TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 18, No. 1, February 2020, pp. 289~300
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v18i1.13293

Iris images encryption based on QR code and chaotic map

Raniah Ali Mustafa, Amal Abdulbaqi Maryoosh, Dena Nadir George, Waleed Rasheed Humood
Department of Computer Science, Collage of Education, Mustansiriyah University, Iraq

Article Info

Article history:

Received Jun 10, 2019
Revised Jul 27, 2019
Accepted Aug 18, 2019

Keywords:

Binarization
Histogram equalization
Image encryption
Logistic map
QR code

ABSTRACT

In this paper an Iris image is encrypted based on QR (quick response) code and chaotic map. The main idea of the proposed system is generating a QR code depending on the input text and then extract the features from QR code by using convolution, these features are used for key generation. After that the permuted iris image is encrypted by using generated key, after that the resulting image will be encrypts using 2D logistic map. The randomness of generated key is tested using the measures of NIST, and quality of images that encrypted in this method are tested by using security analysis tests such as PSNR, UACI, NPCR, histogram, correlation and entropy. The security analysis shows that the proposed system is secure for iris image encryption.

Corresponding Author:

Amal Abdulbaqi Maryoosh,
Department of Computer Science, Collage of Education,
Mustansiriyah University, Iraq.
Email: amalmaryoosh@uomustansiriyah.edu.iq

1. INTRODUCTION

At this time, users attempt to select a shorter password to authenticate their accounts. The password may be easy forgotten and it can be easily attacked. Widely used technologies such as voice recognition, Bar-code, Fingerprint scanning, iris recognition and face recognition now play an important role, particularly in security-related applications [1]. The bar code is one dimensional and becomes illegible when damaged. Bar-code has some disadvantage like it stores only up to 20 digits. For this reason, in the bar code, we cannot store passwords or complex phrases, so it doesn't provide the best method for authentication. QR codes are 2D barcode can be read from any orientation and it has the ability to hold up to 4,296 characters alphabetically. Another feature of QR code is that it can be read after partly damaged. Make its feature of QR code very strong and popular in the security and advertising industry [2]. For this reason, QR code is chosen in this paper.

Several published works are related to the objectives of this work for example, Sim Hiew Moi et al. [1] present a new approach by using iris template to create a unique and more secure encryption key and used AES algorithm to encrypt and decrypt data of identity data. Tejas Mohod et al. [2] implement a system that takes properties of both iris and QR code; this enhances system isolation, cost effective and reliable security system. M. A. Murillo-Escobar et al. [3] proposed a new fingerprint template protection based on logistic map and Murillo-Escobar's algorithm. Mohammad Soltani and Amid Khatibi Bardsiri [4] proposed a hybrid algorithm for encryption and steganography, they generated the QR-code using input text and encrypted the resulting QR image using 2D logistic map then convert the encrypted QR to text, after that they encrypted the original text using AES algorithm and hiding it using LSB algorithm. Sruthi B. Asok et al [5] extracts a secret key from iris image and use it to encrypt data. Nishi Prasad et al. [6] Used three level of security for image encryption. They used logistic map, secret key cryptography, and QR codes. M. Mary Shanthi Rani and K. Rosemary Euphrasia [7] proposed an encryption method by using QR code for message encryption and generate another QR code for authentication and hiding it in cover image. A. Husain and R. Ali [8] increased the security of finger print image based on QR code to extract encryption key. In this paper there is a weakness in the quality of encrypted image, so we suggest a modifying for this method to get better results.

In this paper, a new algorithm is proposed for Iris image encryption based on QR code feature extraction and chaotic map. This algorithm will increase the security of Iris image by using QR code to generate the key, high diffusion that provided by permutation method and the chaotic system that provides the confusion. The randomness of the key that generated using QR code was tested using NIST tests and proved to be efficient. The results of this work are compared with the results of [8] by histogram, entropy, UACI, NPCR, correlation and PSNR. The experimental results show that the proposed approach is more efficient and secure for iris image encryption. The reminder of this paper is arranged as follows. In section 2 the methods that used in proposed algorithm will be presented. In section 3 the proposed method is described in details. In section 4 QR key NIST tests will be display. The security analysis is shown in section 5. Finally, the conclusions are shown in section 6.

2. THEORETICAL BACKGROUND

2.1. Quick response code

The quick response (QR) Code was first designed by Japanese company for cars industry called Denso-Wave in 1994 to track car parts. QR code is kinds of bar-code that can be recognize using a bar-code reader. It can contain encoded information like website URLs, data, and texts, etc. Today, QR codes are widely used as it used in companies, businesses and government departments because of their reliability and ease of use [2, 9]. Also, QR can use in security purpose. The information contained in the code can be encrypted and decrypted by using special software ensuring better security. QR structure is shown in Figure 1. QR codes contain many areas that explain as follow:

a) Finder pattern: It consists of 3 symmetrical structures at three corners of the QR code with one missing at the bottom right. Each pattern is based on a 3x3 matrix of black modules surrounded by white modules that are again surrounded by black modules. The finder patterns enable the decoder software to recognize the QR Code and determine the correct orientation [10].
b) Timing pattern: this pattern for discovering the central coordinate of each data cell the QR code with black and white designs are placed alternately in two places horizontally and vertically between the finder patterns. even if the code is distorted partially or an error for the cell pitch, this allows accurate reading of central coordinates. It tracks the time of incoming code [11, 12].
c) Alignment pattern: a model for correcting the distortion of the code. It is particularly efficient for correcting nonlinear distortions. The central coordinate of the alinement pattern will be discovered to correct the distortion of the symbol. For this purpose, an isolated black cell is directed in the conjunction pattern for getting it easy to detect the central coordinate of the alignment pattern [13].
d) Quiet zone: this area empties from any markings. A margin space is needed for reading QR code rightly. This free zone makes the QR code symbol easy to read by the CCD sensor [14].
e) Data area: in this area the QR code data and error correction code will be stored. The data area is represented by the grey area in Figure 1. The data will be encoded into 1's and 0's. The binary numbers will be converted into white and black cells and then will be arranged [14].

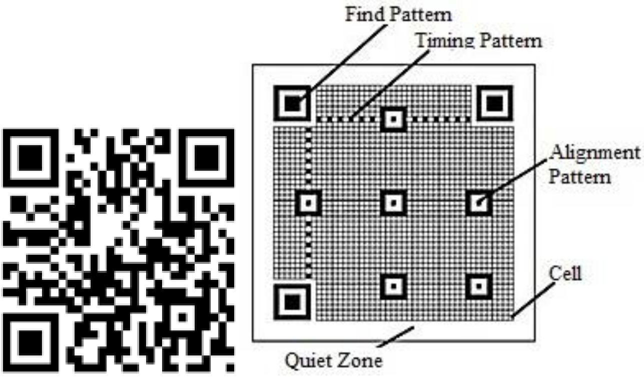


Figure 1. QR structure

2.2. Logistic map

A one-dimensional logistic map is described in the following equation:

$$x_{n+1}=\mu x_n (1-x_n) \quad (1)$$

where x_n refer to the nth output and μ is the map's parameter and the range of it should be within the period (3.56, 4]. The initial value x_0 and μ can be used as a key of encryption [15]. While the 2D logistic has more complex behaviors in image encryption than a 1D logistic map for this reason this paper use it to encrypt images. 2D logistic map can be show as follow [4]:

$$\begin{aligned} x_{n+1} &= r(3y_n+1)x_n(1-x_n) \\ y_{n+1} &= r(3x_{n+1}+1)y_n(1-y_n) \end{aligned} \quad (2)$$

where r is the parameter of system and (x_n, y_n) is is the pair-wise point at the n iteration. As shown in Figure 2 the scatter plot of 30,000 points of 2D logistic map using the parameter r = 1.19 and the initial value (x_0, y_0) at (0.8309,0.3342).

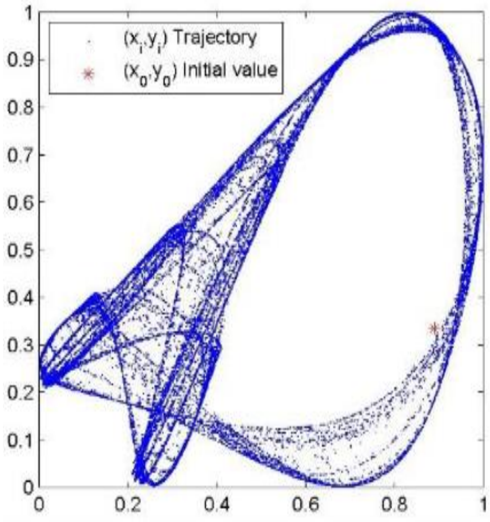


Figure 2. A trajectory of 2D logistic map [4]

3. PROPOSED SCHEME

The proposed scheme contains three main operations are: permutation, encryption with QR key and encryption with 2D logistic map. The general system structure is shown in Figure 3.

3.1. Permutation method

Permutation is most significant step in this algorithm. It works to block the high correlation among pixels of image to increase the security of image encryption algorithm. In this method we relied on scrambling rows and columns based on sum invariance of row and column through circular shift process. In the beginning it shifts each row in image by the total sum of the row and column's pixel values and save the result in a variable, and then implement the same method in each column and save the result in another variable. Finally, implement Xor operation between the two results. Figure 4 shown the plain iris image and the resulting image after permutation.

3.2. QR key generation

The first step is generating the QR code depending on the input text, then implement preprocessing operations such as histogram equalization and binarization on QR image. After that the features will be extracted from QR image by using convolution. These features are representing a random key which used to first encryption process.

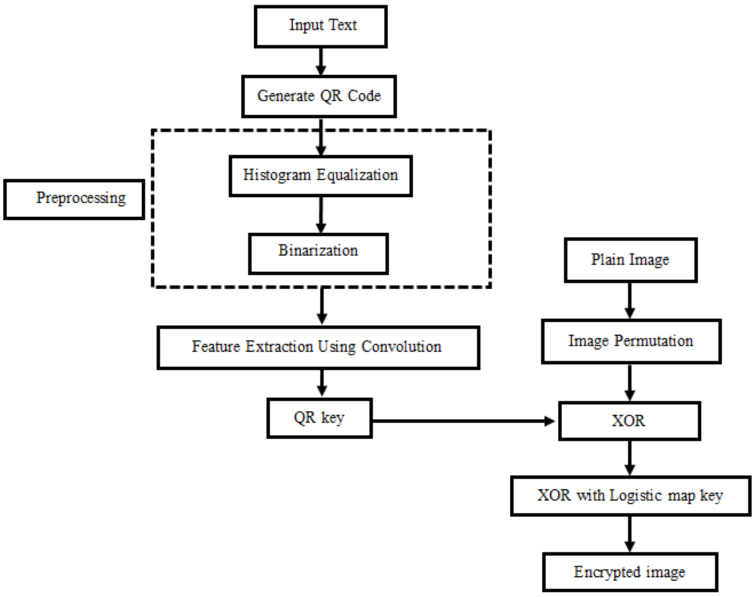


Figure 3. General structure of proposed system

(a)

(b)

Figure 4. (a) Plain iris image, (b) Permuted iris image

3.3. Histogram equalization

It's a method for adjust image contrast. Let f be an image represented as a matrix r x c of integer pixel intensities ranging from 0 to L-1. Where L is the number of gray level values in image, often 256. Let p is the normalized histogram of f [16].

$$p_n = \frac{\text{number of pixels with intensity n}}{t\text{otal number of pixels}} \tag{3}$$

The histogram equalized image g will be defined by:

$$g_{i,j} = floor((L - 1)\sum_{n=0}^{f_{i,j}} p_n) \tag{4}$$

in this paper, after transform any input text to QR code, the next step is histogram equalization and the result of this step shown in Table 1.

Table 1. The result for QR code, histogram equalization and binarization

No. bit of text	8-bit	16-bit	24-bit	32-bit	40-bit	48-bit
QR Code						
Histogram Equalization						
Binarization						

3.4. Binarization

Binarization is the process of convert a gray level image to binary image, this step is an important step to distinguish black-and-white module accurately in QR code images. So, we proposed use binarization operation to extract the features from QR image. In this method, the QR code is divided into 16x160-bit blocks. The value of the intensity of these blocks is analyzed and the pixel value is then determined as 1 if the pixel value is greater than the average intensity of that block, otherwise make it equal to 0. Table 1 shows the result of QR code, histogram equalization and binarization for number bit of text (8-bit, 16-bit, 24-bit, 32-bit, 40-bit, 48-bit).

3.5. Feature extraction using convolution

The convolution between two functions $f(x), g(x)$ which we denote by $(f * g)\ (t)$, the convolution gives the inverse Laplace transform of a product of two transformed functions, for this reason it's an important construct [17]:

$$L^{-1}\ (F(s)\ G(s))=(f * g)\ (t) \tag{5}$$

If $f(x), g(x)$ are causal functions then their convolution is defined by:

$$(f * g)\ (t) = \int_0^t f(t-r)g(r)dx \tag{6}$$

the proposed system used convolution for extract the features from QR code to generate random key. Table 2 shows the masks that used in convolution, and the best result histogram equalization and convolution illustrate in the Table 3.

Table 2. The masks that used in convolution

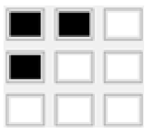
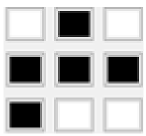
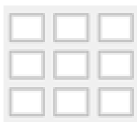
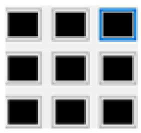
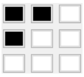
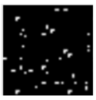
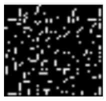
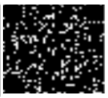
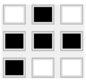
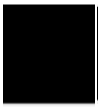
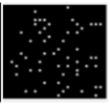
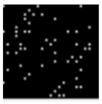
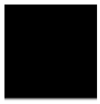
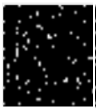
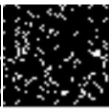
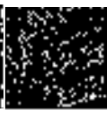
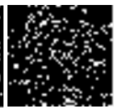
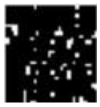
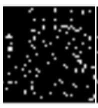
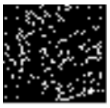
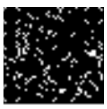
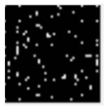
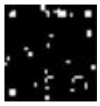
Matrix	No.	3x3 masks	Convolution Matrix
	1		
	2		
	3		
	4		

Table 3. The best result of histogram equalization and convolution

No	Masks		1	2	3	4	5	6	7	8	9
1		Convo									
		Hist	73	217	386	271	270	490	225	93	0
2		Convo									
		Hist	0	56	455	520	444	495	55	0	0
3		Convo									
		Hist	95	211	320	225	252	291	243	121	161
4		Convo									
		Hist	121	243	291	252	225	320	211	95	106

3.6. Encryption algorithm

Input: plain image (*m*), *QR_key*, *Logistic_key*
Output: encrypted image (*E*)
Step1: read colored image (*m*)
Step2: for *c*←1: size (*m*)
    I_1← circular_shift (sum (*m* (column)))
  end
  for *r*←1: size (*m*)
    I_2← circular_shift (sum (*m* (row)))
  end
  p← xor (I_1, I_2)
Step3: *k*← xor (*QR_key*, *p*)
Step4: *E*← xor (*Logistic_key*, *k*)
Step5: end

4. SECURITY ANALYSIS

In this section we present a series of tests results to proof the effectiveness of the proposed scheme and compare the results with [8]. In this test we used dataset that captured by Michal Dobeš and Libor Machala. The dataset contains 3x128 iris images. The irises images were scanned using TOPCON TRC50IA optical device connected with SONY DXC-950P 3CCD camera [18]. The experiments are performed via Matlab R2013a on a computer with Intel Core i7 CPU 1.99 GHz, 8 GB of RAM.

4.1. QR key tests

After features extraction form QR code. The generated key is tested by NIST tests, and the results of key tests are illustrated in Table 4.

4.2. Histogram analysis

Histogram analysis is used to explain the diffusion and confusion characteristic of the encryption algorithm. Table 5 shown the difference in distributed of image among plain iris image, its permutation and its encryption.

4.3. Correlation analysis

The correlation between two adjacent pixels in the ordinary image is permanently strong, and the values of correlation are so close to 1. For this reason, the correlation must be reduce significantly in an efficient encryption algorithm and the value so close to 0 [19, 20]. We can compute the correlation coefficients for three directions horizontal, vertical, and diagonal, according to the following equations:

$$\mathrm{cov}(x, y)=E\{(x - E(x))(y-E(y))\} \tag{7}$$

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{8}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{9}$$

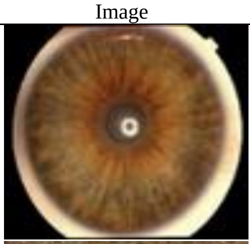
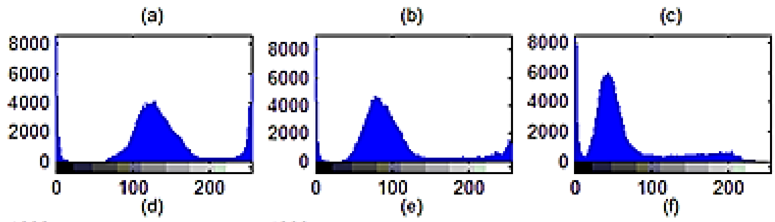
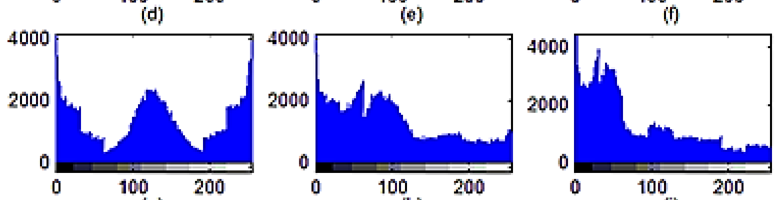
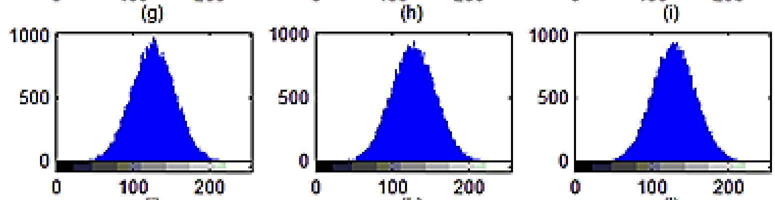
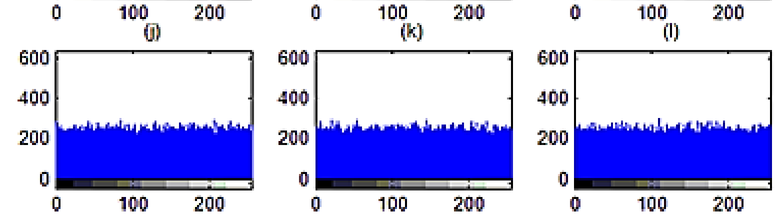
$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{10}$$

in (3), x and y are the values of two neighboring pixels in the image, D(x) and E(x) are the variance and the expectation of x. N in (9) and (10) is the number of pixels in image. Figure 5 shown the horizontal, vertical and diagonal correlation coefficient in plain and encrypted iris image. Table 6 shown the results of correlation for sample of plain iris images and encrypted images and compared it with [8].

Table 4. Test key results

No.	Test Type	Parameterize test	No. Test	Success	Failure	%
1	G using SHA-1	Approximate Entropy TEST	255	255	0	100%
		BLOCK FREQUENCY TEST	255	255	0	100%
		CUMULATIVE SUMS TEST	510	503	7	98.6%
		Discrete FFT TEST	255	255	0	100%
		Frequency TEST	255	253	2	99.2%
		LEMPEL-ZIV COMPRESSION TEST	255	253	2	99.2%
		linear-complexity	255	255	0	100%
		Non periodic-templates	255	255	0	100%
		overlapping-templates	37740	35855	1885	95%
		random-excursions	255	255	0	100%
		runs	255	255	0	100%
		Serial	255	252	3	98.8%
2	Linear Cingruential	Approximate Entropy TEST	128	128	0	100%
		BLOCK FREQUENCY TEST	128	123	5	96%
		CUMULATIVE SUMS TEST	256	248	8	96.8%
		Discrete FFT TEST	128	128	0	100%
		FREQUENCY TEST	128	123	5	96%
		LEMPEL-ZIV COMPRESSION TEST	128	0	128	0%
		linear-complexity	128	128	0	100%
		Non periodic-templates	18944	16675	2269	88%
		overlapping-templates	128	128	0	100%
		RANK TEST	128	128	0	100%
		RUNS TEST	128	126	2	98.4%
		SERIAL TEST	256	250	6	97.6%
3	Blum-Blum-Shub	Approximate Entropy	128	128	0	100%
		BLOCK FREQUENCY TEST	128	125	3	97.6%
		CUMULATIVE SUMS	256	253	3	98.8%
		Discrete FFT	128	128	0	100%
		FREQUENCY TEST	128	125	3	97.6%
		LEMPEL-ZIV COMPRESSION TEST	128	128	0	100%
		linear-complexity	128	128	0	100%
		Non periodic-templates	18944	16705	2239	88%
		overlapping-templates	128	128	0	100%
		RANK TEST	128	128	0	100%
		RUNS TEST	128	128	0	100%
		SERIAL TEST	256	255	1	99.6%
4	XOR	Approximate Entropy	180	180	0	100%
		BLOCK FREQUENCY TEST	180	180	0	100%
		Discrete FFT	180	180	0	100%
		CUMULATIVE SUMS	362	362	0	100%
		FREQUENCY TEST	180	179	1	99.4%
		LONGEST RUNS OF ONES TEST	180	180	0	100%
		LEMPEL-ZIV COMPRESSION TEST	180	180	0	100%
		RANK TEST	180	180	0	100%
		NONPERIODIC TEMPLATES TEST	26788	21429	5359	79.9%
		RUNS TEST	180	177	3	98.3%
		SERIAL TEST	362	357	5	98.6%

Table 5. Histogram analysis of original, permuted and encrypted RGB iris image

Description	Image	R, G and B bands Histogram
Original iris image		
Permuted image		
After add QR key		
After add Logistic key		

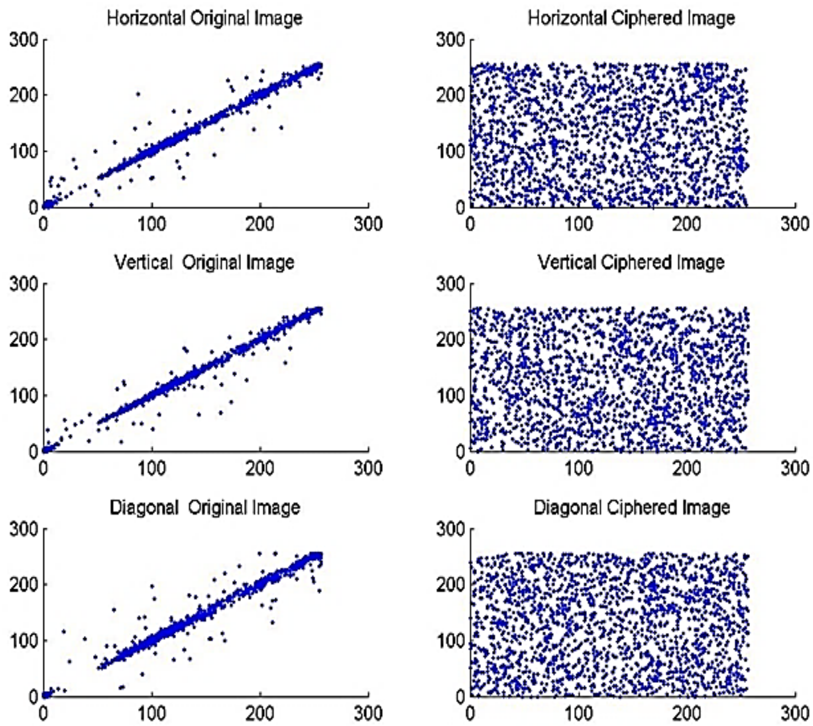
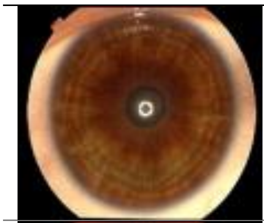
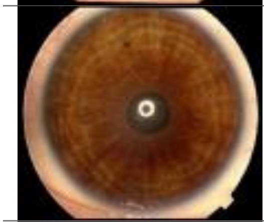


Figure 5. Correlation of two neighboring pixels in plain and encrypted iris image

Table 6. Comparing correlation coefficients of two neighboring pixels in the plain and encrypted images between proposed system and [8]

Images	Correlation of proposed system			Correlation of A. Husain [8]		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
	0.0738	0.0836	0.0743	0.0138	-6.6318e-04	0.01
	-0.0026	-0.0015	0.0043	0.0743	0.0654	-0.0529
	0.0040	-3.1145e-04	0.0027	-0.0041	0.0280	-0.0143
	3.5373e-04	0.0046	0.0034	-0.0184	0.0544	-0.0165

4.4. Information entropy analysis

One of the very important measure to compute the randomness is information entropy. It can be computed by:

$$H(m)=\sum_{i=0}^{2^n-1} p(m_i)\log_2 \frac{1}{p(m_i)} \quad (11)$$

in (11), m is a sample, n is the number of samples, and p(m) is the probability of symbol m. we can get the ideal value of H(m) according to (11) is 8, this mean that random information in image [21]. The values that we obtained of information entropy are closer to eight, this proof that the proposed scheme has well random. Table 7 illustrate the values of information entropy for the various plain and encrypted iris images and compared it with [8].

4.5. Resisting differential attack analysis

The attackers typically make a small change on the selected plain image and then note the changes in the encrypted image. Thus, they may be able to find a relationship between the plain and encrypted image [22]. In order to know the effect of changing a teeny portion of pixels in the normal image on the encrypted image, in this paper we used the number of pixels change rate (NPCR) and unified averaged changed intensity (UACI). The NPCR indicator can be used to know the number of different pixels that have the same location in the original image and in its encrypted image, and it is defined as follows:

$$NPCR=\frac{\sum_{i,j} D(i,j)}{w \times h} \times 100\% \quad (12)$$

here, w and h are the width and height of the image, C1(i, j) and C2(i, j) are the two encrypted images whose corresponding plain images I1 (i, j) and I2 (i, j) have only one-pixel value difference. D (i, j) = 0, if

C1 (i, j) = C2 (i, j); else D(i, j) = 1. The UACI indicator is used to know the effect on encrypted image if one pixel is changed in plain image, and it is defined as follows:

$$\mathrm{UACI} = \frac{1}{\mathrm{w \times h}}\left(\sum_{\mathrm{i,j}} \frac{|\mathrm{C_1(i,j)} - \mathrm{C_2(i,j)}|}{255}\right) \times 100\% \qquad (13)$$

the ideal value of NPCR and UACI are 99.61 and 33.46 [23, 24]. In this paper we implement NPCR and UACI measures on four color iris images and the results of the two indicators are close to ideal value. Table 8 shown the results of NPCR and UACI in proposed scheme and compare it with [8].

4.6. Peak signal to noise ratio (PSNR)

PSNR (peak signal to noise ratio) are more popular tests for image encryption algorithms; Peak signal-to noise ratio can be utilized to evaluate an enciphering scheme. It is a measurement that points the changes in pixel values between the plain image and the cipher image. The lower value of PSNR represents better enciphering quality. The PSNR formula is expressed in equation bellow:

$$\mathrm{PSNR} = 10 \cdot \log_{10}\left[\frac{\mathrm{M} \times \mathrm{N} \times 255^2}{\sum_{\mathrm{i}=0}^{\mathrm{M}-1}\sum_{\mathrm{j}=0}^{\mathrm{N}-1}(\mathrm{P(i,j)} - \mathrm{C(i,j)})^2}\right] \qquad (14)$$

where M is the width and N is the height of digital image. P(I, j) is pixel value of the plain image and C(I, j) is pixel value of the cipher image [25]. Table 8 shown the results of NPCR and UACI in proposed scheme and compare it with [8].

4.7. Encryption and decryption time analysis

The execution time of image encryption and decryption in proposed system and the comparison with [8] are explains in Table 9.

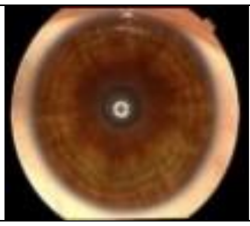
Table 7. Comparing Information Entropy of plain and encrypted iris image between proposed method and [8]

Images	Entropy of plain images	Entropy of proposed system	Entropy of A. Husain [8]
	7.2342	7.9980	7.9974
	7.1288	7.9989	7.9841
	7.3204	7.9990	7.9971
	7.1772	7.9991	7.9974

Table 8. Comparing UACI, NPCR and PSNR indicator of plain and encrypted iris image between proposed scheme and [8]

Images	Proposed system			A. Husain [8]		
	UACI	NPCR	PSNR	UACI	NPCR	PSNR
	33.45	99.62	7.9478	37.71	99.85	6.8802
	34.27	99.62	7.5449	36.13	99.71	7.1288
	35.75	99.60	7.1863	37.52	99.88	6.9512
	34.73	99.56	7.4326	35.42	99.69	7.3138

Table 9. Compering encryption and decryption time in second between proposed system and [8]

Image	Proposed system		A. Husain [8]	
	Enc. time	Dec. time	Enc. time	Dec. time
	2.5	2.5	1.5	1.5

5. CONCLUSION

In this paper, the proposed scheme offers high resistance against differential and statistical attacks. Through the proposal iris image encryption algorithm based on the combination of permutation method, QR code and chaotic system has been introduced to provide high level of security for image encryption. Whereas the random permutation method provide high level of diffusion, and QR key provide high confusion. Also the use of chaotic system offer high randomness, key sensitivity, and confusion. The efficiency of this method has been confirmed through above experiment results. According to these results the proposed scheme offers high resistance against differential and statistical attacks.

ACKNOWLEDGEMENTS

The authors would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad, Iraq for its support in the present work.

REFERENCES

[1] S. H. Moi, N. B. A. Rahim, P. Saad, P. L. Sim, Z. Zakaria and S. Ibrahim, "Iris Biometric Cryptography for Identity Document," *2009 International Conference of Soft Computing and Pattern Recognition*, pp. 736-741, 2009.

[2] T. Mohod, L. Thomas, R. Thorat, Abhinandan Ohara, Manjushri Mahajan, "Security System based on QR Code with Iris Recognition," *National Conference on Advances in Computing, Communication and Networking*, pp. 19-21, 2016.

[3] M. A. Murillo, C. C. Hernández, F. A. Pérez, R.M. López, "A robust embedded biometric authentication system based on fingerprint and chaotic encryption," *Expert Systems with Applications*, vol. 41, no. 21, pp. 8198-8211, November 2015.

[4] M. Soltani, A. K. Bardsiri, "Designing a Novel Hybrid Algorithm for QR-Code Images Encryption & Steganography," *Journal Of Computers*, vol. 13, no. 9, pp. 1075-1088, September 2018.

[5] Sruthi B. Asok1 P. Karthigaikumar, Sandhya R, Naveen Jarold K, Siva Mangai, "Iris Based Cryptography," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, no. 2, pp. 1310-1313, February 2013.

[6] Prasad, Nishi, Vasudharini Moranam Ravi, Lakshmi Chandrasekhar, "Image Encryption with an Encrypted QR, Random Phase Encoding, and Logistic Map," *2008 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1-4, 2018.

[7] M. Mary Shanthi Rani, K. Rosemary Euphrasia, "Data Security Through Qr Code Encryption And Steganography," *Advanced Computing: An International Journal (ACIJ)*, vol. 7 no. 1/2, pp. 1-7, March 2016.

[8] A. Husain, R. Ali, "Finger Print Images Encryption Based on Feature Extraction QR Code," *Conference of College of Education Mustansiriyah University*, pp. 993-1012, 2017.

[9] Abhishek Mehta, "QR Code Recognition from Image," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, no. 12, pp. 781-785, 2015.

[10] Dhwanish Shah, Yash Shah, "QR Code and its Security Issues," *International Journal of Computer Sciences and Engineering*, vol. 2, no. 11, pp. 22-26, 2014.

[11] Anjali Singh and Dr. Parvinder Singh, "A review: QR codes and its image pre-processing method," *International Journal of Science, Engineering and Technology Research (IJSETR)*, vol. 5, no. 6, June 2016.

[12] Masahero hara, "Development and popularaization of QR code", *Synthesiology*, vol. 12, no. 1, pp. 19-27, 2019.

[13] Divya Sharma, "A Review of QR code Structure for Encryption and Decryption Process", *International Journal of Innovative Science and Research Technology*, vol. 2, no. 2, pp. 13-18, February 2017.

[14] Ajay Shanker Mishra, Sachin Kumar Umre, Pavan Kumar Gupta, "QR Code in Library Practice Some Examples", *International Journal of Engineering Sciences & Research Technology*, vol. 6, no. 2, pp. 319-326, 2017.

[15] F. Özkaynak, A. B. Özer, "A method for designing strong S-Boxes based on chaotic Lorenz system," *Physics Letters A*, vol. 374, no. 36, pp. 3733-3738, 2010.

[16] M. S. Khalefa, Z. A. Abduljabar, H. A. Zeki, "Fingerprint Image Enhancement by Develop Mehtre technique," *Advanced Computing: An International Journal*, vol. 6, no. 2, pp. 171-176, November 2011.

[17] D. Heeger, "Signals Linear Systems and Convolution," [Online], Available: https://www.cns.nyu.edu/~david/handouts/convolution.pdf], September 2000

[18] M. Dobeš, J. Martinek, D. Skoupil, Z. Dobešová, J. Pospíšil, "Human eye localization using the modified Hough transform," *Optik-International Journal for Light and Electron Optics*, vol. 117, no. 10, pp. 468-473, Oct. 2006.

[19] A. C. Dăscălescu, R. E. Boriga, "A novel fast chaos-based algorithm for generating random permutations with high shift factor suitable for image scrambling," *Nonlinear Dyn*, vol. 74, No. 1-2, pp. 307-318, October 2013.

[20] W. Zhang, H. Yu, Y. l. Zhao, Z. l. Zhu, "Image encryption based on three-dimensional bit matrix permutation," *Signal Processing*, vol. 118, pp. 36-50, January 2016.

[21] L. Hongjun, W. Xingyuan, "Color image encryption based on one time keys and robust chaotic maps," *Computers & Mathematics with Applications*, vol. 59, no. 10, pp. 3320-3327, May 2010.

[22] Narendra K. Pareek, Vinod Patidar, Krishan K. Sud, "Diffusion-substitution based gray image encryption scheme," *Digital Signal Processing*, vol 23, no. 3, pp. 894-901, May 2013.

[23] L. Liu, S. Miao, "New image encryption algorithm based on logistic chaotic map," *SpringerPlus*, vol. 5, no. 289, pp. 1-12, March 2016.

[24] Amal Abdulbaqi Maryoosh, "A new block cipher algorithm for image encryption based on chaotic system and s-box," *International Journal of Civil Engineering and Technology*, vol. 9, no. 13, pp. 318-327, December 2018.

[25] J. Ahmad, F. Ahmed, "Efficiency Analysis and Security Evaluation of Image Encryption Schemes," *International Journal of Video & Image Processing and Network Security*, vol. 12, no. 4, pp. 18-31, 2012.