Classical Image Encryption and Decryption

Noor Dhia Kadhm Al-Shakarchy[1], Hiba Jabbar Al- Eqabie[2], Huda Fawzi Al- Shahad[3]

Computer Science Department, Science College, Karbala University, Karbala, IRAQ

Abstract: ***The interesting of data production in transmission by any type of multimedia such as digital image, text, audio and video is increases. Many methods are used to provide the secrecy, integrity, confidentiality and to prevent unauthorized access of sensitive information such as Cryptography. Cryptography is secret the original data by converting it to cipher data with ensure retrieve this data in receiver side without losing some data or deformation the resolution. In this paper, we used confusion schemes for scrambling the positions of pixels of the colored images by using Arnold Cat Mapping. Shuffling mechanism combined with diffusion mechanism for encrypting the scrambling image by changing the gray values of the image pixels by using classical methods of encrypted and decrypted of digital color images. The suggested methods involved classical cipher system such as veginner substitution cipher system and hill cipher method. From all experimental and analysis techniques on some color images that used to evaluate the proposed image encryption and decryption methods we found that hill cipher shows significant security and high speed than other methods. Moreover, increase the randomness of the cipher images which led to hide the natural properties of original images.***

Keywords: encryption, decryption, hill cipher, vigener cipher, Arnold Cat Map System, pain image , cipher image and key.

1. Introduction

Encryption is the process of transforming the original data which called plaintext in to encrypted data called ciphertext [1]. Different techniques are used to fulfill the data own features of each data type. Many encryption algorithms used to protect and ciphered text data such as classical cipher system. Digital images used in many communication applications, therefore the protection the content of these images become very important. Image encryption is a technique which coding the original image (plain image) to another un-understanding image (cipher image). This technique must be providing the decoding the cipher image to plain image without losing data or image properties [3]. Divers set of applications ubiquitous depending on digital image encryption and used diver's algorithms to protect the content and information of original images from unauthorized users. There are different types of encryption algorithms according to plaintext message; some used for text data and not be suitable for other multimedia data such as digital image. Others types used for images and not suitable with text data. Due to image powerful attribute such as vast data capacity, the great redundancy and great correlation among pixels of image. These algorithms can't used specifically actualized to image on the grounds that image size is practically. These algorithms need much time when used with image [2]. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable [4]. Textual encryption algorithms presented in this paper. Theses algorithms, such as Vigener and Hill cipher systems; used to encrypted and decrypted color digital images after some enhancement to become suitable with digital image.

The proposed system provide security so nobody can see or get the original image just approved individual, and integrity to guarantee that the image has not altered and secrecy to guarantee that image got to ideal spot amid the transmission of the image. The important goal must the proposed system runs is not lost the image data during the retrieving process such that achievement similarity between the encryption (origin) and decrypted images. In this research, we present some algorithms which are used with raw data, and used in digital image Encryption and Decryption after some advanced to be suitable with digital image. The classical cipher algorithm, which is used in this research, is symmetric algorithm used same key in encryption and decryption process. The key used in proposed system is also digital color image. Vigener system used with digital image Encryption, by using the same equation, but with pixels of the original image and key image after split them in to main color channels such as Red (R), Green (G), Blue (B). The other algorithm used is Hill cipher system, used in digital image Encryption by dividing the original image into blocks inside the image. The sizes of these blocks determined according to the size of key metrics which is other key image, then apply the main hill equation.

2. Related Work

Imaging data is one of famous multimedia which is used in varies field. Therefore the protection of these images against illegal intruder takes a lot of interesting. Many algorithms and schema presented to encrypted these images with less loss quality. There are many methods deals with images only as well as others deals with textual data but employed to been compatible with image data. In 2008, Mohammad Ali Bani Younes and Aman [5] present a change calculation relying upon the combination of image transformation and a surely understood encryption and unscrambling calculation called Blowfish. The image was isolated into squares blocks, which were altered into a changed image using a transfer algorithm, and after that the changed image was mixed using the Blowfish algorithm. Their outcomes showed that the relationship between image segments was through and through decreased. Their outcomes in like manner exhibit that utilizing so as to extend the pieces number more humble squares sizes came to fruition as a piece of a lower association and higher entropy.

Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda in 2009 [3, 6] have done an advanced Hill (AdvHill) cipher algorithm where an obligatory key matrix utilized for encryption. Diverse images encrypted utilizing basic and advanced Hill cipher algorithm. It is clearly perceivable that basic Hill Cipher can't encrypted the image honest to goodness if the image contains sweeping extent secured with same shading or dim level. In the meantime their proposed estimation satisfies desires for any images with unmistakable dark scale and what's more shading images. This works could beat the issues of image encryption with homogenous foundation and exhibited quick, dependable and strong encryption plan as contrasted and existing strategies. In this research, we present the classical cipher system such as Viginer cipher and hill cipher with image key. These methods presented fast and randomly decrypted image as well as the original image can be retrieving during the decryption algorithm without data privation.

3. Research Aims

Actually, the major aim of any image cipher system is used to protect the content and information of original images from unauthorized users using an easy and inexpensive scheme of encryption and decryption of digital data to all authorized users. The block diagram of proposed system is depicts in Figure (1) below. The main algorithm executed in proposed system included encryption and decryption process by using RGB image of row*column*3 stored as a three dimensional matrix of pixels. The confusion and diffusion approach presented during these processes architectures.

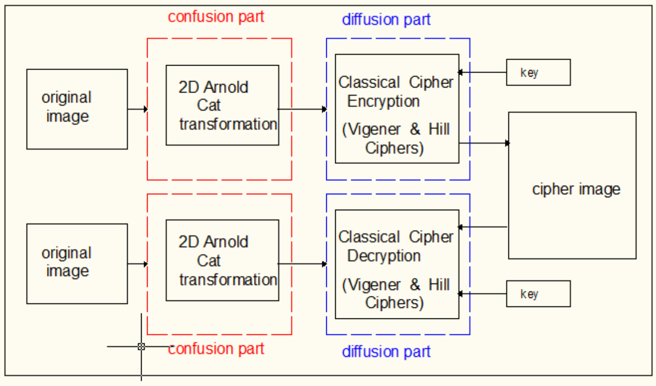


Figure 1: Suggested system block diagram

4. Arnold Cat Map System

Rearrange the pixels of color image are presented using Arnold's Cat Map transformation. This transformation provides additional security of cipher system. The 2D Arnolds cat algorithm don't modify or change the pixels values of the image pixels, yet it just scramble the image information as appeared in equation(1) for image coding (first encryption) and equation(2) for image decoding (last decryption).

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & p*q+1 \end{bmatrix} * \begin{bmatrix} X \\ Y \end{bmatrix} \bmod 256 \qquad ...(1)$$

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & p*q+1 \end{bmatrix}^{-1} * \begin{bmatrix} X' \\ Y' \end{bmatrix} \bmod 256 \qquad ...(2)$$

Where:
p,q: represents the positive secret keys.
X,Y : original position of the image pixel before scrambling.
X',Y': new position of the image pixel after scrambling [7].

The relationship between the neighboring pixels is entirely destroy and the original image seems deformation and meaningless after several iterations of applying 2D Arnold cat transformation. The Arnold cat map is a periodic transform, because the iterating image to many times it will return to original image. The statistical features are same as for encrypt image and original image after image shuffling which increase the security of encryption system [8].

5. Vigener cipher

In general, The key is specified by a sequence of the letters= k1,k2,……..,k_d, where k_i (i=1,2,….,d) gives the shifting amount in the ith alphabet that is [1,2]:

$$F(a) = (a + ki) \bmod n \text{ ……………………. } (1)$$

Where k_i : is the number of positions to be shifted in the i_{th} alphabet.
a : is a single character of the alphabet.
n : is the size of the alphabet.

This formatted used with text data. In digital image plaintext we used digital image key and used same equation (1) but with pixels of original image and key image after analysis them to main colors values Red (R) , Green (G) , Blue (B) such that applying the equation to each value :

$$R' = E_R(ai_R) = (ai_R + ki_R) \bmod 256 \text{ …………. } (2)$$
$$G' = E_G(ai_G) = (ai_G + ki_G) \bmod 256 \text{ …………. } (3)$$
$$B' = E_B(ai_B) = (ai_B + ki_B) \bmod 256 \text{ …………. } (4)$$

Where:
k_i : is a single pixel of key image.
a : is a single pixel of original (plaintext) image .
then captured the encrypted values R',G' and B' to represent the cipher text pixel.

In decryption process we used the decryption equations:

$$R = D_R(ci_R) = (ci_R - ki_R) \bmod 256 \text{ ……………. } (5)$$
$$G = D_G(ci_G) = (ci_G - ki_G) \bmod 256 \text{ ……………. } (6)$$
$$B = D_B(ci_b) = (ci_b - ki_b) \bmod 256 \text{ …………. } (7)$$

Where:
k_i : is a single pixel of key image.
c: is a single pixel of cipher image .

✓ **Vigener encryption Algorithm :**

Step1: read plaintext image and key image.
Step2: check if size of key image equal to or greater than plaintext image**.**
Step3: get pixel of plaintext image orderly, (0 – 255).
Step4: get pixel of key image orderly also, (0 – 255).
Step5: analyze them (plaintext pixel and key pixel) to main colors of R, G, B values.
Step6: apply the equations corresponding to color value, equations (2,3,4) with R, G, B orderly. new values R', G', B' obtained.
Step7: accumulate these new color values to generate new pixel of cipher image.

Step8: repeat these steps (3-8) to plain image pixels.
Step9: display the cipher image.

✓ **Vigener Decryption Algorithm :**
Step1: read cipher image and key image.
Step2: check if size of key image equal to or greater than cipher image
Step3: get pixel of cipher image orderly, (0 – 255).
Step4: get pixel of key image orderly also, (0 – 255).
Step5: analyze them (cipher pixel and key pixel) to main colors values Red (R') , Green (G') , Blue (B').
Step6: apply the decryption equations corresponding to color value, equations (5, 6, 7) with R', G', B' orderly. New values R, G, B obtained.
Step7: accumulate these new color values to generate new pixel of plain image.
Step8: repeat these steps (3-8) to cipher image pixels.
Step9: display the plain image.

6. Hill cipher System

Hill cipher is first algorithm deals with more than two characters together[1,2,3,6]. This algorithm depends on Linear algebraic in its working.
Let d=3
M= m1 m2, ,m3.
C= c1, c2 where:
C1 =(k11m1 +k12m2) mod n
C2 =(k21m1 +k22m2) mod n

Where K=

$$\begin{array}{|c|c|c|}\hline K11 & k12 & K13 \\ \hline K21 & K22 & K23 \\ \hline K31 & K32 & K33 \\ \hline\end{array}$$

That is :

$$\begin{array}{|c|}\hline C1 \\ \hline C2 \\ \hline C3 \\ \hline\end{array} = \begin{array}{|c|c|c|}\hline k11 & k12 & k13 \\ \hline k21 & k22 & k23 \\ \hline k31 & k32 & k33 \\ \hline\end{array} * \begin{array}{|c|}\hline m1 \\ \hline m2 \\ \hline m3 \\ \hline\end{array} \quad \text{Mod 26}$$

$$E_k(M) = K{*}M \text{ ……………………… } (8)$$
$$D_k(C) = K^{-1} * C \bmod n \text{ ……………….. } (9)$$

$= K^{-1}$ K M mod n
= M
Where KK^{-1} mod n = I (Identical matrix) [12]

In this research the same algorithm for encrypted color digital image is used, by breaking up the original image into pixels blocks inside the image. The size of these blocks determined according to the size of key metrics(K).and the vector M is an image also that is each vector m1,m2,m3 are the red, green, blue extracted from the key image.

✓ **Hill Encryption Algorithm**
Step1: read the plain image.
Step2: read square key image as matrix .
Step3: extract d pixels of the plain image orderly.
Step4: analyze d pixels to main colors, values Red (R), Green (G), Blue (B).
step5: analyze Matrix pixels to main colors, values Red (R), Green (G), Blue (B).
Step6: apply encryption equation (8) to each color R, G, B. New values R', G', B' obtained.
Step7: accumulate these new color values to generate new d pixels of cipher image.
Step8: doing the steps (3-6) to all plain image pixels.
Step9: display the cipher image.

✓ **Hill Decryption Algorithm**
Step1: read the cipher image.
Step2: read square key matrix d*d from key image.
Step3: extract d pixels of cipher image orderly.
Step4: analyze these pixels to main color values Red (R'), Green (G'), Blue (B').
Step5: calculate the key matrix inverse k^{-1}, using Gauss elimination method as mentioned in section D.
Step6: apply decryption equation; which is same as encryption equation except using inverse matrix of key; to each color R', G', B'. New values R, G, B obtained.
Step7: accumulate these new color values to generate new d pixels of original image.
Step8: repeat these steps (3-6) to all pixels of cipher image.
Step9: print the original image (plain image).

7. Gauss Elimination Method

Using Gauss elimination method in order to calculate the inverse matrix K^{-1}.As a matter of first importance, we have to dene what it intends to say a matrix is in lessened line echelon structure. A matrix in decreased line (row) echelon structure is a column diminished framework which has been rearranged further by utilizing the heading ones to wipe out the non-zero entrances above them and beneath them.
A framework is in lessened line echelon structure if
1) The First nonzero sections of columns are equivalent to 1
2) The principal nonzero passages of sequential columns seem to the right
3) Lines of zeros show up at the lowest part
4) Entrances above and underneath heading sections are zero. [8]

8. Proposed System Security

The cryptosystem efficiency relies on the difficulty associated with decryption process. Such that nobody can reversing the ciphertext and obtained the original message unless know the authentication keys (decryption key). There are many types and ways to measured and evaluated the cipher system security. Some of them depend on determining the permissible keys by the uncertainty facing. Other methods depending on the randomness associated with encryption process.. The unicity distance U defines as "a point may be reached by the cryptanalyst at which a unique solution is possible"[9, 10]. In this paper the proposed system constructed depending on the diffusion and confusion [11, 14]. The thought of diffusion is to spread the plain's insights space into measurable structure which includes long blends of the things in the cryptogram, and thusly spreads the connections and conditions of the plain as practical in order to amplify the unicity separation. The idea of confusion is to make the connection between a cryptogram and the relating key a complex one so as to brightening any indirection to the key as having originated from any specific zone of the key space. The security of proposed system can be evolution using several ways. Some of these ways:

A. Entropy Function:

Data entropy is an idea of measuring the level of arbitrariness in the encryption system [1,2,14]. Really, for any image encryption algorithm it ought to diminishes the associate data among encoded Image pixels and hence mean expands the entropy value. Additionally, it ought to satisfy a condition that on the data entropy that is the figure picture ought not offer any data about the plain picture. Picture entropy is computed utilizing equation(9).

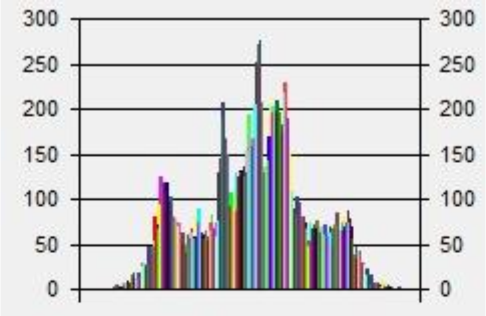
$$entropy = \sum_{i=0}^{255} p(i) * \log_2 * \left(\frac{1}{p(i)}\right) \qquad \text{....}(10)$$

Where P(i) is the probability of existence of pixel i. Truly, the ideal entropy value of random system is equal to8.In general, if calculated entropy value is very close to ideal value this mean that the cipher system is protect upon the entropy attack[13].

B. Histogram

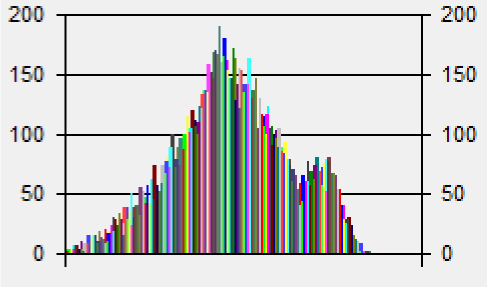
With image cryptosystem the histogram is used as a security evaluation. This methods depends on the comparison between the original image histogram with the cipher image histogram. The histogram represented by count the frequency to each color number in image, and save these frequency counters in a determined matrix. Then plotting from X-axis ; which represents color number; to Y-axis; which represents frequencies number. Figures (2, 4, 6and 8) represent the original image (plain image), key image, encrypted image and decrypted image in sequence. Figures (3, 5, 7and 9) represent the corresponding histogram for each behind image.

Figures 4: The original image



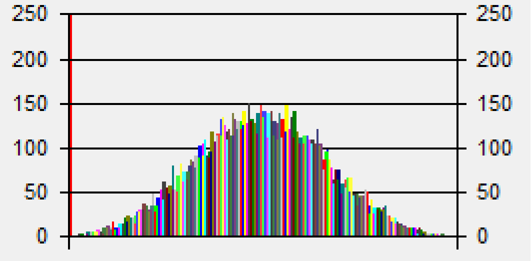
Figures 4: The plain image grayscale histogram (Plain image)

Figures 4: The key image



Figures 5: The key image grayscale histogram

Figures 6: Encrypted (Cipher) image

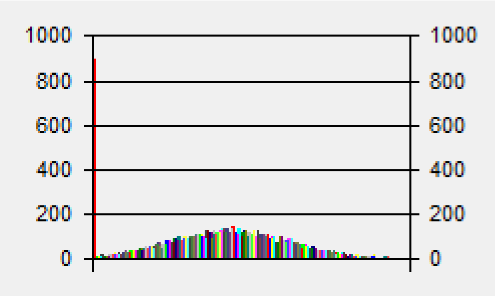


Figures 7: The cipher image grayscale histogram

Above figures shows that any note or signal can't presented or computed to statistical cryptanalysis to breaking the cipher system because the histogram of encrypted image (cipher image) uniform and fairly regularly, and is significantly different from the original image. In the other hand , some loss of image quality after performing encryption and decrypt the original image because of the use of gausses elimination method that the hill ciphering depend on in decrypted process as mentioned previously .Mathematically, there is the possibility of a lack of inverse matrix for a certain matrix and this possibility is very likely and I have stated in our work this possibility and repeat. Requirements to have an Inverse the region of interest of the image must be square .The determinant of the grid should not be zero. This is rather than the genuine number not being zero to have an opposite, the determinant must not be zero to have a reverse.[12]

A lot of mathematical calculation was faced, all the programming is pixel based, all the mathematical calculation was programmed .therefore, a little of slowness noticed. In case of message randomization, black pixels appear in the message image.

Figures 8: Decrypted Image Histogram



Figures 9: The Decrypted Image Grayscale

9. Result

It is recognizable that a genuine irregular image has a regular (flat) histogram a high entropy over the whole image , a low autocorrelation coefficient between neighbor pixels. Also, any picture block of a genuine arbitrary image ought to likewise accomplish a high entropy. This is a presumption that is genuine yet is overlooked in irregularity tests for image encryption. At the end, we accept that a image containing some image obstructs with low Shannon. Entropy scores is not preferably scrambled/arbitrary like, regardless of how high its worldwide Shannon entropy is.

The plaintext image is encoded by some image figure utilizing block handling.

Some image block, on the other hand, is scrambled by a feeble key. From the shading histogram, it is clear that such a frail does not impact the ciphertext circulations all that much. Albeit such a powerless key just prompts a constrained measure of data spillage, it might totally disclose the data of the image.

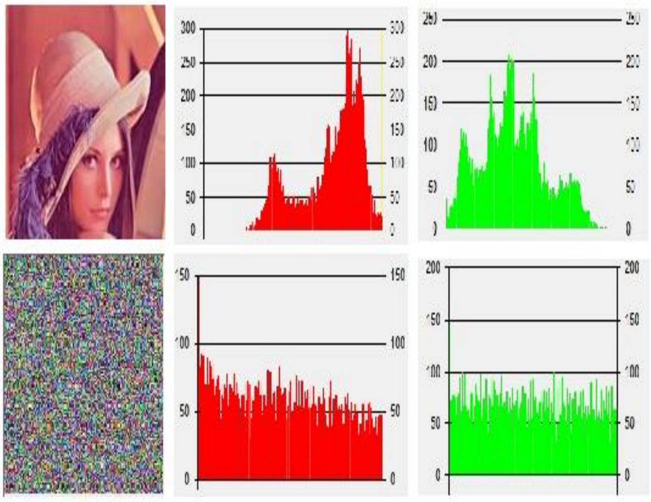


Figure 10: Color distribution comparison before and after the ciphering process

10. Conclusion

Textual algorithms used in proposed system to encrypted and decrypted digital color images. The main points the proposed system provided are:

1) The proposed system provide protection image against cryptanalyst and intruder.
2) Flat color distribution histogram of the ciphering image which can't determine any information about actual colors values of ciphering image.
3) less image quality loss to the decrypted image (the original image) because of the use of gausses elimination method that the hill ciphering depend on in decrypted process as mentioned previously
4) Integrity and authenticity presented such that any modified in image by illegal steals is sensed and no one can decrypt the cipher image and obtained the original image only how know the decryption keys which guarantee that the cipher image reached to the authorized one.
5) Good Speed of encryption and decryption algorithm with no need to especial hardware capability.

Reference

[1] Serberry, Jennifer and Joserf Pieprzyk, " Cryptography, An Introduction to Computer Security", Prentice Hall, 1989.

[2] Schneier, Bruce, " Applied Cryptography, Protocols, Algorithms, and Source Codes in C" , Second Edition, John Wiley & Sons, 1996.

[3] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, "Image Encryption Using Advanced Hill Cipher Algorithm", ACEEE international journal on signal and image processing vol1,no.1,Jan-2010.

[4] Payal Sharma, Manju Godara, Ramanpreet Singh, " Digital Image Encryption Techniques: A Review", International Journal of Computing & Business Research ,2012.

[5] Mohammad Ali Bani Younes and Aman Jantan ,"Image Encryption Using Block-Based Transformation

Algorithm‖ ", IAENG International Journal of Computer Science, 35,2008.

[6] C. Samson and Dr. V. U. K. Sastry, "cryptography of a gray level image and a color image using modern advanced hill cipher including a pair of involutory matrices as multiplicands and involving a set of function", Hyderabad, India, 2012.

[7] P.N.Khade, M.Narnaware,"3D Chaotic Functions for Image Encryption", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, N`o 1 p323-p328, May 2012.

[8] Z. Lv, Lei Zhang, J.Guo,"Symmetric Image Encryption Scheme Based on Composite Chaotic Dispersed Dynamics System",ISBN 978-952-5726-07-7 (Print), 978-952-5726-08-4 (CDROM) Proceedings of the Second Symposium International Computer Science and Computational Technology(ISCSCT '09) Huangsha, P.R. China, 26-28, pp. 191-194,Dec. 2009.

[9] Kh. Manglem Singh, S. Birendra Singh and L. Shyam Sundar Singh, "Hiding Encrypted Message in the Features of Images", IJCSNS, VOL. 7, No.4, April 2007.

[10] S.K.Bandyopadhyay, Debnath Bhattacharyya, Poulumi Das, S. Mukherjee, D. Ganguly, "A Secure Scheme for Image Transformation", IEEE SNPD, pp. 490-493, August 2008.

[11] Yarmolik, V. N.& S. N Demidenko, " Generation and Application of Pseudo Random Sequences for Random Testing " , John Wiley & Suns, 1988.

[12] Jackie Nicholas," The inverse of a n _ n matrix", Mathematics Learning Centre University of Sydney,2010.

[13] I. Ozturk, I.Sogukpinar, "Analysis and comparison of image encryption algorithm," Journal of transactions on engineering, computing and technology December, vol. 3, pp.38, 2004.

[14] William Stalling, " Cryptography and Network Security Principle and Practices, Fourth Edition", Prentice Hall, November 16, 2005.

Author Profile

Noor Dhia Kadhm Al-Shakarchy awarded her B.Sc, and M.Sc, at University of Technology, Department of Computer Science and information systems- information systems in 2000 and 2003 respectively. She is a lecturer at Karbala University, Collage of Science, Computer Department. Here research interests include: Object Modeling, Image processing such as Segmentation and Steganography, Data Security, Artificial intelligent, artificial intelligent applications and information systems.

Hiba Jabbar Al- Eqabie awarded her B.Sc, and M.Sc, at University of Alnahrain, , Science College, Computer Department in 2002 and 2006 respectively. She is a lecturer at Karbala University, Collage of Science, Computer Department. Here research interests include: Image processing such as Segmentation and Steganography, Data Security, graphics and information systems.

Huda Fawzi Al- Shahad awarded her B.Sc, and M.Sc, at University of Alnahrain, , Science College, Computer Department in 2002 and 2008 respectively. She is a lecturer at Karbala University, Collage of Science, Computer Department. Here research interests include: Image processing, Data Security, Artificial intelligent and artificial intelligent applications.