TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 18, No. 6, December 2020, pp. 2995~3002
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v18i6.14340

The quality of image encryption techniques by reasoned logic

Marwah Kamil Hussein[1], Kareem Radhi Hassan[2], Haider M. Al-Mashhadi[3]
[1,3]Department of Information Systems, University of Basra, Iraq
[2]Department of Computer Science, University of Basra, Iraq

Article Info

Article history:

Received Oct 17, 2019
Revised Mar 17, 2020
Accepted Mar 27, 2020

Keywords:

Correlation
Encryption
Entropy
Fuzzy logic
NPCR

ABSTRACT

One form of data is digital images, because of their widespread of frequent exchange over the Internet it is necessary to preserve the security and privacy of the images transmitted. There are many image encryption techniques that have different security levels and there are many standards and protocols for testing the quality of encryption security. The cipher images can be evaluated using various quality measuring criteria, these measures quantify certain features of the image. If there are many methods that can be applied to secure images; the question is what is the most powerful scheme that can be used among these methods? This research try to answer this question by taking three different encryption methods (RC5, Chaotic and Permutation) and measure their quality using the (PSNR, Correlation, Entropy, NPCR and UACI), the results of these criteria were input to a fuzzy logic system that was used to find the best one among them.

Corresponding Author:

Haider M. Al-Mashhadi,
Department of Information Systems,
University of Basra,
College of Computer Science and Information Technology, Garmat_Ali, Basra, Iraq.
Email: mashhad01@gmail.com

1. INTRODUCTION

The quality assessment is a very important tool in order to check the efficiency and effectiveness of the cryptographic algorithms. There are several methods in order to assess the cryptography techniques i.e. depending on the key length, the block or word length, number of the rounds, the execution time and so on. Techniques of the image encryption are widely used to ensure that the secure transmission for the image. Image quality assessment (IQA) can be divided into two types; the first is subjective method, which depends on human beings that assess the quality of the image. While the second method of IQA is the objective methods which can be assess a quality of the image automatically by using several criteria [1-10]. These criteria are widely used in order to evaluate the image quality.

The major idea behind this paper can be dividing into three stages:

- Stage 1: select the image in order to encrypt it by using three encryption techniques which are (RC5 [11], Chaotic [12] and Permutation [13]).
- Stage 2: Using the following metrics of the image encryption quality: Peek Signal to Noise Ratio (PSNR) [14], Correlation [15], Entropy [16], Number of Pixels Changes Rate (NPCR) and Unified Average Changing Intensity (UACI) [17,18]. To measure the encrypted image quality which results from stage 1; the result was fifteen values, five values for each encryption method.
- Stage 3: finally, using the five values of quality resulted from stage 2 as input to the fuzzy logic system (FLS), in order to assess a quality of each encryption techniques. The low result of FLS refers to the best

encryption method. By far, no such work in the field of quality assessment for image encryption techniques by using the fuzzy logic system.

Figure (1) shows the proposed method structure, the image is entered to the encryption method like (RC5) in order to produce a cipher image, after that, the cipher image will input to the quality analysis metrics to evaluate the method efficiency, results of the quality analysis are entering to the FLS to produce the value from FLS depending on the previous results of the quality analysis. This approach applied for other two methods (Chaotic and permutation) in order to determine the best method depending on the fuzzy logic system value. This paper was organized as follows. Section 2 describes the fundamentals of the image quality criteria. While, section 3 describes the fuzzy logic. Section 4 discusses the new scheme for quality analysis of encryption image methods by using the fuzzy logic technique. The experimental results of the new techniques were presented in section 5. Finally, the conclusions were presented in section 6

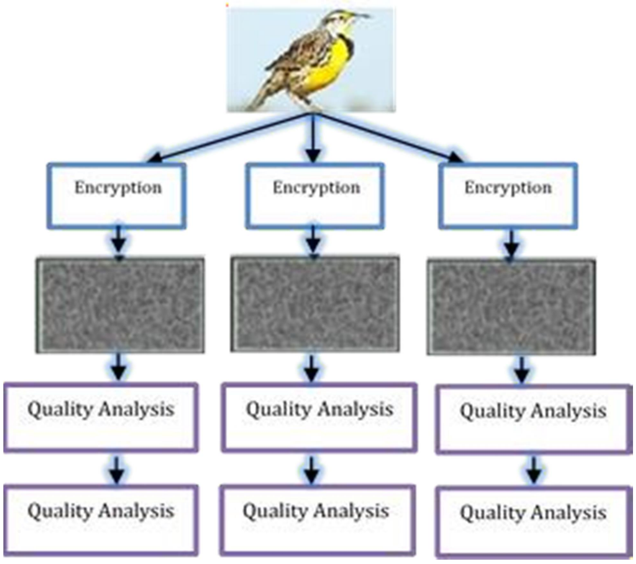

Figure 1. The structure of the quality assessment for image encryption methods using FLS

2. RESEARCH METHOD

The research present image quality evaluation method by explote the classical methods (PSNR, Correlation, Entropy, NPCR and UACI) with an artificial intelligent methods i.e. combine the ordinary image evaluation methods with the fuzzy logic system.

2.1. PSNR

PSNR is a criterion that used in order to measure the quality difference between the resulted images from the compression or the encryption, based on the original image. PSNR which depends on the Mean Square Error (MSE) can be calculated from (1) [19, 20].

$$MSE = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\left[x(m,n) - \hat{x}(m,n)\right]^2 \qquad (1)$$

MSE calculates an average of the error between the original image and the extracted image. PSNR can be calculated as shown in (2) [21, 22].

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \qquad (2)$$

The best value for PSNR is near to zero.

2.2. Corelation

Correlation is the quality analysis that used in order to measure the similarity between the plain image and the cipher image. The correlation can be calculated from (3).

$$\text{Corr} = \frac{\sum_{r=1}^{N}\sum_{c=1}^{M}(I1(r,c)-\bar{I}1)(I2(r,c)-\bar{I}2)}{\sqrt{[\sum_{r=1}^{N}\sum_{c=1}^{M}(I1(r,c)-\bar{I}1)2][\sum_{r=1}^{N}\sum_{c=1}^{M}(I2(r,c)-\bar{I}2)2]}} \quad \dots (3)$$

The best preferred correlation value is near zero.

2.3. Entropy

Entropy is the expected value (or average of information) which can be extracted from the message. The entropy represent the ratio or the quantity of information thet exist in the image, or how much information can be extracted from the image. It can be expressed by using (4).

$$H(s) = -\sum_{i=0}^{2^N-1} P(s_i)\log_2 P(s_i) \quad (4)$$

2.4. NPCR and UACI NPCR

NPCR and UACI NPCR determines the number of the pixels which their values change during the operation of encryption, while, UACI determines the ratio of the changes between two cipher-images. The scale of NPCR is [0, 1], the value 0 shows that there is no change in the pixels of imge1 and image2. While, value 1 shows that all pixels in image2 are different from image1. The scale of UACI is [0, 1], which the most preferred value is near to zero [23, 24].

3. FUZZY LOGIC

Fuzzy logic system has been adopted in order to solve many problems. FLS consists from four stages which are Fuzzification, inference engine, Rule base and Defuzzification as depicted in Figure 2 [25]. There are many types of FLS models like Mamdani and TSK model [26, 27].

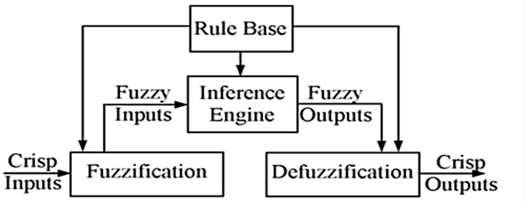

Figure 2. The fuzzy system

4. QUALITY EVALUATION USING FLS

The proposed technique is using three techniques which are (RC5, Chaotic and Permutation) in order to evaluate which of the three encryption algorithms is the more effective than others, by using the following steps:

- Select thre image to encrypt it by using Rc5, Chaotic and Permutation methods.
- The resulted image is evaluated by using the five quality analysis criteria (PSNR, Correlation, Entropy, NPCR, UACI). 3. Enter the quality analysis value which resulted from step to the fuzzyfication step of the FLS.
- Calculate the output value of the rule bases by mapping the (PSNR, Correlation, Entropy, NPCR, UACI) values to the corresponding fuzzy sets.
- Calculate the crisp output value using (5) and (6). Execute the previous steps for other methods (permutation and chaotic). Select the best method depending on the low crisp output value.

The fuzzy rule that implied is the Mamdani type rule with five values of the input (PSNR, Correlation, Entropy, NPCR and UACI) in order to produce one value as an output which represents the optimal value for the quality of the encryption method. Figure (3) represents the structure of FLS with the five inputs and one output and Figure (4) represents the triangle membership function which is used in this approach. The triangle membership function can be calculated by using (5).

$$\mu_A(x) = \begin{cases} \frac{x-low}{center\ -low} & low \le x \le center \\ \frac{x-high}{center\ -high} & center \le ..5 \quad high \\ 0 & othrwise \end{cases} \tag{5}$$

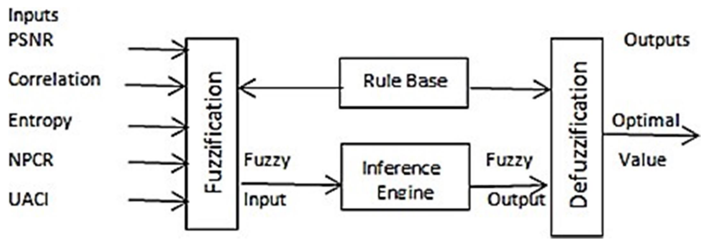

Figure 3. The structure of FLS using five inputs and one output of the optimal quality value for the encryption method

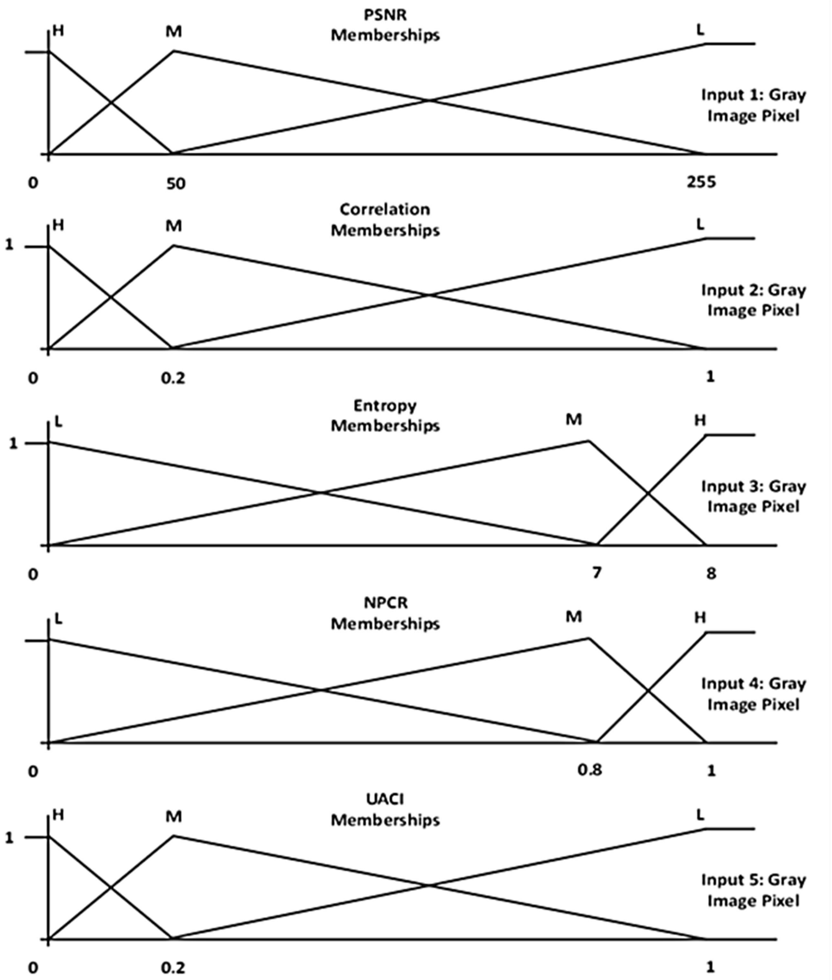

Figure 4. Representation of inputs membership function

In the quality assessment FLS, the input values are processed by using the inference engine, Table (1) shows the fuzzy rules which are used in FLS, the total number of fuzzy rule base is 3^5=243. For example, IF PSNR is Low, Correlation is Low, Entropy is Low, NPCR is High and UACI is Low, the Optimal value (output) is High. The rules run in the inference engine simultaneously. Finally, defuzzification stage finds that the optimal crisp value represents the output from the fuzzy space. This value represents the quality analysis for the method of encryption.

Table 1. Fuzzy rules of the technique

	VL	L	M	H	VH
VL	VH	VH	H	M	L
L	VH	H	H	M	L
M	H	H	M	L	VL
H	H	M	M	L	VL
VH	H	M	M	L	VL

Fuzzy system can be expressed by using the following procedure:

```
Procedure Fuzzy:// Procedure Quality Evaluatio
Begin
    Determine no. of membership function for.
Input1 such as PSNR=3
Input2 such as Correlation=3
Input3 such as Entropy=3
Input4 such as NPSR=3
Input5 such as UACI=3
Output such as Mo=5
      Input the values of PSNR, Corr, Ent, NPCR, UACI from the statistical analysis stage;
    Begin
        Calculate the membership function for the PSNR, Corr, Ent, NPCR, UACI, in the Input1…Input5
by (5); Put the result in Y1...Y5;
```

$$U^K = \sum_{i=1}^{m=1} \sum_{v=1}^{m=2} Yi * Yv$$

```
Calculate the degree of all fuzzy sets $U^k$ by the equation:
Using COG strategies to fixed encryption block as a crisp value according to:
```

$$\textbf{\textit{Optimal Value}} = \frac{\sum_{i=1}^{n} \boldsymbol{Ui * Ci}}{\sum_{i=1}^{n} \boldsymbol{Ui}}$$

```
End; End;
```

5. EXPERIMENTAL RESULTS

In order to evaluate the technique, three encryption algorithms were used (RC5, Permutation and Chaotic). Each one of these methods runs on eight different standard images which are (birds, boat, barco, house, star, peppers, boys and fingerprint). Table (2) represents values of the quality analysis metrics that resulted from RC5 encryption methods for eight images by using five metrics. Table (3) represents the values of FLS which evaluate the metrics of Table (2). Table (4) represents the quality analysis metrics that resulted from chaotic method of eight images. Table (5) represents the values of quality analysis using FLS which evaluate the metrics of Table (4). Table (6), represents the values of quality analysis metrics resulted from the Permutation encryption methods for eight images. Table (7) shows the quality analysis using fuzzy system that resulted from the metrics of the quality analysis for eight images. From Tables (2, 4, 6), it's very difficult to determine which one of three methods is the best to encrypt the image, depending on the ordinary metrics (PSNR, Correlation, Entropy, NPCR and UACI) because the values of these methods are very similar or very closer. So, values of these metrics are using as inputs to FLS in order to determine in precisely which one of these methods is better than the other. Tables (3, 4, 5) show the fuzzy logic values which used to determine a quality analysis for each encryption method.

Table 2. Metr ics of quality analysis for rc5 encıyption method

Image Name	PSNR Plain image vs cipher image	Corrdation Plain image vs cipher image	Entropy for cipher image	NPCR Plain image vs cipher image	UACI
Birds	43.2947	0.0278548	7.94921	0.9993	0.571291
Boat	43.4917	0.00167326	7.93313	1	0.490355
House	43.4073	0.0209042	7.94329	1	0.502669
Barco	43.4172	0.00320752	7.90872	1	0.639404
Boys	43.4806	0.0252667	7.77518	1	0.591233
Star	42.8029	0.0456949	4.8765	0.9998	0.801624
Peppers	43.4035	0.0200264	7.95373	1	0.516007
Finger-print	43.3416	0.0004241111	7.972999	1	0.044125

Table 3. Quality analysis using FLS to RC5 encryption method

Image Name	Birds	Boat	House	Barco	Boys	Star	Peppers	Finger-print
Fuzzy Logic	0.282274	0.258981	0.258991	0.304111	0.302259	0.594698	0.403435	0.470525

Table 4. Quality analysis metrics for Chaotic encryption method

Image Name	PSNR Plain image vs cipher image	Corrdation Plain image vs cipher image	Entropy for cipher image	NPCR Plain image vs cipher image	UACI
Birds	11.8263	0.00265036	7.30424	0.992218	0.196837
Boat	11.7637	7.814875	7.19046	0.990265	0.195799
House	11.6677	0.00239873	7.48304	0.993591	0.268934
Barco	9.38535	0.0010362	7.3561	0.991287	0.268934
Boys	10.5447	0.00032136	7.21731	0.987473	0.240348
Star	7.87947	0.00221533	4.11628	0.639038	0.282137
Peppers	9.67225	0.159637	0.0104066	1	0.257559
Finger-print	9.96458	0.0951743	0.0305328	1	0.0258193

Table 5. Quality analysis by using FLS to Chaotic encryption method

Image Name	Birds	Boat	House	Barco	Boys	Star	Peppers	Finger-print
Fuzzy Logic	0.588561	0.588232	0.593566	0.628818	0.595186	0.662544	0.599226	0.600087

Table 6. Quality analysis metrics for permutation encryption method

Image Name	PSNR Plain image vs cipher image	Corrdation Plain image vs cipher image	Entropy for cipher image	NPCR Plain image vs cipher image	UACI
Birds	11.8263	0.00265036	7.30424	0.992218	0.196837
Boat	11.7637	7.81487e-5	7.19046	0.990265	0.195799
House	11.6677	0.00239873	7.48304	0.993591	0.210841
Barco	9.38535	0.00101362	7.3561	0.991287	0.268934
Boys	10.5447	0.000312136	7.21731	0.987473	0.240348
Star	7.87947	0.00221533	4.11628	0.639038	0.282137
Peppers	10.6217	0.00516135	7.53269	0.994217	0.239001
Finger-print	10.9255	0.00349311	6.73171	0.9899	0.232249

Table 7. Quality analysis values by using FLS to Permutation method

Image Name	Birds	Boat	House	Barco	Boys	Star	Peppers	Finger-print
Fuzzy Logic	0.408072	0.412495	0.397225	0.380794	0.39548	0.414579	0.695494	0.414579

6. CONCLUSIONS

Quality assessment of the encryption methods is very important in order to determine the encryption mechanism strength. Several quality assessment methods which are implemented to determine the cryptographic method efficiency by using so many metrics. In this work, a new method of the quality assessment has been applied on three image encryption algorithms which are (RC5, Chaotic and Permutation), by calculating the quality analysis for each method by using five metrics (PSNR, Entropy, Correlation, NPCR and UACI), the results of these metrics enter to FLS in order to determine the fitness of each method of encryption. The results show that the best method was RC5. Therefore, FL quality assessment for the image encryption methods adds a new method in order to analytical comparison among the implemented methods. As a future work, exploring more methods and investigating the performance of using the methods to check its effectiveness by using FL system.

REFERENCES

[1] Sheikh H. R., Bovik A. C., "Image information and visual quality," *IEEE Transactions.on Image Processing*, vol. 15, no. 2, pp. 430-444, February 2006.

[2] You J., et al., "Perceptual quality assessment based on visual attention analysis," *in Proceedings of the 17th ACM international conference on* Multimedia, pp. 19-24, Oct 2009.

[3] Zhai G., Zhang W. and Lin W., "LGPS: Phase based image quality assessment metric," *IEEE Workshop on Signal Processing* Systems, pp. 605-609, Oct 2007.

[4] Liu Z. and Laganiere R., "On the use of phase congruency to evaluate image similarity." *IEEE International Conference on Acoustics Speech and Signal Processing Proceedings*, May 2006.

[5] Davis L. S., Wu Z. and Sun H., "Contour-based motion estimation." *Computer vision, Graphics, and. image Process*, vol. 23, no. 3, pp. 313-326, September 1983.

[6] Han S., Mao H. and Dally W. J. A., "Deep neural network compression pipeline: Pruning, quantization, huffman encoding." *arXiv Prepr*, February 2016.

[7] Fu W., GuX. and Wang Y., "Image quality assessment using edge and contrast similarity." *IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence)*, pp. 852-855, June 2008.

[8] Yap V. V., "Wavelet-based image compression for mobile applications." *Middlesex University*. 2005.

[9] Yang C.-L., Wang F. and Xiao D., "Contourlet transform-based structural similarity for image quality assessment." *IEEE International Conference on Intelligent Computing and Intelligent Systems*, pp. 175-179, November 2009.

[10] Alhijaj A. A. and Hussein M. K., "Stereo images encryption by OSA & RSA algorithms." *Journal Physics Conference Series*, vol.1279, no. 1, pp. 1-7, January. 2019.

[11] Hussein M. K., Alhijaj A, "TDL and Ron Rivest, Adi Shamir, and Leonard Adleman in Stereo images encrypt**."** *Journal of Advanced Research in Dynamical and Control Systems*-JARDCS, vol. 11, no. 01, pp. 1811-1817, 2018.

[12] Sathishkumar G.A., Bhoopathy K., Siriaam N., "Image encryption based on diffusion and multiple chaotic maps." *International Journal of Network Security & Its Applications*, vol. 3, no. 2, pp. 181-194, 2011.

[13] Sesha P., Indrakanti, Avadhani P. S., "Permutation based Image encryption technique." *International Journal of Computer Applications*, vol. 28, no. 8, pp.45-47, August 2011.

[14] Wang Z., Bovik A. C., Sheikh H. D. and Simoncelli E., "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 4, no. 4, pp. 600-612, April 2004.

[15] Xuehu Yan, et al., "A new assessment measure of shadow image quality based on error diffusion techniques." *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no.2, pp. 118-126, January 2013.

[16] Shannon C.E., "Communication theory of secrecy systems."' *Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, Oct 1949.

[17] Chen G., Mao Y. and Chui C. A., "Symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749-761, July 2004.

[18] Mao Y., Chen Y. and Lian S. A., "Novel fast image encryption scheme based on 3D chaotic baker maps, *International Journal of Bifurcation and Chaos*, vol. 14, no. 10, November 2011.

[19] Sencar H.T., Ramkumar M., Akansu A.N., "Data hiding fundamentals and applications." *New York, Elsevier Academic Press*. 2004.

[20] Chang C.C., Lin C.C., Chen Y.H., "Reversible data-embedding scheme using differences between original and predicted pixel values." *IET Information Security*, vol. 2, no. 2, pp. 35-46, June 2008.

[21] Hussein M. K., Abdul-Kareem H., "Video compression for communication and storage using wavelet transform and adaptive rood pattern search matching algorithm," *Al-Mustansiriyah Journal of Science*, vol. 24, no. 5, pp. 393-406, January 2013.

[22] Dirankov D., Hellendron H. and Reinfrank M., "An introduction to fuzzy control," *Springer New York*. 1993.

[23] Haider M., Al-Mashhadi, Iman Q. Abduljaleel, "Color image encryption using chaotic maps, triangular scrambling, with DNA sequences," *International Conference on Current Research in Computer Science and Information Technology (ICCIT)*, pp. 93-98, April 2017.

[24] Haider M., Al-Mashadi, Ala'a A. Khalaf, "Hybrid homomorphic cryptosystem for secure transfer of color image on public cloud," *Journal of Theoretical and Applied Information Technology*, vol. 96, no. 19, pp. 6474-6486, Oct 2018.

[25] Mitaim, Sanya, and Bart Kosko, "The shape of fuzzy sets in adaptive function approximation." *IEEE Transactions on Fuzzy Systems,* vol. 9, no. 4, pp. 637-656, August 2001.

[26] Schmidt M., Stidsen T., "Hyprid system: genetic algorithms, neural networks, and fuzzy logic." *Denmark*. 1996.

[27] Hussein M. K., "Encryption of stereo images after estimated the motion using spatially dependent algorithms." *International Journal of Computer Science and Mobile Computing*, vol. 5, no. 12, pp. 150-159, Dec 2016.

BIOGRAPHIES OF AUTHORS

Marwah K. Hussein is a lecturer in computer information systems since (2013), University of Basra in Iraq. Her current research interests included information security, Video and image processing.

Dr. Kareem Radhi Hassan, he Is an assistant professor in Computer system department, since (1996), university of Basrah, Iraq. His current research interests include information security, IoT, GIS, AI.

Dr. Haider M. Al-Mashhadi, he is a professor in computer information systems department since 2003, university of Basrah, Iraq. His research interests in the network and information security, IoT, embedded systems, AI and image processing.