IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

New Image Encryption Algorithm Based on Diffie-Hellman and Singular Value Decomposition

Nidhal Khdhair El Abbadi[1], Samer Thaaban Abaas[2], Ali Abd Alaziz[3]

Computer Science Department, Education College, University of Kufa, Najaf, Iraq[1, 2, 3]

Abstract: With the fast progression of using images in many applications, it is important to protect the confidential image data from unauthorized access. In this paper we suggested a new way to encrypt image based on three main steps: the first one aims to scrambling the image values by using Fibonacci transform, while the second step focus on generating public and private key based on Diffie -Hellman Key Exchange, these keys used to encrypt the diagonal matrix which created by Singular Value Decomposition (SVD) in third step. Decryption is the inverse process of encryption. The results were promised and the decrypted image retrieved without loss any of its information. Encryption and decryption time was very trivial. The contribution of this paper is to encrypt image by using singular value decomposition with Diffie -Hellman Key Exchange. Paper novelty based on scrambling values based on Fibonacci transform and encryption image by using SVD.

Keywords: Encryption, Decryption, SVD, DH, Fibonacci.

I. INTRODUCTION

In today's world, new branch in computer science emerged called Information Security, which deal with keeping the information safe from unauthorized person's to use the information's. There are many methods suggested every day to keep the information secure, but the hackers and unauthorized persons always trying to break those methods [7]. Nowadays, information security is becoming more important in data storage and transmission. 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 [2].

The important different between image encryption and text encryption is the image size which is almost always much greater than the text size. For that the use of traditional cryptosystems need much time to encrypt the image. The other different is related to decryption, the decrypted image allowed to some changing from the origin image while this case not allowed in text decryption [5]

There are two main types of cryptography:

- Secret key cryptography
- Public key cryptography

Secret key cryptography is also known as symmetric key cryptography. With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

Public key cryptography, also called asymmetric key cryptography, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys.

Cryptography technique is used when secret message are transferred from one party to another over a communication line. Cryptography technique needs some algorithm for encryption of data.

II. RELATED WORKS

There are many researches in this context, we select some of them which are most related:

Nidhal El Abbadi, proposed new encryption algorithm based on scrambling the image data according to suggested keys (two sequence scrambling process with two different keys) which ultimately produce two different matrices. The diagonal matrix from the SVD of the resulted two matrices will be interchanged. Another scrambling and diagonal matrices interchange will apply to increase the complexity [4].

Chao-Wen Chan, apply Diffie and Hellman (DH) key agreement method and total auto-morphism (TA) such that visual cryptography can be reused. Both secret and symmetry key are represented in binary image [1].

Rinki Pakshwar, described a method for new digital image scrambling method based on Fibonacci numbers. The standardization and periodicity of the scrambling transformation are discussed. The scrambling transformation has the following advantages: Encoding and decoding is very simple and they can be applied in real time situations. The scrambling effect is very sensible, the data of the image is re- distributed randomly across the whole image [6].

III. METHODOLOGY

In this paper we suggested new method for encrypt images. This method based on some of mathematical processes, we have to explain the process used in this method, then we declare the encryption and decryption process.

A. Diffie -Hellman Key Exchange (DH)

The DH scheme was first proposed by Whitfield Diffie and Martin Hellman in 1976, it is one of the first key exchange algorithms that is still used to this day [3].

DOI 10.17148/IJARCCE.2016.5147

Suppose there are two parties A and B, with C trying to snag the key through the insecure communications channel.

- The first step is to suggest a large prime number n and a nonzero integer gthat approved by both A and B. Both n and g has no need to be kept secret, so C might know them.
- In the second step A pick a secret integer (a) that is kept secret, even to B. Also B picks another integer (b) that is also kept secret to A.

A computes X = g^amod n
B computes Y = g^bmod n
A send X to B and B send Y to A
A computes x = Y^amod n
B computes y = X^bmod n
Now x and y should be the same, because
x = Y^amod n =(g^b)^{a}mod n = g^{ba}mod n = g^{ab}mod n = (g^a)^{b}mod n = X^bmod n = y

This shared values is now regard as encrypted key. C can only know the shared values but will be useless, since C doesn't know the secret numbers (a) and (b).

An example to explain the above phenomena:

- A and B agree to use the prime number n = 51053 and primitive root g = 13
- A choose secret key a = 7 and compute
$X = (13)^7 mod\ 51053 = 62745817 mod\ 51053 = 4380$
- B choose secret key b = 5 and compute
$Y = (13)^5 mod\ 51053 = 371293\ mod\ 51053 = 13922$
- A send X to B and send Y to A, this is often done through an insecure communication, so C can know these values but useless since (a) and (b) is kept secret.
- Both A and B compute (x and y):
$x = Y^a mod\ n = (13922)^7 mod\ 51053 = 8116$
$y = X^b mod\ n = (4380)^5 mod\ 51053 = 8116$

(8116) is the shared secret number, which can be used as a symmetric key to encryption, without this number itself there is no a communication channel. Figure 1 summarized the example.

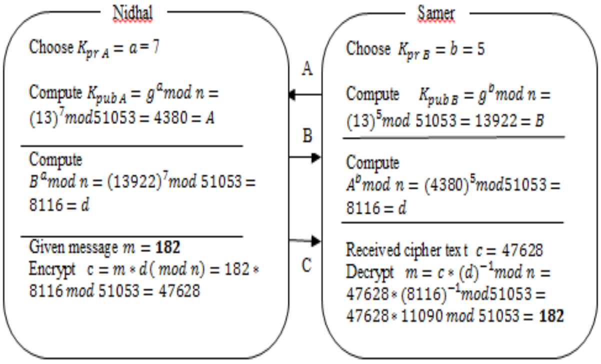

Nidhal
Choose $K_{pr\,A} = a = 7$
Compute $K_{pub\,A} = g^a mod\ n = (13)^7 mod51053 = 4380 = A$
Compute
$B^a mod\ n = (13922)^7 mod\ 51053 = 8116 = d$
Given message m = **182**
Encrypt $c = m * d(\ mod\ n) = 182 * 8116\ mod\ 51053 = 47628$
A
B
C
Samer
Choose $K_{pr\,B} = b = 5$
Compute $K_{pub\,B} = g^b mod\ n = (13)^5 mod\ 51053 = 13922 = B$
Compute
$A^b mod\ n = (4380)^5 mod51053 = 8116 = d$
Received cipher tex t $c = 47628$
Decrypt $m = c * (d)^{-1} mod\ n = 47628 * (8116)^{-1} mod51053 = 47628 * 11090\ mod\ 51053 =$ **182**

Fig. 1: Summarized the above example

B. Fibonacci Transform

Fibonacci sequence F_n can be defined as follows

$$F_n = \begin{cases} 0 & n = 0 \\ 1 & n = 1 \\ F_{n-1} + F_{n-2} & otherwise \end{cases} \qquad (1)$$

By applying equation (1) we build Fibonacci series which constitutes of the numbers (0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144,……….)

Fibonacci transform can be easily represent as a $2x2$ matrix by any four consecutive terms of the Fibonacci numbers,this matrix can be regard as a mask usefor image scrambling. A generalized Fibonacci mask can be define as:

$$\begin{bmatrix} \dot{x} \\ \dot{y} \end{bmatrix} = \begin{bmatrix} f_i & f_{i+1} \\ f_{i+2} & f_{i+3} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod(n) \qquad (2)$$

Where $x, y, \dot{x}, \dot{y} \in \{0, 1, 2, 3, 4, \dots \dots \dots, n-1\}$, fi is the ith term of the Fibonacci series, and n is the size of the digital squared image. x, y is the pixel coordinate in origin image and $\dot{x}, \dot{y}$ is the new coordinate for the pixel in the scrambled image.

This mask can scan theentire image from left to right and top to down, which scramble the pixels to create new image.

C. Singular Value Decomposition (SVD)

For any given matrix $A \in R^{m \times n}$ there exist the singular value decomposition matrices such that **U**orthogonal matrix of size $m \times m$, **V** orthogonal matrix of size $n \times n$ and **S** diagonal matrix of size $m \times n$ where all the entries s_{ij} are 0 when $i \neq j$.

$$\boldsymbol{A_{mn} = U_{mm} S_{mn} V_{nn}^T}$$

Where $U^T U = I,\ V^T V = I$ and $s_{11} \geq s_{22} \geq \cdots s_{pp} \geq 0$, where p = min {m, n}.

The columns of **U** are orthonormal eigenvectors of AA^T,
The columns of **V** are orthonormal eigenvectors of $A^T A$,
And **S** is a diagonal matrix containing the square root of Eigenvalue from U or V in decreasing order [8].

If matrix$M$ is 5×3 this would look like

$$M = U \times S \times V^T \quad \dots\dots\dots\dots\dots\dots\dots \quad (3)$$

$$\begin{bmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \\ m_{41} & m_{42} & m_{43} \\ m_{51} & m_{52} & m_{53} \end{bmatrix} = \begin{bmatrix} u_{11} & u_{12} & u_{13} & u_{14} & u_{15} \\ u_{21} & u_{22} & u_{23} & u_{24} & u_{25} \\ u_{31} & u_{32} & u_{33} & u_{34} & u_{35} \\ u_{41} & u_{42} & u_{43} & u_{44} & u_{45} \\ u_{51} & u_{52} & u_{53} & u_{54} & u_{55} \end{bmatrix} \begin{bmatrix} s_{11} & 0 & 0 \\ 0 & s_{22} & 0 \\ 0 & 0 & s_{33} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} v_{11} & v_{12} & v_{13} \\ v_{21} & v_{22} & v_{23} \\ v_{31} & v_{32} & v_{33} \end{bmatrix}^T$$

D. Encryption method

Encryption will follow the following steps:

(1) The input image will be read as a matrix X. For best result it is better to process the image as square image, for that the image or the matrix will be transform to square matrix (image) if it is not square.

(2) Change the elements of the matrix X randomly by using Fibonacci Transform to get matrix B.

(3) Convert the matrix B to three matrices by transform it with SVD transformation as following

$$[U, S, V] = SVD\ (B)\dots\dots\dots\dots(4)$$

(4) Split the Diagonal matrix S into two Diagonal matrices A and P where the matrix A contain only integer part of S values, and matrix P contain only fractional part of S values, Where:

$S = A + P$ ………… . (5)

(5) By suggestion two keys (large key and small key) to exchange with the receiver, we can create private key to use in the encryption process.

(6) Encrypt the matrix A with HD method based on private key created in the step 5. The result of this step is the matrix$F$.

(7) Now, the matrix F will be replaced instead of matrix A in relation (5) to build new matrix G as in the following relation:

$G = F + P$ ……………… (6)

(8) The final step in encryption process is to build the encrypted matrix X' by using the same matrices resulted from SVD (U and V) and the diagonal matrix (relation 6), which encrypted in the step7 as follow:

$H = U * G * V^T$ ………… (7)

(9) Final step is option.

To increase the encryption complexity we add new key (small value).The new key subtracted from the matrix H to get new matrix D.Matrix D will be split to two equal matrices (Z and W), where Z is:

$Z = mod(D, 256)$ ……………...... (8)

And W is: $W = fix(D/256)$…………… (9)

Then the final encrypted matrix is the matrix resulted from merging the two matrices (Z and W) according to the previous agreement between the sender and receiver. The result can view as image and send to the receiver.

E. Decryption

Following are the steps for decrypt the encrypted image, is the inverse of encryption process:

(1) Separate the encrypted (image) matrix R to two square matrices Z and W based on the previous agreement of merging the two matrices.

(2) Multiply the matrix W by 256 then sum the result with the matrix Z to get the matrix W_1

$W_1 = W * 256 + Z$ …………….. (10)

(3) Add the smallest value y to W_1 to get the new matrix W_2.

(4) Find SVD of the matrix W_2 according to the following relationship

$[Q, K, L] = SVD\ (W_2)$ ………… (11)

(5) Split Diagonal matrix K to two diagonal matrices (C, N), where C contains integers part and N contains fractional part only where:

$K = C + N$……………………… (12)

(6) Decrypt the elements of the diagonal matrix C by using the private key (which created according to the small key and large key exchanged with sender previously), to get the Diagonal matrix E.

(7) Add the matrix E to matrix N to get the matrix M:

$M = E + N$……………………… (13)

(8) Rebuild the transformed matrix by using the matrices (Q and L) resulted from the SVD transformation in step 4, and the diagonal matrix M, as follow:

$A_1 = Q * M * L^T$…………………(14)

(9) Elements of matrix A_1 should be rounded to nearest integer numbers.

(10) The final matrix can be produced by the inverse of Fibonacci transform which we did in the first step of encryption.

(11) Therefore, after complete the decryption steps the result is the original image.

IV. EXPERIMENTAL RESULTS

To check the performance of suggested algorithm we choose many images and test the algorithm on its (some of them in figure 2). The selected images were color images and grayscale images, in case of color images each image will be converted to three matrices one for each color band (Red, Green, and Blue), and then the encryption process will be apply for each (band) matrix. Some of the selected images showed in table 1.

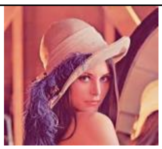
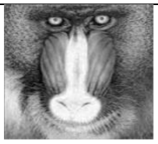
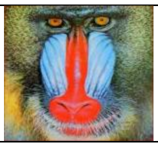
Image	Type	Dimension	Size (Byte)
Lena Grayscale		225 × 225	65025
Lena Color		225 × 225	195075
Baboon Grayscale		225 × 225	65025
Baboon (Color)		225 × 225	195075

Fig.2.some of selected images and their dimensions

There are some criteria used to test the selected images, the first one we test the resulted image (encrypted and decrypted image) visually as shown in Fig. 3.

The important test was to check PSNR which compare the origin image and the decrypted image as shown in table1.

Also we check the encryption and decryption time as shown in Table2.

The encryption and decryption time for different images size showed in Fig. 4.

Fig. 5 showed the histogram for origin, encrypted, and decrypted images.

Another criteria used to check the proposed algorithm are (mean, standard deviation and entropy) as showed in Table 3.

The last thing is Table 4, which compare the encryption and decryption times for suggested algorithm with other algorithms.

DOI 10.17148/IJARCCE.2016.5147

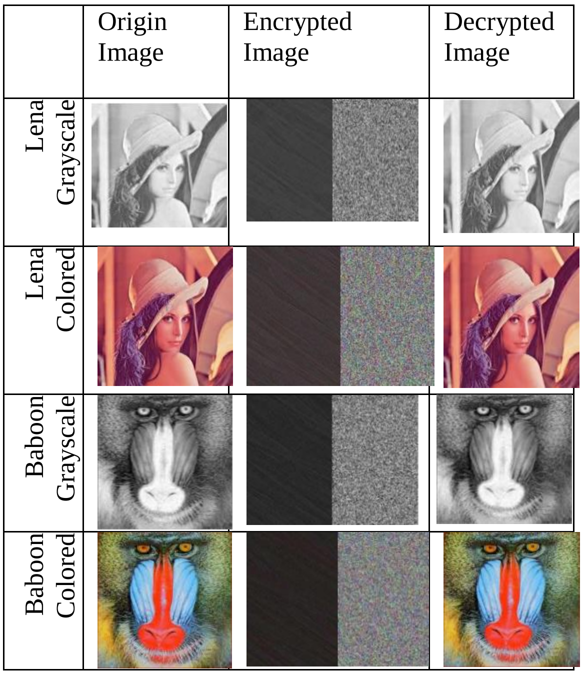


Fig.3.show the origin images, encrypted images and decrypted images

Table 1: PSNR for the encrypted image showed in table 1.

Image	PSNR
Lena (grayscale)	inf
Lena (Colored)	inf
Baboon (Grayscale)	inf
Baboon (Colored)	inf

Table 2: Encryption and decryption times

Image	Time of encryption in (seconds)	Time of decryption in (seconds)
Lena (grayscale)	0.425981	0.317532
Lena (Colored)	0.834972	0.661290
Baboon (Grayscale)	0.447617	0.306005
Baboon (Colored)	0.827898	0.674729

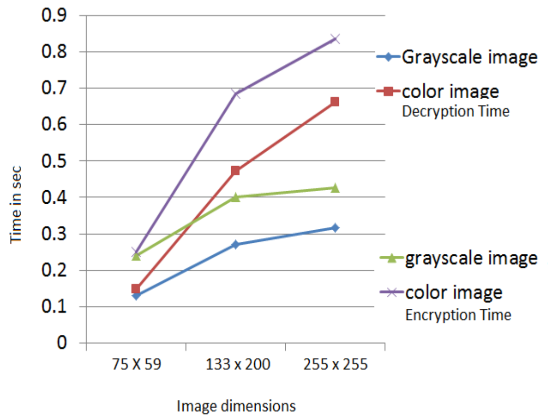


Fig.4.showed encryption and decryption times for different images size

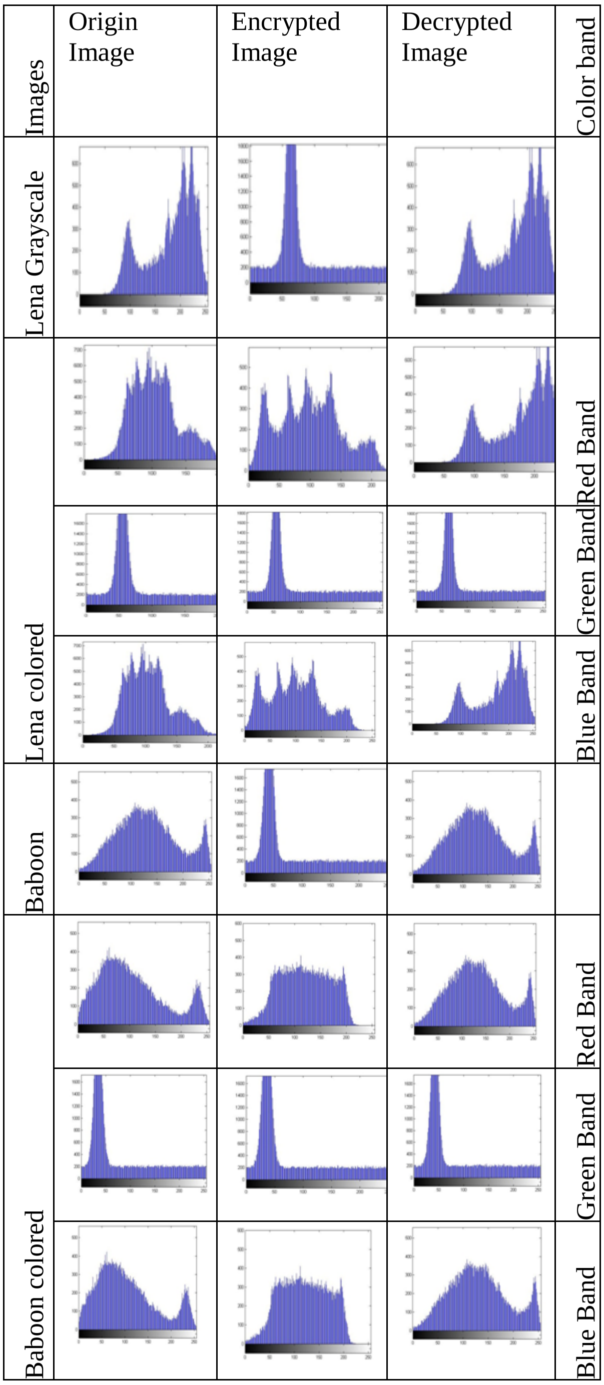


Fig. 5.Histogram for origin images, encrypted images, and decrypted images.

Table 3: entropy, mean and standard deviation for origin images, encrypted images and decrypted images.

Image	Features	Origin Image	Encrypted Image	Decrypted Image
Lena Grayscale	Entropy	7.3029	7.1319	7.3029
	Mean	180.1372	95.8314	180.1372
	Standard Deviation	49.2257	61.6351	49.2257
Lena Colored	Entropy	7.7721	7.2209	7.7721
	Mean	128.2411	92.8911	128.2411
	Standard Deviation	58.8898	63.2847	58.8898

DOI 10.17148/IJARCCE.2016.5147

Baboon Grayscale	Entropy	7.7834	7.1745	7.7834
	Mean	132.2186	84.7419	132.2186
	Standard Deviation	58.3033	67.8604	58.3033
Baboon Colored	Entropy	7.8143	7.2273	7.8143
	Mean	118.8019	82.8206	118.8019
	Standard Deviation	58.1761	69.3639	58.1761

Table 4: comparing proposed algorithm with other algorithms [5].

algorithm	image	Encryption time (s)	Decryption time (s)
MIE	Lena grayscale	0.27	0.22
MIE	Lena color	5.0	5.16
MIE	Baboon grayscale	0.49	0.22
MIE	Baboon color	9.23	9.23
VC	Lena grayscale	1.98	*
VC	Lena color	4.56	*
VC	Baboon grayscale	3.57	*
VC	Baboon color	8.35	*
Our algorithm	Lena grayscale	0.27	0.13
Our algorithm	Lena color	2.522	2.924
Our algorithm	Baboon grayscale	0.763	0.97
Our algorithm	Baboon color	2.338	3.104

* Visual cryptography exploits the human visual system to read the secret message from some overlapping shares.
MIE – Mirror-like Image Encryption
VC - Visual Cryptography

V. CONCLUSION

In this paper, a new improved approach for image encryption using a combination of DH and SVD techniques is proposed. The proposed method uses concept of uniform scrambling based on Fibonacci transform. Public and private keys generated based on Diffie -Hellman Key Exchange, these keys used to encrypt the diagonal matrix which created by Singular Value Decomposition (SVD).

The experimental results showed that the proposed image encryption system has a very large key space; also the cipher image has entropy information close to the ideal value 8. Thus the analysis proves the security, correctness, effectiveness and robustness of the proposed image encryption algorithm.
Encryption and decryption time for proposed algorithm were reasonable when comparing with other algorithm as in table 4. Proposed algorithm can easily uses with text.

REFRENCES

[1] Chao-Wen Chan and Yi-Da Wu, 2008, "A Visual Information Encryption Scheme Based on Visual Cryptography and D-H Key Agreement Scheme", International Journal of Computer Science and Network Security, vol.8,no.4. 2008.

[2] HiralRathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma,**"**Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)",International Journal of Computer Technology and Electronics Engineering,vol. 1, issue 3. 2011.

[3] Komal D Patel, SonalBelani, "Image Encryption Using Different Techniques: A Review", International Journal of Emerging Technology and Advanced Engineering, vol. 1, issue 1. 2001

[4] El Abbadi Nidhal, Adil Mohamad and Mohammed Abdul-Hameed, "Image Encryption Based on Singular Value Decomposition", Journal of Computer Science 10 (7), pp. 1222-1230, 2014.

[5] Ozturk, I. and Sogukpınar I., "Analysis and comparison of image encryption algorithms". International Journal of Computer, Electrical, Automation, Control and Information Engineering, Vol. 1, No. 3, 2007

[6] Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya, "A Survey On Different Image Encryption and Decryption Techniques", International Journal of Computer Science and Information Technologies, Vol. 4,issue 1, pp. 113 – 116, 2013.

[7] Somdip Dey, "An Image Encryption Method: SD-Advanced Image Encryption Standard: SD-AIES**",** International Journal of Cyber-Security and Digital Forensics, vol. 1, issue 2,pp. 82-88, 2012.

[8] B. Kolman and D. Hill , 2008, "Elementary Linear Algebra With Applications", Pearson Education, Inc., Ninth Edition.

BIOGRAPHIES

Nidhal El Abbadi, received B.Sc. in Chemical Engineering, B.Sc. in computer science, M.Sc. and Ph.D. in computer science, worked in industry and many universities, he is general secretary of colleges of computing and informatics society in Iraq, Member of Editorial board of Journal of Computing and Applications, reviewer for a number of international journals, has many published papers and three published books (Programming with Pascal, C++ from beginning to OOP, Data structures in simple language), his research interests are in image processing, security, and steganography, He's Associate Professor in Computer Science in the University of Kufa – Najaf, IRAQ.

Samer Thaaban Abaas, received B.Sc. in mathematics from al-Mustansirya university, M.Sc. in mathematics from university of Kufa, currently worked in university of Kufa, Najaf, IRAQ.

Ali Abd Alaziz, received B.Sc. in civil engineering, B.Sc. in computer science, M.Sc. In computer science, now he is PhD student in Babylon University, worked in university of Kufa, Najaf, IRAQ.