2003.** Elliptic Curve Cryptography on FPGAs. Helsinki University of Technology, *Signal Processing Laboratory*, Finland.,p:30.
11. William Stallings, **2005.** *Cryptography and Network Security Principles and Practices*. Fourth Edition,Prentice Hall.
12. Lala Krikor, Sami Baba, Thawar Arif, Zyad Shaaban, **2009.** Image Encryption Using DCT and Stream Cipher. Faculty of Information Technology, Applied Science University, Jordan, *Euro Journals Publishing.*, Vol.32, No.1, p: 48.
13. Priyanka Agrawal, Manisha Rajpoot, **2012.** Partial Encryption Algorithm for Secure Transmission of Multimedia Messages. *International Journal of Computer Science and Technology*, Dept of CSE, India, Vol. 3. Issue 1, p: 467.
14. S. E. Ghrare, M. A. M. Ali, M. Ismail, K. Jumari, **2008.** The Effect of Image Data Compression on the Clinical Information Quality of Compressed Computed Tomography Images for Teleradiology Applications. *European Journal of Scientific Research Publishing.*,no.1,p 7.
15. Raghad Z. Y. Al-Macdici, Dr.Muzhir S. M. Al-Ani, **2001.** Modified Large-Scal Randomization Key-Stream Generator for Digital Image Encryption. *Second National Conference on Computer, Communication and Control Engineering.*
16. Ikhlas Khalaf Alsaadi, **2005.** *Lossless Wavelet Based Image Comparession With Hybird 2D Decomposition*. M.Sc. Thesis, University of Technology at Computer Science.
17. S. Poobal, and G. Ravindran, **2011**. The Performance of Fractal Image Compression on Different Imaging Modalities Using Objective Quality Measures, *International Journal of Engineering Science and Technology (IJEST)*, India, Vol. 3 No. 1, p 527.