Quality Assessment for Image Encryption Techniques using Fuzzy Logic System

Haider M. Al-Mashhadi
University of Basrah,
College of Computer
Science and Information Technology,
Computer Information Systems Dept.,
Basrah, Iraq.

ABSTRACT
There are many applications in image processing field; one of them is how to secure the image during transmission. In many cases there are different methods to encrypt the image. Each one of them has a different level of security that can be determined by using quality assessment techniques. The cipher image 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. The fuzzy logic output determine the degree of effectiveness for each method, many experiments have been executed on various images to show the ability of work to assess quality of the encryption method.

General Terms
Quality Assessment Mechanisms using Fuzzy Logic.

Keywords
Correlation, encryption, entropy, fuzzy logic, NPCR, PSNR, quality assessment, UACI.

1. INTRODUCTION
Quality assessment is a very important tool to check the efficiency and effectiveness of cryptographic algorithms. There are many methods to assess cryptography techniques i.e. depending on the length of key, the length of block or word, the number of rounds, execution time and so on. Image encryption techniques are widely used to ensure the secure transmission for the image. Image quality assessment (IQA) can be divided into two types; the first is subjective method which depends on the human beings assess the quality of an image. The second method of IQA is the objective methods that can be assess the quality of an image automatically using various criteria [1-14]. These criteria are widely used to evaluate the quality of image. The main idea behind this paper can be dividing into three stages:

Stage 1: select an image to encrypt using three encryption techniques (RC5 [15], Chaotic [16] and Permutation [17]).

Stage 2: Using the following image encryption quality metrics: Peek Signal to Noise Ratio (PSNR) [18], Correlation [19], Entropy [20], Number of Pixels Changes Rate (NPCR) and Unified Average Changing Intensity (UACI) [21, 22]. To measure the quality of encrypted image that results from the stage 1; the result is 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), to assess the 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 using fuzzy logic system.

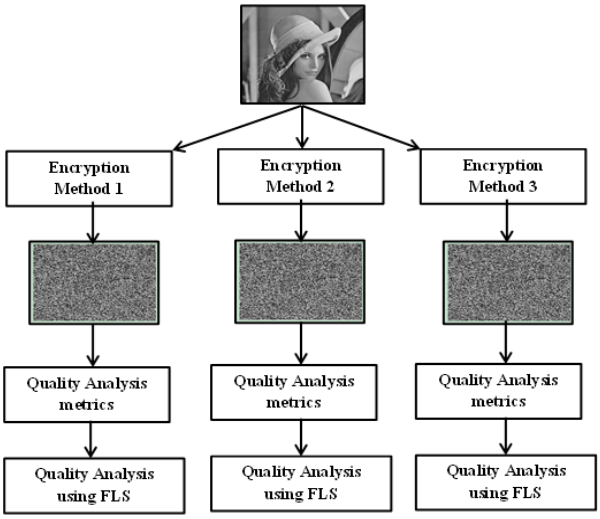

Fig 1: The Structure of the Quality Assessment for Image Encryption Methods using FLS.

Figure (1) shows the structure of the proposed method, the image is entered to the encryption method like (RC5) to produce the cipherimage, the cipherimage then input to the quality analysis metrics to evaluate the efficiency of the method, the results of the quality analysis are enter to the FLS to produce a value from the FLS depending on the previous quality analysis results. This approach applied for the other two methods (Chaotic and permutation) to determine the best method depending on the value of the fuzzy logic system.

This paper is organized as follows. Section 2 describes the fundamentals of the image quality criteria. Section 3 describes the fuzzy logic. Section 4 discusses the new scheme for quality analysis of encryption image methods using fuzzy logic technique. The experimental results of the new techniques are presented in section 5. The conclusions are presented in section 6.

2. FUNDAMENTALS OF THE IMAGE QUALITY CRITERIA

In this section, the fundamentals of the image quality criteria are described in details.

2.1 PSNR

The PSNR is a criteria used to measure the quality difference between the resulted images from compression or encryption, based on the original image.

PSNR depends on the Mean Square Error (MSE) that can be calculated from equation (1) [23, 24].

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

MSE calculates the average of error between the original image and the extracted image.

PSNR can be calculated as shown in equation (2) [25, 26].

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

The best value for PSNR is near to zero.

2.2 Correlation

Correlation is a quality analysis used to measure the similarity between the plainimage and the cipherimage. The correlation can be calculated from equation (3).

$$Corr = \frac{\sum_{r=1}^{N}\sum_{c=1}^{M}(I_1(r,c) - \bar{I}_1)(I_2(r,c) - \bar{I}_2)}{\sqrt{[\sum_{r=1}^{N}\sum_{c=1}^{M}(I_1(r,c) - \bar{I}_1)^2][\sum_{r=1}^{N}\sum_{c=1}^{M}(I_2(r,c) - \bar{I}_2)^2]}} \quad \ldots (3)$$

The best preferred value of correlation is near the zero.

2.3 Entropy

Entropy is the expected value (or average of information) that can be extracted from the message, and expressed by equation (4).

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

2.4 NPCR and UACI

NPCR determines the number of pixels that their values change during the encryption operation, while, UACI determines the ratio of changes between two cipher-images.

The scale of NPCR is [0, 1], the value 0 shows that there is no change in pixels of imge1 and image2. Value 1 show that all pixels in image2 are different from image1.

The scale of UACI is [0, 1], the most preferred value is near to zero.

3. FUZZY LOGIC

Fuzzy logic system has been adopted in solving many problems. The FLS consists of four stages Fuzzification, Rule base, Inference engine and Defuzzification as depicted in figure (2) [27- 29].

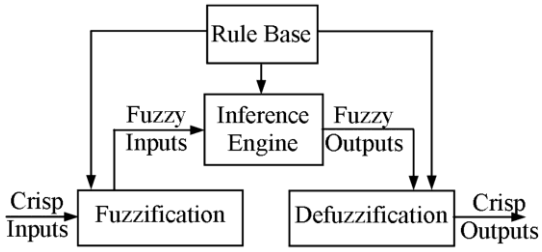

Fig 2: The Fuzzy System (FS).

There are many types of FLS models like Mamdani and TSK model [30, 31].

4. QUALITY ASSESSMENT USING FLS

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

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

Select the best method depending on the low crisp output value.

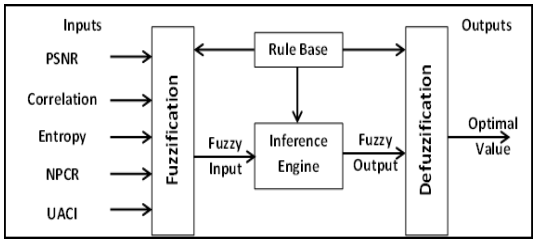

Fig 3: The structure of FLS using five inputs and one output of the optimal quality value for the encryption method.

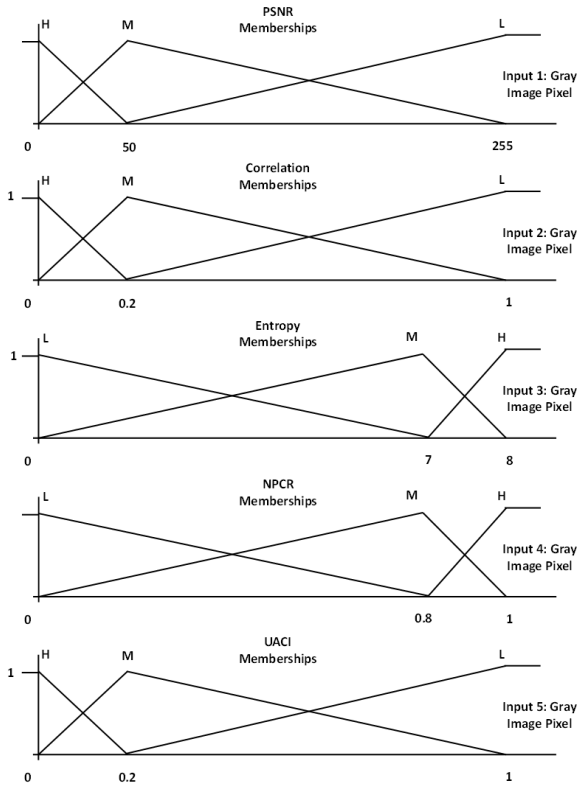

Fig. 4: Representation of inputs membership functions.

The fuzzy rule which implied is the Mamdani type rule with five values of input (PSNR, Correlation, Entropy, NPCR and UACI) to produce one value as an output that represents the optimal value for quality of the encryption method. Figure (3) represents the structure of FLS with 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 equation (5).

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

Where *x* is a crisp input value.

In quality assessment FLS, the input values are processed by the inference engine, Table (1) shows the fuzzy rules 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 an inference engine simultaneously. Finally, the defuzzification stage finds the optimal crisp value that represents the output from the fuzzy space. This value represents the quality analysis for the encryption method.

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

The fuzzy system can be expressed by the following procedure:

Procedure Fuzzy ; // Procedure Quality Evaluation

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 NPCR =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 functions for the PSNR, Corr, Ent, NPCR, UACI in the input1..Input5 by the equation 5, put the result in Y1..Y5;

$$U^k = \sum_{j=1}^{m1} \sum_{v=1}^{m2} Yi * Yv$$

Calculate the degree of all fuzzy sets U^k by the equation:

Using COG strategies to find encryption block as a crisp value according to:

$$OptimalValue = \frac{\sum_{i=1}^{n} Ui * ci}{\sum_{i=1}^{n} Ui}$$

End;

End;

5. EXPERIMENTAL RESULTS

To evaluate the technique we used 3 encryption algorithms (RC5, Permutation and Chaotic). Each method runs on eight different standard images (birds, boat, house, barco, boys, star, peppers and fingerprint).

Table 2: Quality analysis metrics for RC5 encryption method

Image Name	PSNR Plain image vs cipher image	Correlation 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
Fingerprint	43.3416	0.000424111	7.97299	1	0.044125

Table (2), represents the values of quality analysis metrics resulted from the RC5 encryption methods for eight images using the five metrics.

Table 3: Quality analysis by using FLS to RC5 encryption method

Image Name	birds	boat	house	barco	boys	star	peppers	finger-print
Fuzzy	0.282274	0.258981	0.258991	0.304111	0.302259	0.594698	0.403435	0.470525

Table (3), represents the values of FLS that evaluate the metrics of table (2).

Table (4): Quality analysis metrics for Chaotic encryption method

Image Name	PSNR Plain image vs cipher image	Correlation 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**
Pep-pers	**9.67225**	**0.159637**	**0.0104066**	**1**	**0.257559**
Finger-print	**9.96458**	**0.0951743**	**0.0305328**	**1**	**0.0258193**

Table (4), represents the quality analysis metrics resulted from chaotic method of eight images.

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 (5), shows the quality analysis metrics by using fuzzy system resulted from the quality analysis metrics for the eight images.

Table (6): Quality analysis metrics for permutation encryption method

Image Name	PSNR Plain image vs cipher image	Correlation 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 (6), represents the values of quality analysis metrics resulted from the Permutation encryption methods for eight images.

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	0.395488	0.414579	0.695494	0.414579

Table (7), shows the quality analysis by using fuzzy system resulted from the quality analysis metrics for the eight images.

From tables (2, 4, 6) it's very difficult to determine which one of the 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 the values of these metrics are using as inputs to the FLS 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 the quality analysis for each encryption method.

6. CONCLUSIONS

The quality assessment of encryption methods is important to determine the strength of the encryption mechanism. Several quality assessment methods are implemented to determine the efficiency of the cryptographic method using many metrics. In this work, a new quality assessment method has been applied on three image encryption algorithms (RC5, Chaotic and Permutation), by calculating the quality analysis for each method using five metrics (PSNR, Entropy, Correlation, NPCR and UACI), the results of these metrics enter to FLS to determine the fitness of each encryption method. Results show that the best method is RC5.

Therefore, the FL quality assessment for image encryption methods adds a new method to analytical comparison among the implemented methods.

As a future work, exploring more methods and investigating the performance of using methods to check its effectiveness using FL system.

7. REFERENCES

[1] H. R. Sheikh and A. C. Bovik, 2006. Image information and visual quality, IEEE Transaction on Image Processing 15, pp. 430–444, 2006.

[2] Z. You, A. Perkis, M. M. Hannuksela, and M. Gabbouj,

2009. Perceptual quality assessment based on visual attention analysis, in: Proceedings of ACM International Conference on Multimedia, Beijing, China, pp. 561-564, 2009.

[3] G. Zhai, W. Zhang, Y. Xu, and W. Lin, 2007. LGPS: Phase based Image Quality Assessment Metric, in: Proceedings of IEEE Workshop Signal Processing Systems, Shanghai, China, pp. 605-609, 2007.

[4] Z. Liu and R. Laganiere, 2006. On the use of phase congruency to evaluate image similarity, in: Proceedings of International Conference on Acoustics, Speech, Signal Processing, Toulouse, France, pp. 937-940, 2006.

[5] D. M. Chandler and S. S. Hemami, 2007. VSNR: A wavelet-based visual signal-to-noise ratio for natural images, IEEE Trans. Image Processing 16, pp. 2284-2298, 2007.

[6] R. Ferzli and L. J. Karam, 2007. A no-reference objective image sharpness metric based on just-noticeable blur and probability summation, in: Proceedings of International Conference on Image Processing, San Antonio, TX, pp. 445–448, 2007.

[7] F. Wei, X. Gu, and Y. Wang, 2008. Image quality assessment using edge and contrast similarity, in: Proceedings of IEEE International Joint Conference on Neural Networks, Hong Kong, China, pp. 852–855, 2008.

[8] C.-L. Yang, W.-R. Gao, and L.-M. Po, 2008. Discrete wavelet transform-based structural similarity for image quality assessment, in: Proceedings of IEEE International Conference on Image Processing, San Diego, CA, pp. 377-380, 2008.

[9] A. Shnayderman, A. Gusev, and A. M. Eskicioglu, 2006. An SVD-based grayscale image quality measure for local and global assessment, IEEE Transaction on Image Processing 15, pp. 422–429, 2006.

[10] H.-S. Han, D.-O Kim, and R.-H. Park, 2006. Structural information-based image quality assessment using LU factorization, IEEE Transaction on Consumer Electronics 55, pp. 165–171, 2006.

[11] D.-O Kim and R.-H. Park, 2006. "New image quality metric using the Harris response, IEEE Signal Processing Letters 16, pp. 616–619, 2006.

[12] D.-O Kim and R.-H. Park, 2007. "Joint feature-based visual quality assessment, Electronics Letters 43, pp. 1134-1135, 2007.

[13] L. Cui and A. R. Allen, 2008. An image quality metric based on corner, edge and symmetry maps, in: Proceedings of British Machine Vision Conference, Leeds, UK, 2008.

[14] G.-H. Chen, C.-L. Yang, and S.-L. Xie, 2006. Gradient-based structural similarity for image quality assessment, in: Proceedings of International Conference on Image Processing, Atlanta, GA, pp. 2929–2932, 2006.

[15] R. Rivest. "The RC5 Encryption Algorithm," In: Proceedings of the Leuven Workshop on Fast Software Encryption, pp. 86–96, Springer Verlag, 1995.

[16] G.A.sathishkumar, K.Bhoopathy, N.Siriaam, "Image Encryption Based on Diffusion and Multiple Chaotic Maps", International Journal of Network Security & Its Applications, Vol: 3, No: 2, pp: 181-194, 2011.

[17] Sesha P. Indrakanti, P.S.Avadhani, "Permutation based Image Encryption Technique", International Journal of Computer Applications. Vol: 28, No: 8, pp: 45-47, 2011.

[18] Z. Wang, A.C. Bovik, H.D. Sheikh, E.P. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," IEEE Transactions on Image Processing, Vol. 13, pp. 600–612, 2004.

[19] 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, Volume 4, Number 2, April 2013.

[20] C.E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, vol. 28, No. 4, pp. 656-715, October 1949.

[21] G. Chen, Y. Mao, and C. Chui, "A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps," Chaos, Solitons and Fractals, vol. 21, pp. 749-761, 2004.

[22] Y. Mao, G. Chen, and S. Lian, "A Novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps," Int. J. Bifurcation and Chaos in June, 2003.

[23] H.T. Sencar, M. Ramkumar, A.N. Akansu, "Data Hiding Fundamentals and Applications," New York, Elsevier Academic Press, 2004.

[24] C.C. Chang, C.C. Lin, Y.H. Chen, "Reversible Data-Embedding Scheme using Differences Between Original and Predicted Pixel Values," IET Information Security, Vol. 2, pp. 35–46, 2008.

[25] A.N. Netravali, B.G. Haskell, "Digital Pictures: Representation, Compression and Standards", New York, Plenum Press, 1995.

[26] M. Rabbani, P.W. Jones, "Digital Image Compression Techniques," Washington, SPIE Optical Engineering Press, 1991.

[27] L. Zadeh. "Fuzzy sets," Information Control, pp. 338-353, 1965.

[28] Dirankov, D., H. Hellendron, and M. Reinfrank. "An Introduction to Fuzzy Control," Springer New York, 1993.

[29] Mitaim, Sanya, and Bart Kosko. "The shape of fuzzy sets in adaptive function approximation." Fuzzy Systems, IEEE Transactions on 9.4 (2001): 637-656.

[30] K. M. Passino, S. Yurkovich, "Fuzzy Control," Adison Wesley Longman Inc., 1998.

[31] M. Schmidt, T. Stidsen, "Hyprid System: Genetic Algorithms, Neural Networks, and Fuzzy Logic," Denmark, 1996.