Selective Image Encryption Based On Chaotic Maps And Elliptic Curve Cryptography

Ali Soleymani (ali.soleymani@iranian.ac.ir)
Iranians University an e-Institute of Higher Education
Md Jan Nordin
Universiti Kebangsaan Malaysia (UKM)

Research Article

Keywords: Image, Encryption, Decryption, Selective, Chaotic, Elliptic Curve Cryptography

Posted Date: May 21st, 2021

DOI: https://doi.org/10.21203/rs.3.rs-509136/v1

SELECTIVE IMAGE ENCRYPTION BASED ON CHAOTIC MAPS AND ELLIPTIC CURVE CRYPTOGRAPHY

Ali Soleymani $^{\text{(Corresponding Author)}}$

ali.soleymani@iranian.ac.ir

Iranians University an e-Institute of Higher Education, Tehran, Iran

Md Jan Nordin

jan@ukm.edu.my

Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia

ABSTRACT

The rapid evolution of imaging and communication technologies has transformed images into a widespread data type. Different types of data, such as medical information, official correspondence or governmental and military documents saved and transmitted in the form of images over public networks. Cryptography is a solution to protect confidential images by encrypting before transmission over unsecure channels. Most of the current image encryption methods based on symmetric cryptosystems, which the encryption and the decryption keys are the same and will be shared. However, asymmetric cryptosystems are more useful and secure because of the decryption key kept secret. This paper will focus on asymmetric image encryption algorithms to improve and enhance the security of transmission. Elliptic Curve Cryptography (ECC) is a new public key cryptosystem and provides equivalent security with shorter key length, low mathematical complexity and more computationally efficient rather than RSA. Selective encryption is a solution to decrease the consumed time for asymmetric cryptosystems, which reduce the encryption regions as small as possible. Hence, a hybrid cryptosystem is proposed based on the combination of ECC and chaotic maps that detects the face(s) in an image and encrypt the selected regions. This scheme will encrypt around five percent of the whole image and only confidential regions rather than whole image. The results of security analysis demonstrate the strength of the proposed cryptosystem against statistical, brute force and differential attacks. The evaluated running time for both encryption and decryption processes guarantee that the cryptosystem can work effectively in real-time applications.

Keywords: Image, Encryption, Decryption, Selective, Chaotic, Elliptic Curve Cryptography

1. INTRODUCTION

Images have become a common data type due to the rapid expansion of imaging and communication technology. Wide variety of media, such as personal medical information, official communication, or governmental and military documents, are stored and sent as images across public networks. Cryptography is a method of protecting secret photos by encrypting an image before transmission over unsecure networks. Many image encryption methods are proposed based on private pre-shared key for ciphering, which use the same key for encryption and the decryption. However, asymmetric cryptosystems are more useful and secure because of the decryption key kept secret. In some applications a secure channel could not be established to transmit the private key or prefer to keep the decryption key secret, hence public key cryptography is applied. This paper will focus on asymmetric image encryption algorithms to improve and enhance the security of transmission. Elliptic Curve

Cryptography (ECC) is a new public key cryptosystem and provides equivalent security with shorter key length, low mathematical complexity and more computationally efficient rather than RSA. This paper will focus on asymmetric image encryption algorithms to improve and enhance the security of transmission. Selective encryption is a solution to decrease the consumed time for asymmetric cryptosystems, which reduce the encryption regions as small as possible. Hence, a hybrid cryptosystem is proposed based on the combination of ECC and chaotic maps that detects the face(s) in an image and encrypt the selected regions. This scheme will encrypt around five percent of the whole image and only confidential regions rather than whole image. The results of security analysis demonstrate the strength of the proposed cryptosystem against statistical, brute force and differential attacks. The evaluated running time for both encryption and decryption processes guarantee that the cryptosystem can work effectively in real-time applications.

Digital Images are pervasive due to the advanced of imaging technology. High-resolution cameras take pictures in a range of megapixels in personal, medical and official applications. Image encryption is a solution for securing images that transmitted over public and unsecure channels. In some applications, particularly in military and medical images, applying encryption is necessary. However, encrypting whole image is not needed. For instance, an image that contains picture of criminals or intelligence services staff may only need to encrypt the faces parts. This object-based approach will minimize the secret part as much as possible to reduce the required time for encryption and decryption process. Another approach is in partial encryption which applied on entire image but in case of frequency and spatial domain. In spatial domain selective encryption, only a few bits of every pixel in an image encrypted. In frequency domain, an image is transferred into frequency space and only high frequencies that contain more information about the image are encrypted. The selective encryption that is proposed in this paper focused on the spatial domain category. A face detection algorithm scans the input image to find and locate the human face(s). The proposed hybrid encryption algorithm in this paper is a combination of binary grouping approach and a chaotic scheme. ECC is deployed for more security as a public key cryptosystem and chaotic scheme results in more diffusion and confusion. This technique is applied to three different images containing some human faces. Finally, each encrypted face is analyzed particularly for statistical attacks.

Partial or selective encryption which also known as perceptual ciphering is a method for not encrypting the full image. The true objective is to minimize computation times for real-time applications. The main purpose is to divide the image content into two parts: public and protected. Minimizing the protected region in an image is the main feature in selective encryption.

Digital Images are massive due to advanced imaging technology. High-resolution cameras take pictures in range of megapixels in personal, medical and official applications. Image encryption is a solution for securing images transmitted over public and unsecure channels. In some applications, particularly in military and medical images, applying encryption is mandatory, but encrypting the whole image is not compulsory. For instance, an image that contains picture of criminals or intelligent staff only the face parts of the image may need to be encrypted. This object-based approach will minimize the secret part as much as possible to reduce the required time for encryption and decryption process. Another approach in partial encryption is applied on an entire image but in case of frequency and spatial domain. In spatial domain selective encryption, only a few bits of every pixel in an image are encrypted. In frequency domain, an image is transferred to frequency space and only high frequency that contains more information about the image encrypted.

According to table 1, selective encryption usually comes with compression. In frequency domain, low frequency coefficients carry most information of the image and high frequency coefficients carry the details1. In lossy compression techniques, such as JPEG standard, an image is transformed into a frequency domain by DCT, and then zeros multiply some high frequency coefficients and the new compressed image is reconstructed. Hence only some low frequency coefficients are encrypted rather than all in frequency domain which also has many advantages2: (1) It is easier to identify the critical parts to be encrypted and (2) It is easier to identify what parts of the data are not compressible.

One of the first studies on selective multimedia encryption3 was done by proposing Aegis mechanism based on MPEG video transmission and DES cryptosystem to secure MPEG video sequences from unauthorized access. By employing proposed video compression technique, this approach reduces the quantity of data that must be encrypted and decrypted. This is due to reducing the size of transmitted video images by encrypting intra I-frames of an MPEG stream. However, Agi & Gong4 found that this and some other methods are not suitable for sensitive applications and may not be sufficiently secure for some types of video and one can see pattern of movements. Therefore, they tried to improve the security by increasing the I-frame frequency but it results in the increase of bandwidth consumption and higher computational complexity. An alternative way is to encrypt I-blocks in all frames rather that I-frames which enhance confidentiality.

Droogenbroeck & Benedett5 also proposed two techniques for selective encryption of both compressed and uncompressed images. Considering randomness pattern of 4 or 5 least significant bits of pixels value, it is more difficult to attack on plaintext. Another partial ciphering method declared in this paper is based on compressed JPEG images and encrypts a particular amount of AC coefficients. Results of execution time on three different encryption algorithms (DES, 3-DES and IDEA) show that real-time processing is quite possible. Another technique for real-time applications proposed by Droogenbroeck6. In his suggested algorithm, for each DCT block it encrypts corresponding bits to a selected number of AC coefficients. Finally, he concluded that this scheme provides flexibility, multiplicity, spatial selectivity and format compliance. A multilevel partial image encryption (MPIE) was proposed by Odibat et al.7 which applies the encryption prior to compression. Low frequency coefficients which determined by Haar Wavelet are encrypted and the approximation coefficients are transformed by DFT. The output of transformation is then permuted using a permutation matrix as an encryption key, and ultimately compressed using Huffman coding. Despite the algorithm's drawbacks, such as its complexity, poor compression rate, and high time consumption, it has certain advantages, such as security and flexibility in modifications and compression of image.

Another different approach in partial image encryption is to extract some special and secret features in an image and encrypt these features rather than encrypting the whole image. An idea in this scope is to detect faces of input image and encrypt them, for some applications such as transmission of images with criminals or members of security organizations and military applications.

A high-speed chaotic image encryption scheme for all types of images such a color, gray-scale and binary8. The plain image is splitting into blocks and after computing the correlation coefficient value of the blocks, the proposed technique is determining whether a block should be encrypted or not. SKWE tent map is performed to generating random values and XORing with the pixel values. TD-ERCS map is applied to generating random vectors to achieve confusion regarding row and column shuffling respectively. The proposed scheme is resilient against different types of attacks while the encryption time is less than9 and10.

A partial encryption method proposed using the face region as a feature because a face has semantic information and is the most important part in an image or video11. They used Multi-Layer Perceptron to detect face region and for higher precision, Gaussian skin-color was applied to discriminate between skin regions and non-skin regions. Both DES and AES encryption algorithms were compared and results show that encryption time is less for DES. According to experiments, for video content encryption, full encryption methods provide two or three frames per second whereas their proposed method encrypts 25 to 30 frames per seconds. A different scheme by Rodrigues et al.12 for selective encryption in video was also offered for face protection based on AES stream cipher for JPEG image sequences by performing three steps on DCT blocks. The steps are construction of plain text, ciphering the plain text and substitution of the original Huffman's vector with the ciphered information. This scheme provides advantages such as portability, constant bit rate and selective encryption of the region of interest and does not affect the JPEG compression rate at all, which makes it useful for a large range of applications with good information confidentiality results.

Table 1. Different categories of selective encryption and related works

Spatial Domain		**Frequency Domain**		
Region Based	**Bit Based**	**DFT**	**DCT**	**DWT**
Rodrigues et al.[12]	Bhatnagar et al.[13]	Abuhaiba & Hassan[14]	Droogenbroeck & Benedett[5]	Ghaffari et al.[15]
Rodrigues et al.[16]	Moon et al.[17]	Sharma et al.[18]	Emir Dirik & Memon[19]	Taneja et al.[20]
Hong & Jung[11]	Podesser et al.[21]	Ashutosh & Sharma[22]	Xingyuan Wang & Yining Su[23]	Bao et al.[24]
Naik et al.[25]	Zhenjun Tang et al.[26]	Nguyen et al.[27]	Abdmouldeh et al.[28]	Khalifa et al.[29]

2. ENCRYPTION SCHEME

Figure 1 shows the encryption process architecture. This scheme is a combination of region and bit based on selective encryption. The purpose is to utilize elliptic curve cryptography, and, to propose a novel asymmetric image encryption scheme. Due to complexity and computational characteristics of the public key cryptography, encryption parts are minimized as small as possible to achieve an efficient encrypting time with considered security. In this paper, a hybrid selective image encryption is proposed based on ECC and chaotic maps.

In this scheme, the input image, which consists of human face(s) is preprocessed to detect the face(s). Pixels of all selected region(s) are then integrated to create a uniform matrix. After changing these pixel values to binary format, four bits in high significant position are encrypted with elliptic curve cryptography and other bits kept unchanged. Finally, all bits are permuted *r* rounds to achieve more diffusion and confusion in the encrypted parts.

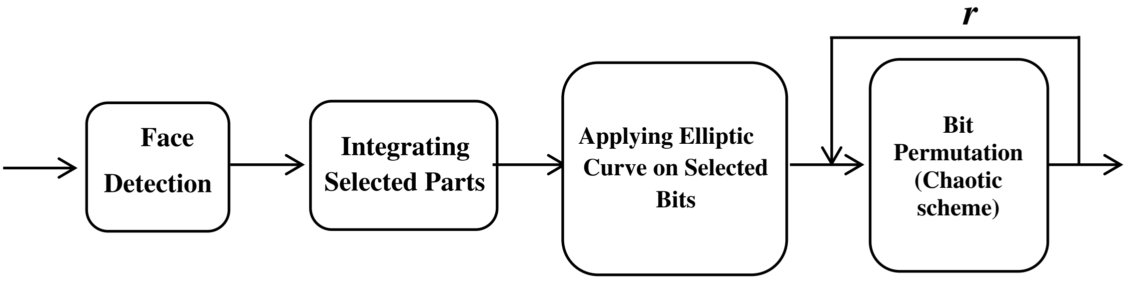

r
Face Detection
Integrating Selected Parts
Applying Elliptic Curve on Selected Bits
Bit Permutation (Chaotic scheme)

Figure 1. Architecture of encryption for securing selected regions (faces)

A. FACE DETECTION

The main purpose in this scheme is to restrict the secret regions as small as possible to reduce the consumed time for encryption and decryption. A raw image that may contain some human faces processed to detect all faces in it and return bounding box values. The output of the face detection function is an array such as shown in (1) which *n* is the number of detected faces, (x_i, y_i) is the coordinate of top-left corner, H_i and W_i are height and width of the i^{th} detected face in pixels. Face detection in this work is based on Viola-Jones object detection30 . They proposed a fast detection framework with high successful detection rate. This framework is implemented by three major phases that are feature extraction, classification and multi-scale detection algorithm.

$$detected\_Faces = \begin{bmatrix} x_1 & y_1 & H_1 & W_1 \\ x_2 & y_2 & H_2 & W_2 \\ & & \vdots & \\ x_n & y_n & H_n & W_n \end{bmatrix} \quad (1)$$

B. INTEGRATING SELECTED REGIONS

After detecting faces in the previous phase, selected regions should be integrated to have an array of all selected pixels before encryption. All pixels in i^{th} region is scanned column by column as shown in figure 2 and stored in an array. This process is done for all regions and pixels arranged in the form of (2). The total number of selected pixels is calculated by (3) where *n* is the number of detected faces. Subsequent step in this phase is converting the array of integrated pixels into binary format. Each pixel has an 8-bit value between 0 and 255 in the form of (4) where *b(8)* is the most and *b(1)* is the least significant bit. Number of rows of created array (5) is equal to the total number of selected pixels and 8 columns with elements of 0 and 1.

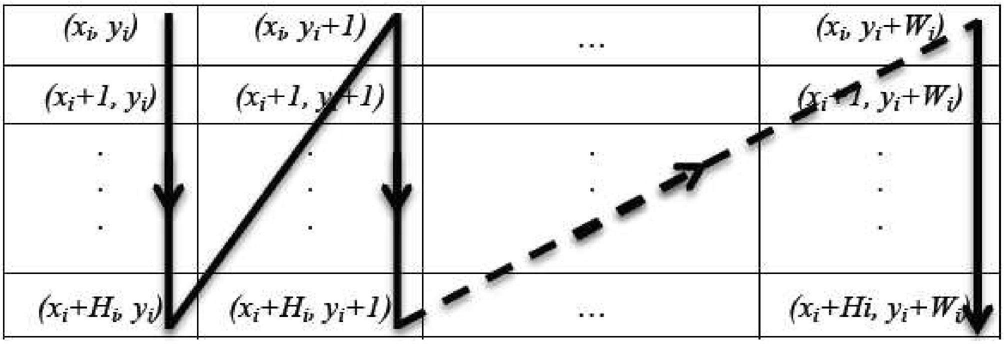


Figure 2. Scanning model for selected pixels

$$\boldsymbol{integrated\,pixels} = \begin{bmatrix} img(x_1.y_1) \\ img(x_1+1.y_1) \\ \vdots \\ img(x_i.y_i) \\ img(x_{i+1}.y_i) \\ \vdots \\ img(x_i+H_i.y_i+W_i) \\ \vdots \\ img(x_n.y_n) \\ \vdots \\ img(x_n+H_n-1.y_n+W_n) \\ img(x_n+H_n.y_n+W_n) \end{bmatrix} \qquad (2)$$

$$\boldsymbol{total\_pix} = \sum_{i=1}^{n} (H_i \times W_i) \qquad (3)$$

$$\boldsymbol{pix} = b(8)b(7)\ldots b(1) \qquad (4)$$

$$\boldsymbol{Bin\_pix} = \begin{bmatrix} b_1(8)b_1(7)\ldots b_1(1) \\ b_2(8)b_2(7)\ldots b_2(1) \\ \vdots \\ b_{total\_pix-1}(8)\ldots b_{total\_pix-1}(1) \\ b_{total\_pix}(8)\ldots b_{total\_pix}(1) \end{bmatrix} \qquad (5)$$

A bit in a pixel's value carries amount of information according to its position. Based on the Shannon theory, the information ratio of bit *b(i)* in a pixel is calculated by (6). These values for all *b(i)* positions are given in table 2 in percentage31. As shown in the table, the bits in positions 5 to 8 carry 94.125 percent of information. Therefore, encrypting these four bits rather than whole 8-bits will reduce the encryption time.

$$p(i) = \frac{2^{i-1}}{\sum_{i=1}^{8} 2^{i-1}} \qquad (6)$$

Table 2. Information ratio of bits in a pixel

Bit position in a pixel	Percentage of i^{th} bit information
1	0.3922
2	0.7843
3	1.5686
4	3.137
5	6.275
6	12.55
7	25.10
8	50.20

C. ELLIPTIC CURVE CRYPTOGRAPHY

In ECC-Based cryptosystems, mapping plain message to the points on the curve is a challenge. Different techniques are proposed for converting a message whether it is a text or an image. In order to map plaintext *m* to the point *(x, y)* on the curve, Koblitz proposed his method32. Having a plaintext *m,* in equation (6.7), j is incremented to find the first *x* which results a square *f(x)* in (6.8) and if it satisfied the equation (6.9), *(x, y)* is the corresponded point to plaintext *m.*

$$x = mk + j \quad 0 \le j < k \qquad (7)$$
$$f(x) = (x^3 + ax + b) \ mod\, p \qquad (8)$$
$$y^2 \ mod\, p = f(x) \qquad (9)$$

Li et al. utilized Koblitz method to propose an additive homomorphic encryption scheme based on EC-ElGamal33. This scheme is applied for sharing secret images over unsecured networks.

The current work is a combination of Li et al.33 and the proposed scheme in section 2 to propose a novel hybrid selective public key scheme which provides both security, speed and efficient encryption which reduce the consumed time for encryption and decryption process. The proposed encryption technique is a combination of elliptic curve and chaos-based cryptography, which will be applied on selected regions and bits to reduce the encryption time while profit the advantages of asymmetric cryptography.

Some standard parameters of elliptic curve cryptography are defined by NIST for governmental applications. These parameters are a and b coefficients, p as a large prime number and $G = (Gx, Gy)$ as base point. Parameters are classified by key-length and p in bits. For instance, standard parameters of *curve P-192* are shown in table 3.

Table 3. Standard Parameters of curve *P-192*

p	Decimal	6277101735386680763835789423207666416083908700390324961279
	Hex	fffffffffffffffffffffffffffffffeffffffffffffffff
a	Decimal	6277101735386680763835789423207666416083908700390324961276
	Hex	fffffffffffffffffffffffffffffffefffffffffffffffc
b	Decimal	2455155546008943817740293915197451784769108058161191238065
	Hex	64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1
G_x	Decimal	602046282375688656758213480587526111916698976636884684818
	Hex	188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012
G_y	Decimal	174050332293622031404857552280219410364023488927386650641
	Hex	07192b95ffc8da78631011ed6b24cdd573f977a11e794811

In this scheme, ECC is applied on four higher significant bits $(b_i(8)\ b_i(7)\ b_i(6)\ b_i(5))$ of selected regions rather than whole bits of pixels. This is because of the amount of information they carry. Such as explained in table 1, these four bits carry 94.125% of overall information of a pixel that is the meaningful information about the image. The four remain bits have pseudo-random distribution and discarded in encryption.

Selecting bits is depended on the chosen standard curve for encrypting an image. For instance, if *curve P-192* is selected for cryptography, all bits classified are in groups of 191 bits or encryption. In addition, 191 is considered as *m* in equation (7) to find the appropriate *x* that satisfies (8) and compute *y*. In this case, the result is a point which *x* and *y* are 192-bit. Hence, the encrypted part is larger than the original in size. The number of extra bits is equal to the number of groups and has an inverse relation with the key length.

In this scheme, the encrypted file size is larger than original image. This is because selected bits classified in 191-bits but the encrypted points are 192-bits. Hence, the extra bits are equal to the number of groups.

D. BIT PERMUTATION

According to the previous phase, ECC is performed only on the 4-bits of pixels [b(8)b(7)b(6)b(5)] that carry 94.125% of information and the 4-bits with less information kept unchanged. These bits have a random distribution. As calculated for different image, the entropy of the bits is very near to 4. But for more diffusion and confusion, all bits are shuffled after performing ECC.

Here, a novel approach is proposed for bit permutation. Unlike similar works that proposed bit permutation, which is applicable only on square images with equivalent height and width, the proposed scheme is working on any size of images. Since in partial encryption, the selected regions may not be square in form, hence such a bit permutation scheme is needed. In this scheme, all selected pixels are arranged in an array in one column and converted to its binary format. Therefore, an array of zeroes and ones with *total_pix* (from equation 3) rows and 8 columns is created. Figure 3 shows the sliding window model. Permutation is then performed on the 8×8-bits windows based on Arnold cat map. After permuting the first window, it slides down one row and permuting in new position. This process is continued to meet the last row and total number of permutation is equal to *total_pix-7* because at this row, it is not possible to move down the sliding any more.

Henon map34 is the simplified form of Lorenz model35, a two-dimensional discrete dynamic system, and defined by (10). The generated *x_i* and *y_i* by equation (10) are utilized as parameters for p and q to be use in Arnold map, respectively. Since, Henon iterations generate real coordinates, equations (11) and (12) are applying modular, multiply, absolute and floor functions to convert *x_i* and *y_i* to integers.

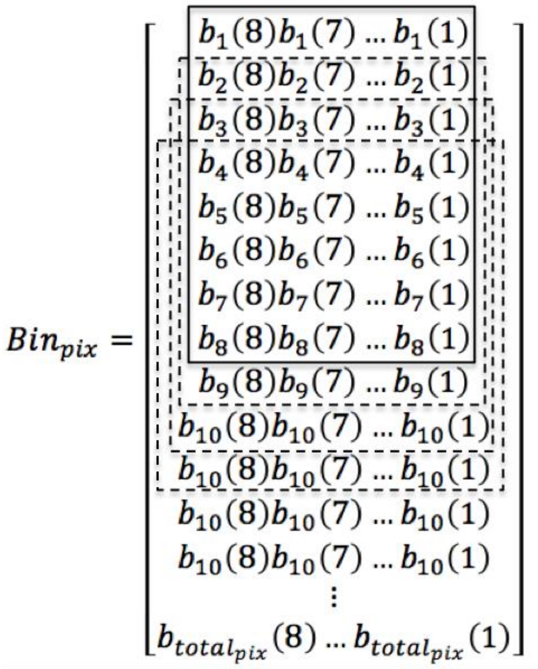

$Bin_{pix} =$
$b_1(8)b_1(7) \dots b_1(1)$
$b_2(8)b_2(7) \dots b_2(1)$
$b_3(8)b_3(7) \dots b_3(1)$
$b_4(8)b_4(7) \dots b_4(1)$
$b_5(8)b_5(7) \dots b_5(1)$
$b_6(8)b_6(7) \dots b_6(1)$
$b_7(8)b_7(7) \dots b_7(1)$
$b_8(8)b_8(7) \dots b_8(1)$
$b_9(8)b_9(7) \dots b_9(1)$
$b_{10}(8)b_{10}(7) \dots b_{10}(1)$
$b_{10}(8)b_{10}(7) \dots b_{10}(1)$
$b_{10}(8)b_{10}(7) \dots b_{10}(1)$
$b_{10}(8)b_{10}(7) \dots b_{10}(1)$
$\vdots$
$b_{total_{pix}}(8) \dots b_{total_{pix}}(1)$

Figure 3. Sliding window model

The Arnold cat map is an area preserving and reversible 2D transformation that maps a point *(x, y)* to the new position *(x', y')* by (13). This equation is applied in the encryption phase. The reverse operation by (14) is applied in decryption phase to map the result into the original position and reconstruct the input image. ACM is a periodicity transformation and mapped points are return to their initial position after finite iterations. To prevent such an undesirable reconstruction, permutation parameters are pseudo-random and different for each window and they are generated by Henon map.

$$x_{i+1} = y_{i+1} + 1 - \alpha x_i^2 \qquad (10)$$

$$y_{i+1} = \beta x_i$$

$$p_i = abs(\lfloor x_{100+i} \times 10^{14} \rfloor)\ mod\ \ \delta \quad . \quad i = 1. \dots . total\_pix - 7 \qquad (11)$$

$$q_i = abs(\lfloor y_{100+i} \times 10^{14} \rfloor) mod\ \ \vartheta \quad . \quad i = 1. \dots . total\_pix - 7 \qquad (12)$$

$$\Gamma\text{:} \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod\ n \qquad (13)$$

$$\Gamma'\text{:} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} pq+1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} mod\ n \qquad (14)$$

E. DECRYPTION SCHEME

Figure 4 shows the decryption architecture process. This scheme performs the reverse steps of encryption process to decrypt the ciphered regions in the received image. A matrix of all encrypted pixels is created at first step to integrate all encrypted regions. The last step was the bit permutation in the encryption process. The created matrix of encrypted pixels converted to binary values in order to perform inverse bit permutation. For inverse bit permutation process, the reverse ACM is performed on the binary matrix and 8×8 sliding window is moving from bottom to top one by one. After permuting the last eight rows, it is moving up one row. This process is continued to meet the first row and total number of permutation is equal to *total_pix-7.* The decryption process of the encrypted points on the elliptic curve is the next step, which applies the equation to decrypt the encrypted points. According to Koblitz method33, after decryption, the decrypted points should be converted into image pixels. The parameter k in equation (15) is used to transform each point to its corresponding pixels value.

$$m = [x/k] \tag{15}$$

While m is the combination of selected bits of pixels in binary mode, they should be split and reconstructed in four-bit groups and replaced with four higher significant bits of pixels.

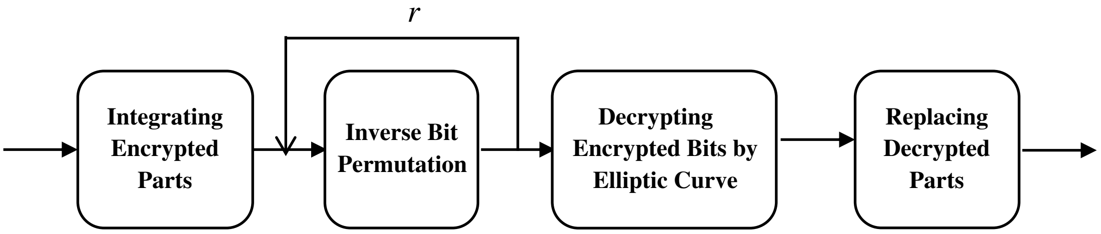

r
Integrating Encrypted Parts
Inverse Bit Permutation
Decrypting Encrypted Bits by Elliptic Curve
Replacing Decrypted Parts

Figure 4. Architecture of decryption process

3. IMPLEMENTATION AND ANALYSIS

i. Initialization

Experiments are performed on figure 5, which includes human faces. At first step, all faces in plain image are detected. According to the mentioned technique in section 2, the matrix of detected faces is generated in the form of table 3 and the selected regions are demonstrated in figure 6 by squares. In table 4, $(x_{i,1}, y_{i,1})$ is the coordinate of the top-left corner and $(x_{i,2}, y_{i,2})$ is the coordinate of the bottom-right corner of the square which covered a face. H and W is the height and width of the selected region in pixel and the last column is the number of the pixels in each selected face. The plain image resolution is 194×259, which means that it consists of 50246 pixels. After performing face detection step, selected regions have 2402 pixels totally, which is less than 5 percent of the whole image. Hence, more than 95 percent of the plain image pixels do not carry any critical information and it is not required to encrypt it. This aspect will result in fast and efficient encryption. Elliptic curve parameters chosen according to table 3 and chaos maps are initialized base on parameter values in table 4. After performing the encryption process on the selected faces, the encrypted faces are demonstrated in figure 7.

Table 4. Initial values for chaos maps

Parameter	Initial Value
α	1.4
β	0.3
δ	12345
r	1
ϑ	67890
x_0	1.211
y_0	0.361

Table 5. Coordinates and size of detected faces

Face #	$x_{i,1}$	$y_{i,1}$	$x_{i,2}$	$y_{i,2}$	H_i	W_i	*No. of pixels*
1	198	42	221	65	24	24	576
2	88	50	111	73	24	24	576
3	144	62	166	84	23	23	529
4	45	64	67	87	23	23	529

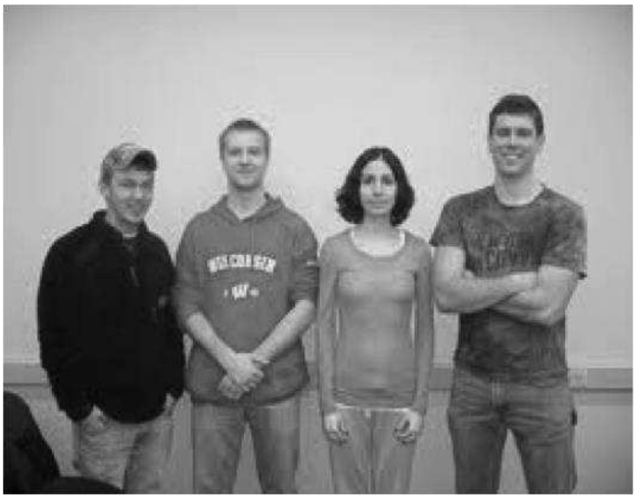


Figure 5. Plain image

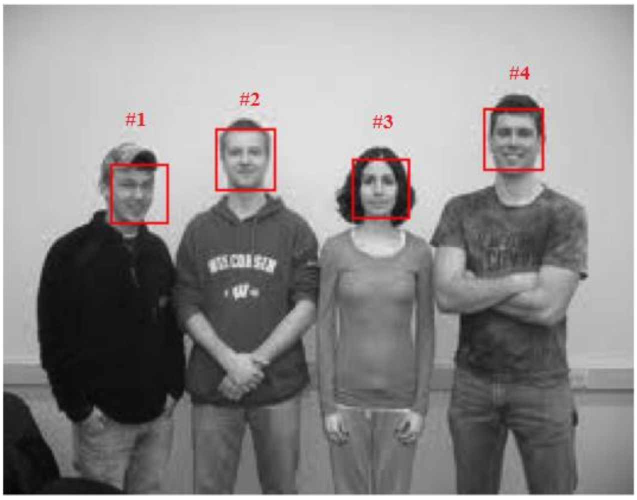


Figure 6. Detected faces

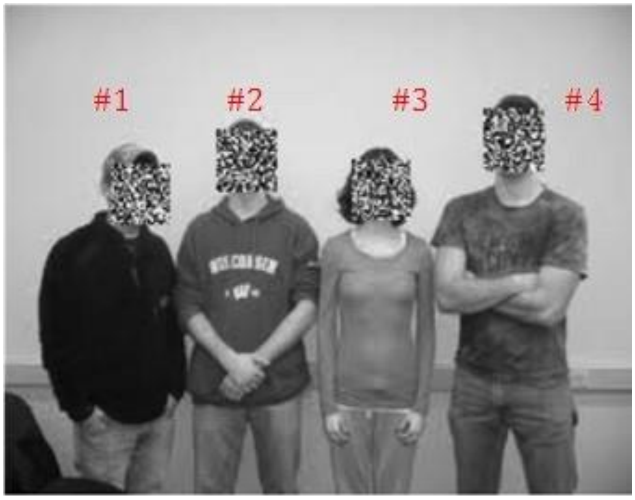
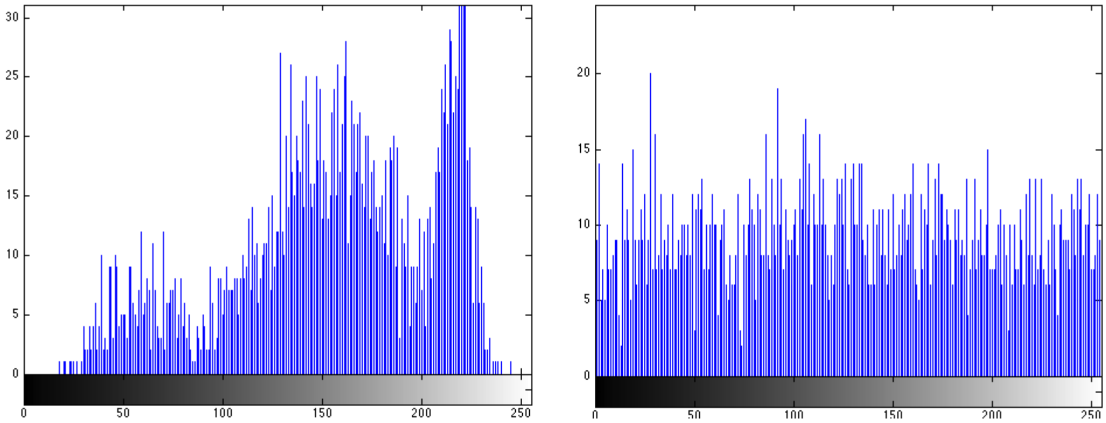


Figure 7. Encrypted Faces

ii. Histogram Analysis

Histogram of the selected integrated faces is drawn before and after encryption in figure 8. For better comparison and analyzing the result, histogram of all faces are demonstrated in figure 9 before and after encryption, separately for each of the selected region. Histograms are not uniform. This is due to the limitation of pixels' numbers but it is completely different with the plain face. Due to the natural characteristics of color and intensity of lighter human skin, most of the pixel intensity values are more than 128 and cumulated at the right side of histogram. Actually in the third histogram which is related to the woman's in the picture, as one can see, some pixels in the selected region are referring to her hair and this is the cause of difference in the histogram. So there is a cumulative of pixels in the bound of 20 to 70.



(a) (b)

Figure 8. Histogram of integrated selected pixels (a) Before and (b) After encryption

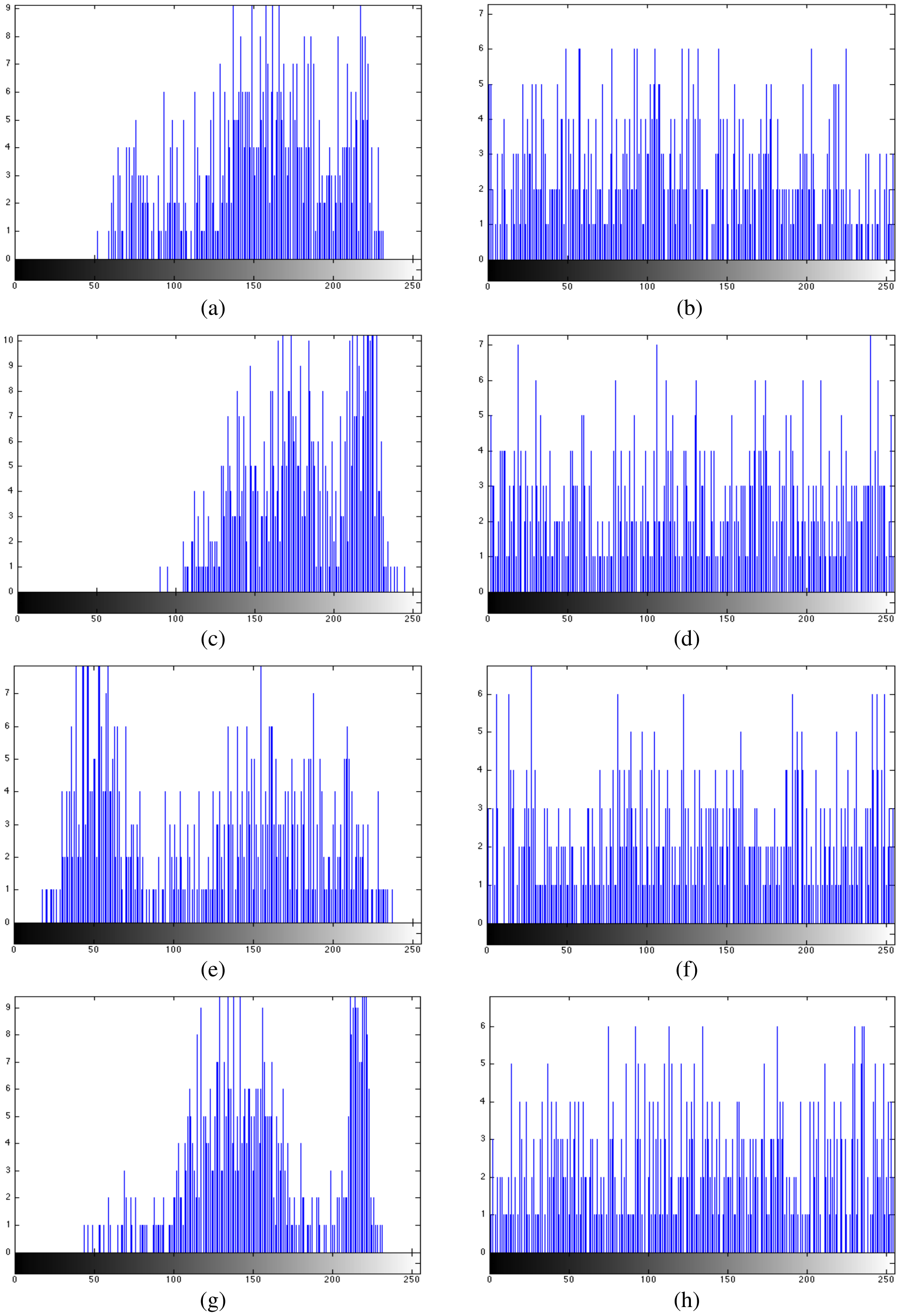

(a)
(b)
(c)
(d)
(e)
(f)
(g)
(h)

Figure 9. Histogram of selected faces #1 (a), #2 (c), #3 (e) and #4 (g) in plain image and histogram of selected faces #1 (b), #2 (d), #3 (f) and #4 (h) after encryption, respectively.

iii. Image Entropy

Entropy is measured to determine the randomness of encrypted image. According to Shannon theory36, entropy for a secure image encryption algorithm should have the value of very close to 8. Calculated entropy by (16) for selected faces before and after encryption is shown in table 5. The entropy value for each face is not ideal because it is not close to eight. This is because of the pixels' number, which according to table 5 is few for each face. However, for total selected pixels, it is almost eight. In fact, the calculated results in table 6 proved that the entropy for cipher faces increased. It results to increase the randomness in distribution of the pixel values.

$$entropy = \sum_{i=0}^{n} P_i \log_2 P_i \tag{16}$$

Table 6. Entropy values for plain faces and ciphered faces

Face	Plain Entropy	Cipher entropy
#1	7.0426	7.6612
#2	6.7247	7.6162
#3	6.8215	7.6142
#4	7.2897	7.6105
Integrated Pixels of Faces	7.4052	7.9215

iv. Key Space

In the brute-force attack, an intruder may attempt to find decryption key by trying all combinations of secret values to find the private key. A sufficiently large key space will make the try-an-error method too long and impossible. In the proposed cryptosystem, initial point *(x_0, y_0)* of the Henon map and control parameters are *δ, ϑ, p, q* and *r* should be kept secret and be used as secret keys. In addition, with these values, *x* and *k* are private keys of the sender in elliptic curve cryptography. The combination of these numerous values will provide a large key space of approximately 2^{560} that is sufficient to make the brute-force attack infeasible37. Table 7 is the maximum length for each variable.

Table 7. Secret parameters length in bit

Parameter	Length (bit)
x	*192*
k	*192*
r	*10*
δ	*24*
ϑ	*24*
x_0	*64*
y_0	*64*

Another image containing faces for analyzing cryptosystem is shown in figure 10. It contains four faces, which has higher resolution than figure 5. This image is 600×450 pixel in height and width. Selected area for faces and encrypted faces is shown in figure 11 and 12, respectively.

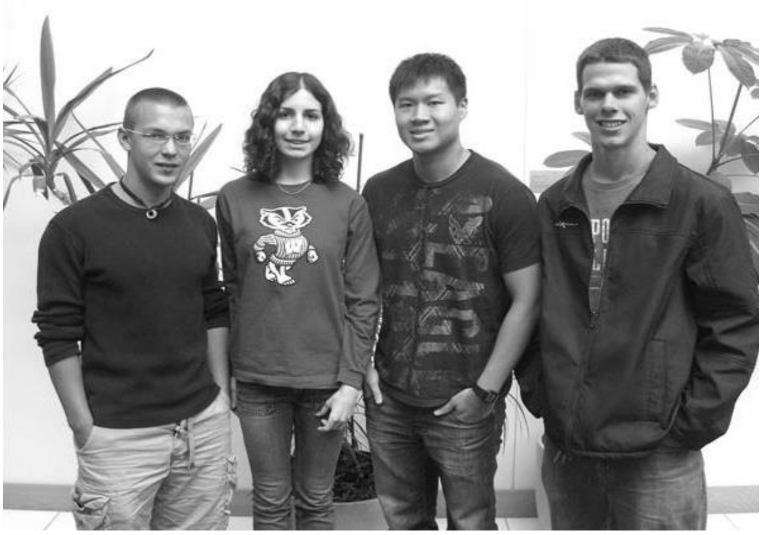


Figure 10. Plain image

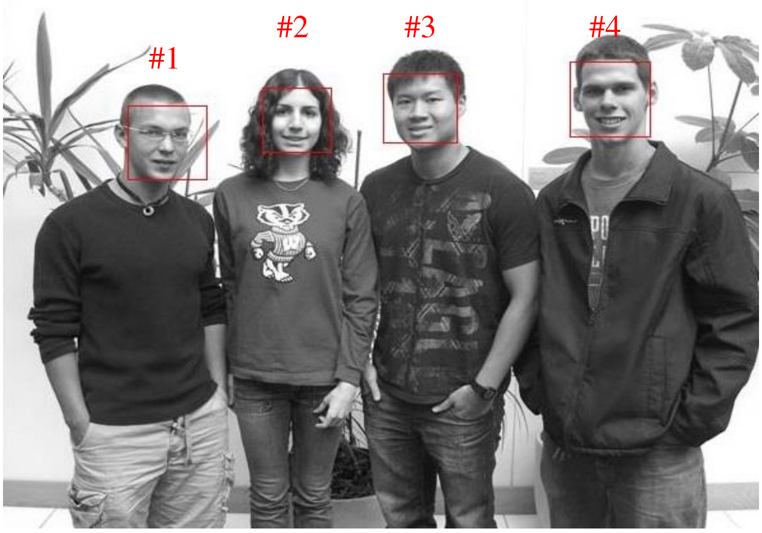


Figure 11. Detected faces

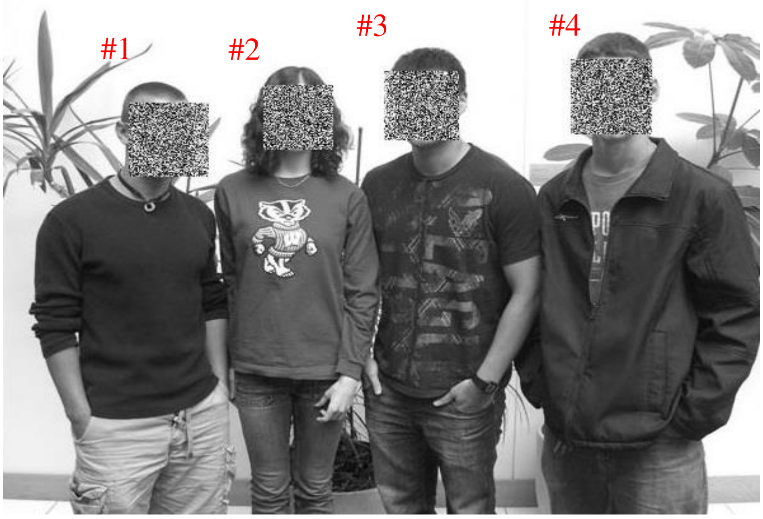


Figure 12. Encrypted faces

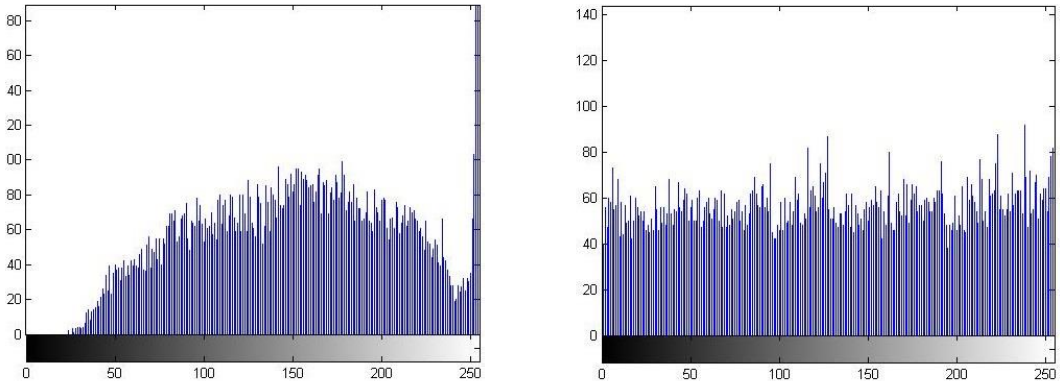
Security analysis is performed on encrypted faces in figure 12. Analysis on several images is necessary to evaluate the strength of a cryptosystem and rely on the results. Total pixels of this test image are 600×450=27000. After applying face detection on the image, coordinates of the selected faces are listed in table

8. Adding all the values in the last column, the result will be 14571, which is the total number of pixels of the selected faces. It is almost 6.4 percent of the whole image.

Table 8. Coordinates and size of detected faces

Face #	$x_{i,1}$	$y_{i,1}$	$x_{i,2}$	$y_{i,2}$	H_i	W_i	**No. of Pixels**
1	208	79	262	133	55	55	3025
2	450	57	513	120	64	64	4096
3	303	67	361	125	59	59	3481
4	102	94	164	156	63	63	3969

Figure 13 illustrates the histogram of selected integrated pixels before and after encryption. The non-uniform distribution histogram of plain faces has changed to a uniform histogram. Calculated entropy values for integrated pixels, each plain face, and its corresponding cipher face individually are shown in table 9.



(a) (b)

Figure 13. Histogram of integrated selected pixels (a) before and (b) after encryption.

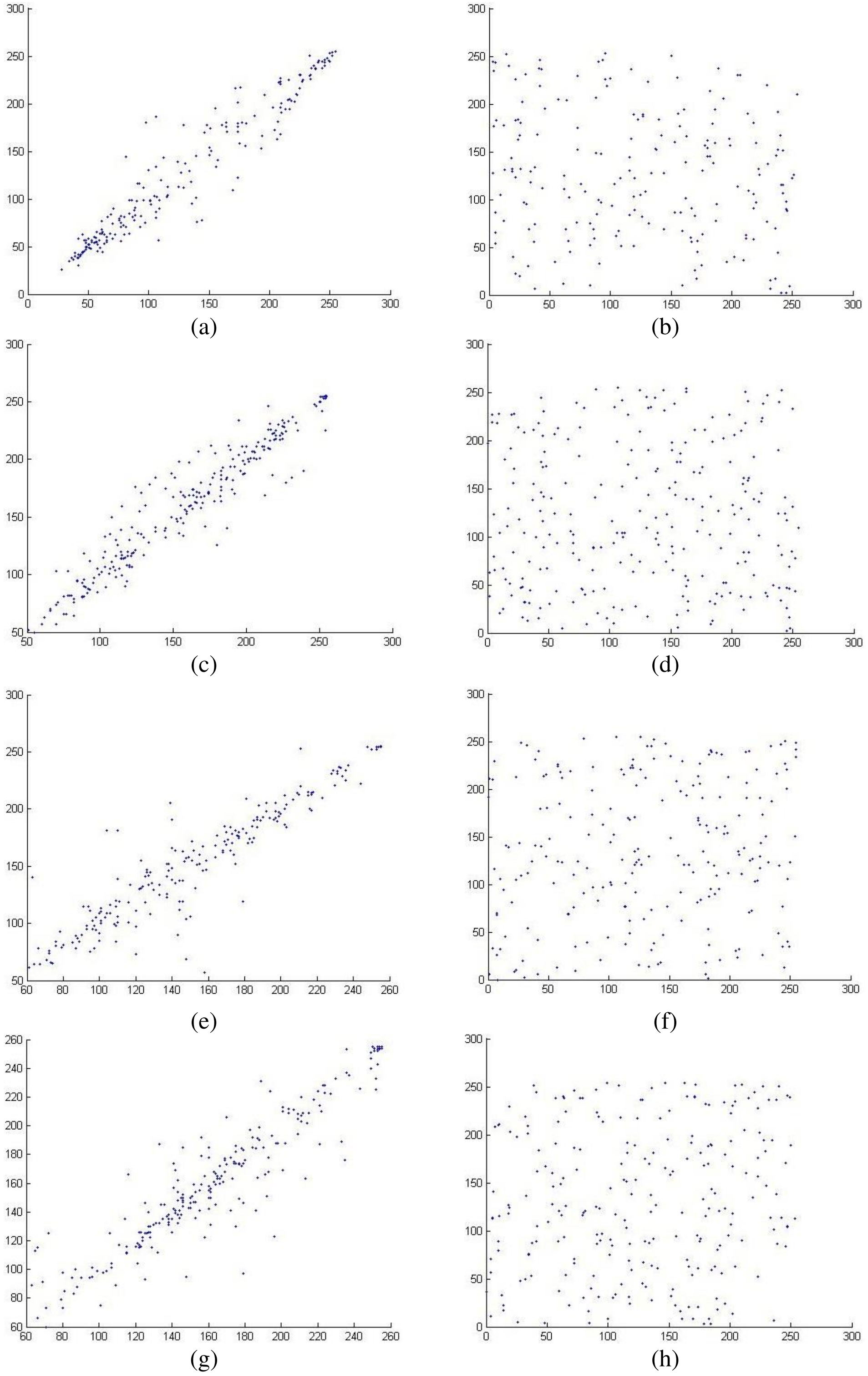
Table 9. Entropy values for plain faces and ciphered faces

Face	Plain Entropy	Cipher entropy
#1	7.6704	7.9514
#2	7.4322	7.9490
#3	7.2803	7.9395
#4	7.2172	7.9371
Integrated Pixels of Faces	7.5880	7.9823

In table 10, correlation values calculated for each face before and after encryption. Related plots for horizontal correlations and histograms are demonstrated in figure 14 and 15, respectively.

Table 10. Correlation values for plain faces and ciphered faces

Face	**Plain Face Correlations**			**Cipher Face Correlations**		
	HC	**VC**	**DC**	**HC**	**VC**	**DC**
#1	0.9469	0.9597	0.9136	0.0092	-0.1576	0.0062
#2	0.9298	0.9599	0.9002	-0.0484	-0.0003	-0.0009
#3	0.9593	0.9473	0.9196	0.0166	0.1270	0.0426
#4	0.9288	0.9333	0.8613	0.0358	0.1227	0.1170



(a) (b)

(c) (d)

(e) (f)

(g) (h)

Figure 14. Horizontal correlation for plain faces #1 (a), #2 (c), #3 (e) and #4 (g) and encrypted faces #1 (b), #2 (d), #3 (f) and #4 (h)

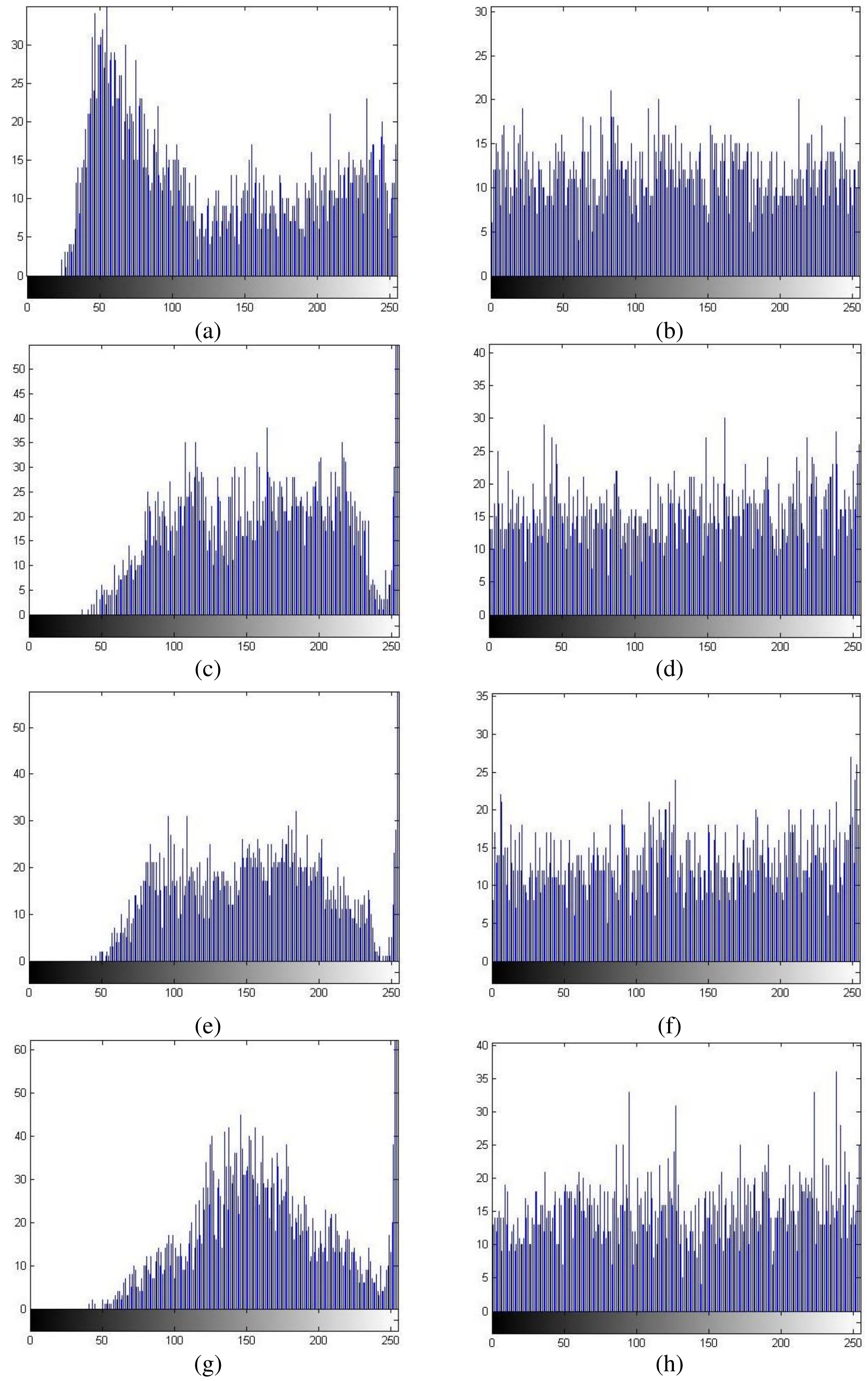


Figure 15. (a) Histogram of selected faces #1, (b) #2, (d) #3, (e) and #4, in (f) plain image and encrypted faces #1, (g) #2, (h) #3 and (h) and #4.

Lena is another image that tested and analyzed. This image is selected to compare the running time with two other works that encrypt the whole image. Visual results are shown in figure 16. The entropy values before and after encryption are 7.3652 and 7.9757, respectively. As it was expected, a uniform histogram and a high entropy value are achieved for encrypted face of Lena.

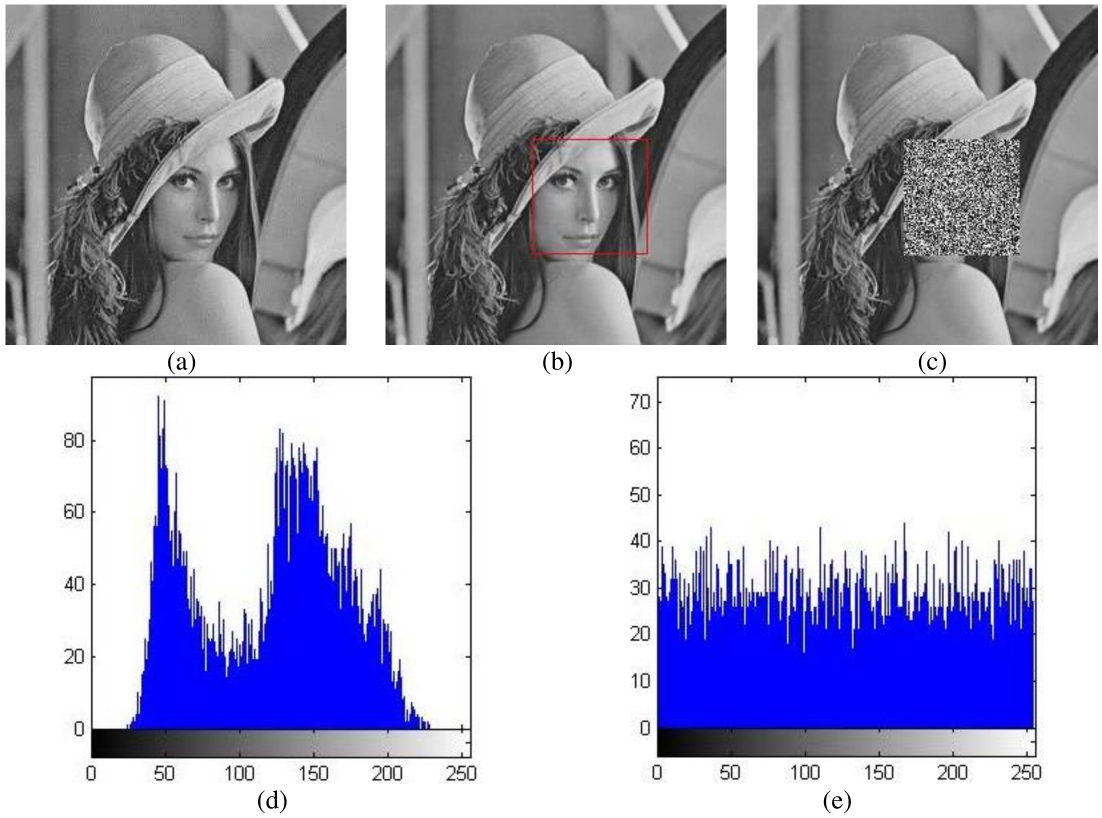


Figure 16. (a) Plain Lena image, (b) selected face, (c) encrypted face, (d) Lena's plain face histogram, (e) and Lena's encrypted face histogram

v. Running time

Three major functions in encryption scheme are face detection, elliptic curve encryption and bit permutation. Inverse bit permutation and elliptic curve decryption are main operators in decryption scheme. These functions are effective and determinative in evaluating the execution time of this scheme. Table 11 is the estimated elapsed time for encryption and decryption functions. Total encryption and decryption time are computed by equations (16) and (17), respectively. In these equations, the variable *r* is the number of iteration rounds and *P* is the elliptic curve key length in bit.

Table 11. Estimated running time for main functions

Variable	Function	Running Time (*ms*)
T_{FD}	Face Detection Running Time	90
T_{BP}	Bit Permutation Running Time (One Window)	0.014
T_{ECE}	Elliptic Curve Encryption Time (One Point)	20
T_{IBP}	Inverse Bit Permutation Time (One Window)	0.01
T_{ECD}	Elliptic Curve Decryption Time (One Point)	18

$$T_E = T_{FD} + (total\_pix - 7) \times r \times T_{BP} + (tota\_pix/P - 1) \times T_{ECE} \tag{17}$$

$$T_D = (total\_pix - 7) \times r \times T_{IBP} + (tota\_pix/P) \times T_{ECD} \tag{18}$$

The calculated encryption and decryption time for figure 5 are based on equations (17) and (18) which results in values in table 12. The value of *total_pix* based on table 11 is the sum of the values in the *number of pixels* column that is equal to 2204 and *P* is *192*.

Table 12. Calculated running time for encryption and decryption

Variable	Function	Running time (*ms*) for figure 5	Running time (*ms*) for figure 10	Running time (*ms*) for figure 16
T_E	Encryption Time	340	2059	1130
T_D	Decryption Time	264	1813	941

In the proposed image encryption scheme by Li et al.33, the whole image (256×*256*) is encrypted by elliptic curve in 6.232 seconds. Whereas proposed selective encryption in this scheme reduces the confidential area to less than 5 percent of the whole image, the encryption time will also reduce to almost 1 second, which is a proper time for real time applications. Homomorphic cryptography is not secure against chosen-plaintext and chosen-ciphertext attacks. The proposed encryption scheme in this paper is a solution to overcome the weakness of Li et al. [33] scheme which is a homomorphic scheme. Applying *r* rounds iteration of bit permutation will increase diffusion and confusion.

4. CONCLUSION

In this paper, a novel public key selective image encryption scheme is proposed based on the elliptic curve and chaotic maps. Unlike similar works that the permutation process is applied on square images with equal height and width, the proposed scheme in this paper is a new approach and independent from the image size. Using the elliptic curve for encrypting a whole image is not efficient for real-time applications. Selective encryption is an efficient approach that encrypts only the confidential parts of an image. In some applications such as sharing the picture of suspects or criminals, the identity of the people in an image is secret. Hence, in such images, only the face of the people should be encrypted, not the whole image. This approach is called as selective or partial encryption. In comparison with another similar work based on ECC, this scheme is much more efficient in security and running time. It reduces the time and less computation is needed and practically encrypts less than 5 percent of an ordinary image. These characteristics turn this cryptosystem as an acceptable choice for highly secure and real time applications. In this paper, an approach is implemented to reduce the running time for public key encryption. It is appropriate for images that contain human face(s). This approach omits approximately 95 percent of an image in encryption process and only 5 percent of the image is encrypted. This method is finalized by combining chaotic map and elliptic curve. Chaotic map is applied to shuffle pixels for confusion and diffusion. Shuffling the pixels will reduce the chance of successful know-plaintext and chosen-plaintext attacks. Subsequently, pixels are encrypted using elliptic curve based on the binary grouping approach and Koblitz method. Evaluation results prove the efficiency of the proposed selective scheme regarding the security and running time. Ideal values for correlation, entropy and histogram analysis results prove the strength of this scheme against statistical attacks. Apart from that, running time for this scheme is compared in table 11 with two other similar works that encrypt the whole image of Lena. This is to emphasize on efficiency of selective encryption from running time point of view

REFERENCES

1. W. Effelsberg and R. Steinmetz, Video Compression Techniques: From JPEG to Wavelets., Morgan Kaufmann, 1998.
2. W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video," *IEEE Transactions on Multimedia,* vol. 5, no. 1, p. 118–129, 2003.
3. S. G. A. and M. T. B., "Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-Time Video," in *Proceedings of Fourth International Conference on Computer Communications and Networks*, 1995.
4. I. Agi and L. Gong, "An empirical study of secure MPEG video transmissions," in *Proceedings of Internet Society Symposium on Network and Distributed Systems Security, hlm.137–144. IEEE Comput. Soc. Press*, 1996.
5. M. V. Droogenbroeck, R. Bendet, "Techniques for a selective encryption of uncompressed and compressed images," *Advanced Concepts for Intelligent Vision systems,* pp. 90-97, 2002.
6. M. V. Droogenbroeck, "PARTIAL ENCRYPTION OF IMAGES FOR REAL-TIME APPLICATIONS," *Fourth IEEE Benelux Signal Processing,* vol. 4, pp. 11-15, 2004.
7. O. Odibat, M. Abdallah and M. Al-Zoubi, "New Techniques in the Implementation of the Partial Image Encryption," in *4th International Multi-conference on Computer Science and Information Technology*, 2006.
8. K. J. Sher and A. Jawad, "Chaos based efficient selective image encryption," *Multidimensional Systems and Signal Processing,* vol. 30, no. 4, 2019.
9. A. M. Ayoup, H. A. H. and A. M. A., "Efficient selective image encryption," *Multimedia Tools and Applications,* pp. 1-16, 2015.
10. I. Ullah, W. Iqbal and A. Masood, "Selective region based images encryption," in *2nd National conference on information assurance*, 2013.
11. K. Hong and K. Jung, "Partial encryption of digital contents using face detection algorithm," in *Trends in Artificial Intelligence*, 2006.
12. J. M. Rodrigues, W. Puech and A. G. Bors, "Selective encryption of human skin in JPEG images," in *International Conference on Image Processing, ICIP*, 2006.
13. G. Bhatnagar and Q. M. Jonathan Wu, "Selective image encryption based on pixels of interest and singular value decomposition," *Digital Signal Processing,* vol. 22, no. 4, p. 648–663, 2012.
14. I. Abuhaiba and M. Hassan, "IMAGE ENCRYPTION USING DIFFERENTIAL EVOLUTION APPROACH IN FREQUENCY DOMAIN," *Singal & Image Processing: An International Journal,* vol. 2, no. 1, pp. 51-69, 2011.
15. A. Ghaffari, "Image compression-encryption method based on two-dimensional sparse recovery and chaotic system," *Scientific Report,* vol. 11, 2021.
16. J. M. Rodrigues, W. Puech, P. Meuel, J. C. Bajard and M. Chaumont, "Face protection by fast selective encryption in a video," in *IET Conference on Crime and Security*, 2006.

17. D. Moon, Y. Chung, S. B. Pan, K. Moon and K. I. Chung, "An efficient selective encryption of fingerprint images for embedded processors," *ETRI Journal,* vol. 28, no. 4, pp. 444-452, 2006.

18. D. Sharma, R. Saxena and A. Rajput, "Robust Image Encryption Using Discrete Fractional Fourier Transform with Eigen Vector Decomposition Algorithm," *Advances in Microelectronic Engineering,* vol. 1, no. 4, pp. 77-82, 2013.

19. A. Emir Dirik and N. Memon, "Selective Robust Image Encryption for Social Networks," *Multimedia Communications, Services and Security,* vol. 368, pp. 71-81, 2013.

20. N. Taneja, B. Raman and I. Gupta, "Selective image encryption in fractional wavelet domain.," *Internationa l Journal of Electronics and Communications,* vol. 65, no. 4, pp. 338-344, 2011.

21. M. Podesser, H. Schmidt and A. Uhl, "Selective bitplane encryption for secure transmission of image data in mobile environments," in *Proceedings of the 5th IEEE Nordic Signal Processing Symposium*, 2002.

22. Ashutosh and D. Sharma, "Image Encryption Using Discrete Fourier Transform and Fractional Fourier Transform," *International Journal of Engineering and Advanced Technology ,* vol. 4, pp. 886-890, 2013.

23. X. Wang and Y. Su, "Color image encryption based on chaotic compressed sensing and two-dimensional fractional Fourier transform," *Scientific Report,* vol. 10, 2020.

24. L. Bao, Y. Zhou and C. Chen, "Image encryption in the wavelet domain," *SPIE Defense,* 2013.

25. K. Naik, A. K. Pal and R. Agarwal, "Selective Image Encryption using Singular Value Decomposition and Arnold Transform.," *The International Arab Journal of Information Technology,* vol. 15, no. 4, pp. 739-747, 2018.

26. Z. Tang, Y. Yang, S. Xu, C. Yu and Xianquan Zhang, "Image Encryption with Double Spiral Scans and Chaotic Maps," *Security and Communication Networks,* 2019.

27. B. N. Van, S.H. Lee and K.R. Kwon, "Selective Encryption Algorithm Using Hybrid Transform for GIS Vector Map," *Journal of Information Processing Systems,* vol. 13, no. 1, pp. 68-82, 2016.

28. K. Abdmouleh, M. Khalfallah and S. Bouhlel, "A Novel Selective Encryption Schemefor Medical Images Transmission based-on JPEG Compression Algorithm," *Procedia Computer Science,* vol. 12, pp. 369-376, 2017.

29. N. Khalifa, R. Filali and M. Benrejeb, "A Fast Selective Image Encryption Using Discrete Wavelet Transform And Chaotic Systems Synchronization," *Information Technology and Control,* vol. 45, pp. 235-242, 2016.

30. M. Jones and P. Viola, "Robust real-time object detection," *International Journal of Computer Vision,* pp. 34-47, 2001.

31. Z. Zhu, W. Zhang, K. Wong and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Sciences,* vol. 181, no. 6, pp. 1171-1186, 2011.

32. N. Koblitz, "A Course in Number Theory and Cryptography," *The Mathematical Gazette,,* vol. 73, 1989.

33. C. Li, L. Y. Zhang, R. Ou, K. W. Wong and S. Shu, "Breaking a novel colour image encryption algorithm based on chaos," *Nonlinear Dynamics,* vol. 70, no. 4, p. 2383–2388, 2012.

34. M. Hénon, "A two-dimensional mapping with a strange attractor," *Communications in Mathematical Physics,* vol. 77, pp. 69-78, 1976.

35. E. Lorenz, "Deterministic nonperiodic flow," *Journal of the atmospheric sciences,* vol. 20, pp. 130-141, 1963.

36. S. Deng, D. Xiao, Y. Li and W. Peng, "A novel combined cryptographic and hash algorithm based on chaotic control character," *Communications in Nonlinear Science and Numerical Simulation,* vol. 14, no. 11, p. 3889–3900, 2009.

37. B. Furht and D. Kirovski, Multimedia security handbook, 2005.