Chained QR Keys Generation Based on Chaotic Hybrid Encoding and Fourier Transform Shifting for Image Encryption

Walaa Ali H. Jumiawi [1] , Haider A. Abbas Mohammed [2]

[1] *Department of Mathematics and Computer Science*, Faculty of Science, Beirut Arab University, Lebanon.
[2] *Department of Computer Science*, College of Basic Education, University of Diyala, Iraq.

Email: walaali@hotmail.com; mr_haider81@yahoo.com

***Abstract* - Image encryption has unique characteristics that differs from other data, with pixels representation having undergone many encryption techniques, such as data embedding, AES, chaotic transpositions, DES etc. Some of these techniques are not really practical for the modern security application, although other techniques proposed against reversible attack, by combining both Chaotic Steganography and Cryptography together, in order to increase encryption strength. In this proposal work, we used structural and non-linear technique, using pre-defined encoding system and FFT shifting, to produce QRs keys for both encryption and decryption processes, the initial keys are present, but not dependent as secrets keys, they are encoded dynamically each time, to generate vector of Bar Codes, then reshaped to QR codes thru generation phases. We calculated the information entropy that reached up to 7.995 for the encrypted image, and NPCR is 99.62%, as well as, the average changing intensity UACI up to 33.95% for some results on our samples. These results are compared with some previous methods and it came with good ranking.**

Keywords - Image Encryption, Image Steganography, Quick Response Code, Fourier Transform, Hybrid Keys Generation

I. INTRODUCTION

Throughout the digital history and the wide use of images over internet and isolated communication systems, images encryption used in various applications include fingerprints authentications, biometric signatures, medicals applications, military records, and much more.

The fast deployment of the applications of the communication networks generated sensitive impact on our daily life; many methods proposed to enhance the security of images, some methods used cryptographic techniques by modifying their pixel values or locations [3]. Some new methods used cryptosystem based on binary bit planes extraction and multiple chaotic maps were proposed, which includes two main parts: bit-level permutation and bit-wise XOR diffusion, and some methods used Chaotic systems as a source of randomness [1][4]. Some other algorithms such as DES, AES, 3DES include public data capacity, higher pixel correlation [2]. The initial conditions in these methods can be reduced to weak encryption performance and low resistance against attack, there have been some techniques used for image encryption based on chaotic maps, like the Logistic map and higher dimension functions are proposed and indicated high security from attacks [6][7]. Random chaotic encryptions theory was firstly used by Edward Lorenz 1963 [5]. In the last few years, image encryptions got attention to enhance the techniques of mixing initial conditions and key sensitivity. Information security and many image encryption techniques based on chaotic systems have been proposed based on binary bit plane extraction and pseudo-orbits from 1D chaotic map.

In section II we discussed the approach of Fourier Transform and the phases of key generation to shuffle the intensity levels by specific factor, in order to generate the chaotic map represented by the QR code and equalize its histogram. In section III we have discussed the proposed method and comparing its result with previous work. In section IV we show the methodology of comparison based on the performance measures Number of Changing Pixel Rate NPCR, and higher Unified Averaged Changed Intensity UACI, as well as the information Entropy value. The higher probability value of information entropy functions around the maximum which is 8, considered higher result of security feature against attacks. From the related works, there are two ways of image encryption techniques, the first one was based on permutation in pixels positions without touching pixels values, the second technique was by changing the value of pixels or overall transformation and without changing pixels coordinates. By using XOR operations with the chained key, the linear process act as independent process among multiple variables, thus it generate new pixels values and lead to transformation, in addition to the shuffling of the pixels coordinates, this mix add hardness against anti reverse operation, while XOR is very hard or likely impossible without knowing the mixed and chained keys, we discussed these phases in the our work in section III work.

II. FOURIER TRANSFORM SHIFTING

Frequency domain defined by Fourier transforms which include many applications in image processing. Fourier Transform is an integral transform of one function into another. Jean Baptiste Joseph Fourier (1768-1830), a French mathematician and physicist introduced Fourier transform. The FFT has played an important role in image processing for many years [8] [9] [10] [17]. Let f(x) is a continuous function of a real variable x. The Fourier Transform of f(x), denoted by F (u) is defined as:

$$F(u) = \int \quad f(x)e^{-j2\pi ux}dx \quad Where\ j = \sqrt{-1} \qquad (1)$$

Two dimensional Fourier Transforms in continuous case:

$$F(u,v) = \iint \quad f(x,y)e^{-j2\pi(ux+vy)}dxdy \qquad (2)$$

The Fourier Transform Circular Shifting in (4) is to shift by factor m from the Discrete Fourier Transform represented by (3) , such that if x(n) equal the DFT X(K) then the circular shift will be modified in (4) where the X(n-m) is the circular shift by m factor.

$$x(n) = X(K) = \sum_{n=0}^{N-1} x(n)e^{\left(-\frac{j2\pi}{N}\right)*K*n} \qquad (3)$$

A. Proposed Fourier Transform Aprouch

In the proposed work, we mixed the DFT in spatial domain to be applied on images, represented by the QR matrix, in order to shift the columns and the rows in chaotic pattern, plus the various conditional shifting and pixels value transposition.

The DFT of circular shifting X (n-m) by factor m will be represented in (4) its derivative from (3) , note that the value of n and K are between 0 and N-1, the factor m evaluated to give higher percent of good results every time it change its value, this is because the upcoming formula (4), as well as the phases of key encoding and along with it, plus the chaotic distribution of the generated QR codes that work as chain and each code applied on pixels coordinates shifting and value transposition.

$$x(n-m) = X(K) * \ e^{\left(-\frac{j2\pi}{N}\right)*K*m} \qquad (4)$$

Where 0 ⩽ n ⩽ N-1 and 0 ⩽ K ⩽ N-1, Implementing DFT circular shift in Matlab, without using circshift(Xn,m) function:

```
Xn=input(‘sequence:');
m=input('required shifting:');
N=length(Xn);
Xk=fft(Xn,N);
K=0:N-1;
a=exp(-1i*((2*pi)/N).*K*m);
Xk2=Xk.*a;
Xn2=ifft(Xk2);
```

B. Previous Wrok Aprouch

In the previous hybrid methods, the encryption techniques usually depend logistic maps, 3d chaos generation, confusion and diffusion operations on pixels and keys, some of them have good results and the security considered hard with higher information entropy between 7.975 and 7.99, although they still depend on initial conditions, and the chaotic maps complexity somehow not considered, while the process goes thru conditional values, like alpha, beta and lambda values, to be applied on the hybrid formulas for keys generation and pixels shifting process, for example logistic map formula and Henon, in logistic map: Xk+1= $a * Xk *$ (1- Xk) and Henon map: Xk+1=Yk- 1+ $a * Xk$^2 and Yk+1= $b * Xk$, in case of Henon map to a different point location in space of (Xk,Yk), the value of a and b can exhibits chaotic nature only when the value is 1.4 and 0.3 respectively.

Some techniques proposed with good results based on the initial values [5] [11] [12], note that these values having ranges, the results may be various depending on the range of initial values, may be trial and error of some values can produce high results, thus this will be the starting spark of system vulnerability, while security robustness need more chaotic space and very high attempts of probabilities for more hardness.

III. PROPOSED ENCRYPTION METHOD

The main idea of the proposed method is to mixed hybrid phases of encryption, as shown in Fig.1. This mix going to increase the chaotic space, while each chain iteration works independently from the other chain, thus it the performance increase while estimating probability almost not exist in our case, and brute force attack will suffer.

The first phase, is the key encoding process, which is represented by dynamic dictionary encoding for characters, the encoding consist 16-bit binary represented in chaotic distribution pattern, such that the generation process depend on system inputs on the dictionary rather than using standard and known representation. The second phase is to convert the keys into its equivalents Bar Code vector based on the value 0 and 1.

The next phase is to generate the mask size that produced from reshaping process of the Bar Code in the second phase, for 256*256 image size, the Bar Code of single key will be multiplied by 16 as a vector, then reshaped to N*N matrix. The QR keys generation will be produced by applying (4), in shifting process step, the process perform mixed row, col, and row/col shifting based on the generated QRs.

In the proposed method we have generated three QRs, both pixels shifting and transposition were depending on the total chain sequence as shown in Fig.2 They were chained based on QR and QR+n, where n is the number of QRs, while the first QR already consist very good probability of 0 and 1 that are fair enough for our process, moreover, we applied mean filter (6) thru the chain, to increase the probability of even/odd values, these values used for our conditional pixels shifting and pixels value transposition as it shown in Fig.2. Also the second QR produced based on the results from applying (4) with various factor m on the second QR, and the third as well from the results of the second QR and so on until the last QR.

In addition to the higher probability of pixels distribution, the higher security will highly improved by applying histogram equalization process (10), this is to ensure the equal probability for intensity levels along the keys, while brute forces attack depend on the sequence, this process add very high level of security against this kind of attack, the proposed shown in Fig.2, and the steps will be as following:

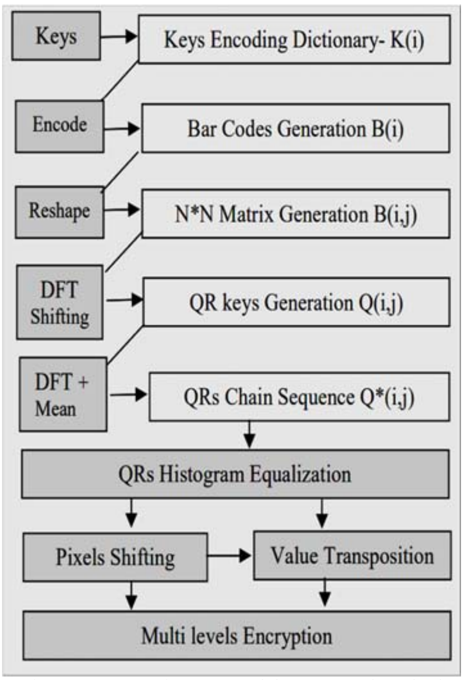

Keys
Keys Encoding Dictionary- K(i)
Encode
Bar Codes Generation B(i)
Reshape
N*N Matrix Generation B(i,j)
DFT Shifting
QR keys Generation Q(i,j)
DFT + Mean
QRs Chain Sequence Q*(i,j)
QRs Histogram Equalization
Pixels Shifting
Value Transposition
Multi levels Encryption

Figure 1. Processing Steps of the proposed method

A. Key Encoding

Encoding each character in the keys with dynamic 16 bit, the dictionary will include the chaotic encoding bits for every character in the key, including alphabet letters and symbols; the order does matter for probability of key sensitivity in this phase, such that, the binomial coefficient (5), for both keys generation and keys encoding generation are accumulative, because it represent the selection from 16 char and encoding 16 bit for each character, for example if n is the total letters and symbols are 44, then (5) represent the number of ways k can be selected from the number of total characters n.

$$P(n,k)=(n¦k)= n!/((n-k)!) \qquad (5)$$

B. Bar Code Generation and Reshaping

Bar Code generation produced from multiplying the numbers of bit, i.e. 16*16 = 256, to produce the initial chaotic vector, and reshaping the barcodes to square Images i.e. 256*256 = 65536 , the total length. For each color the probability will be from 0 to 255 after applying histogram equalization, Eq(10), the frequency will be (0,255).

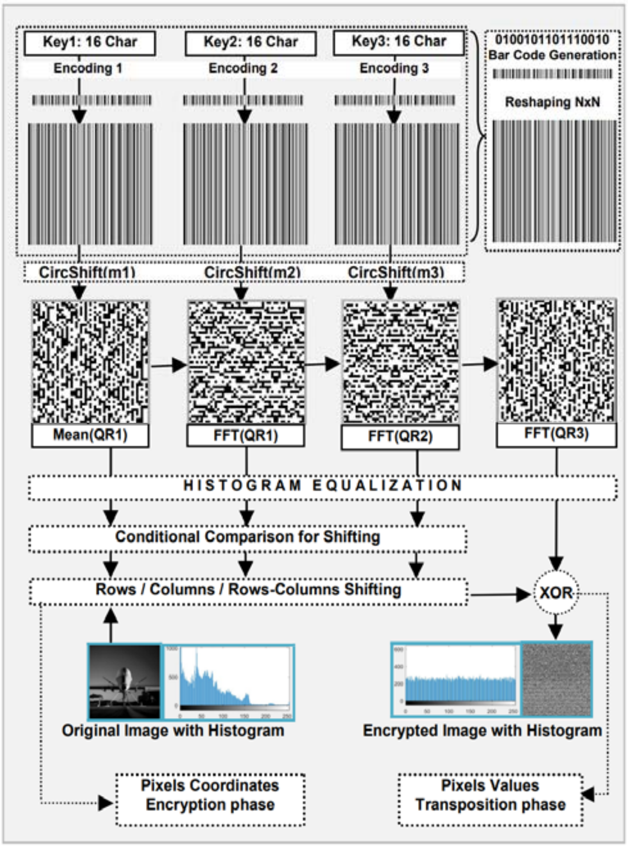


Figure 2. Simulation Steps of the proposed method.

C. Mean Filter and Fourier Transform Shifting

We have discussed in section II the modification of (3) to (4), such that the shifting occur with factor m, in order to produce the chaos odd/even pixels value for the QR matrix, as a result from the previous step, also by applying Mean filter (6), on the result, we obtained very high percent of odd/even distribution that considered good in our conditional encryption steps.

$$f(x,y) = \frac{1}{mn} \sum_{(s,t)\in Sxy} g(s,t) \qquad (6)$$

D. QRs Histogarm Equalization

Histogram equalization is a process for adjusting image intensities to enhance contrast, Let p indicate the normalized histogram of f with for each probability of intensity, thus P in (7), is the normalized histogram:

$$\mathrm{Pn} = \frac{number\ of\ bixels\ of\ level\ n}{total\ number\ of\ pixels} \tag{7}$$

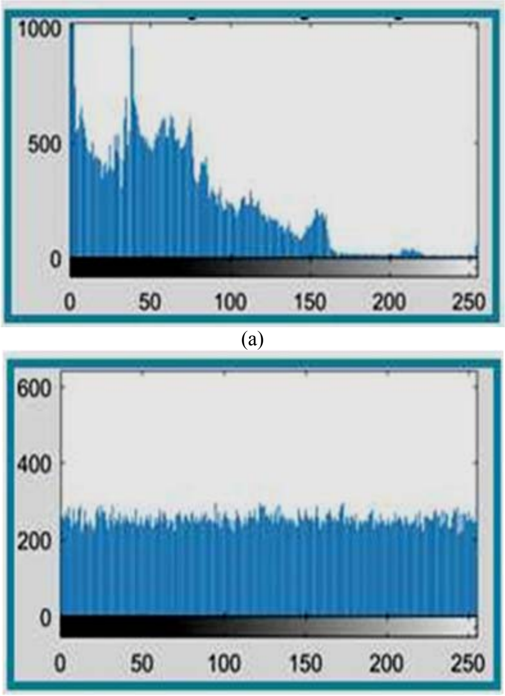
Where n between 0 and L-1, the histogram equalization of image g will be represented in (8), where the floor round down to the closest integer, thus the process is to transform the intensity levels k of image f in (9).

$$\mathrm{g(i, j)} = \mathrm{floor}((\mathrm{L}-1)\ \textstyle\sum_{n=0}^{f(i,j)} \mathrm{Pn}) \tag{8}$$

$$\mathrm{HE(k)} = \mathrm{floor}((\mathrm{L}-1)\ \textstyle\sum_{n=0}^{k} \mathrm{Pn}) \tag{9}$$

In Fig.3 (a) show that the histogram distribution is in non-uniform mode, thus for higher security we need to equalize that histogram to produce uniform intensity level as it shown in Fig.3 (b). For example if image size M*N the histogram equalization will be represented in (10), where B is the large integer number for equalization quality, we selected various values for each QR in the chain sequence.

$$\mathrm{HE(k)} = \big(\mathrm{int}(\mathrm{k} * \mathrm{B})\big)\mathrm{mod}(\mathrm{QR\ hight}) \tag{10}$$



(a)

(b)

Figure 3. Histogram equalization of QR intensity level.

E. Encryption using Pixels Coordinates Shifting

The conditional shifting based on the QRs sequence can be achieved from checking the values from the equalized QRs keys i.e. even, odd, or even adjacent to right odd, odd adjacent to right even, and so on, by performing mixed shifting i.e. columns, rows, and columns and rows together, this process depend on the whole sequence of the chain, as it shown in Fig.2, thus the probability from the binomial coefficient (5) duplicated accumulatively in each iteration across encryption process.

F. Encryption "Pixels Value Transpostion"

In this step we will produce a non-reversible values of original pixels after shifting, the real values changed in every iteration, this transposition occur by performing XOR operation across the chain sequence, between the last shifting process and the last QR key in the chain, this key is the final step along the sequence after step (E) when it becomes completed, thus, at this step the encrypted image become ready.

IV. ENCRYPTION PERFORMANCE MEASURE

In Fig.4 we can see the result and how the diffusion of the encrypted image appear with its histogram equalization, although this doesn't mean we got the required Unless there are analytical approach, the statistical analysis in this work represented by calculating information entropy to ensure the uniformity of pixels distribution, as well as, NPCR to calculate the percentage of different number of pixels, also we have calculated the UACI for average difference of intensity level [16], finally we have analyzed Correlation Coefficient, this is to measure the quality of pixels pair relocation.

A. Information Entropy

In (11) the information entropy calculated, this is to check the maximum value of P(S). Where P' (Si) is the probability of item Si, entropy can be represented by bits. If S is 2^8 char with similar probability, i.e. Si = s1 to s256, then entropy P(S) = 8, which is the highest random representation of encryption, and it mean there is uniform pixels distribution.

$$P(S) = -\textstyle\sum_{0=1}^{N-1} \mathrm{P'(Si)}Log_2\mathrm{P'(Si)} \tag{11}$$

B. NPCR, Number of Pixel Change Rate

The percentage of different number of pixels in encrypted images, or the pixels change rate, it represented by NPCR calculation in (12). Where V(i,j) is the difference between two pixels in encrypted images from different keys i.e. and its value between 1 and 0, if toward 1, means that the pixels are not equal, and if toward 0, the pixels are equal in encrypted image.

$$NPCR = \frac{\sum_{i,j}\ \ \mathrm{V}(i,j)}{N*N} * 100\% \tag{12}$$

C. UACI, Unified Average Changing Intensity

An average difference of intensity levels in encrypted image can be calculated in (13).

$$UACI = \frac{1}{N*N}\sum_{i,j} \frac{|I1(i,j)-I2(i,j)|}{Frequency} * 100\% \quad 100\% \qquad (13)$$

Where I1 (i,j) and I2 (i,j) are pixels from two images and Frequency=255, as they are equalized along histogram of grayscale image.

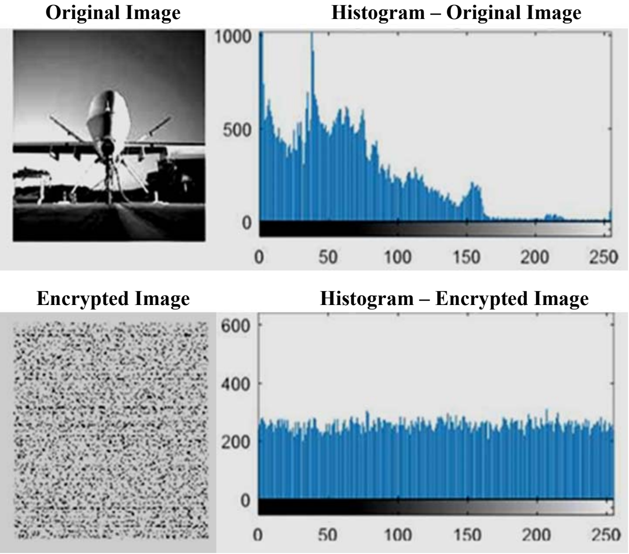


Figure 4. Encryption and Histogram Equalization.

D. Correlation Coefficient Analysis

The measurement of the quality of pixels pair relocation in (14), represents the encryption quality; the correlation coefficients will check the rows, columns and rows-columns pixels adjacent in the final result as it shown in Fig.5.

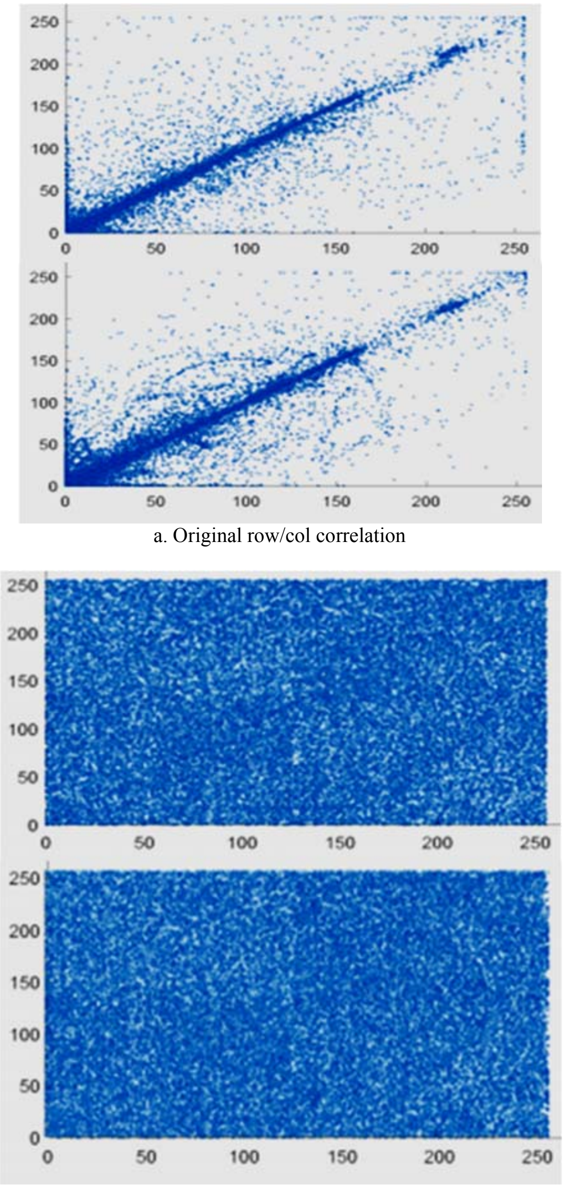
$$CV(x,y) = \frac{1}{P}\sum_{i=1}^{\mathrm{P}}(\mathrm{x}-\mathrm{x}')(\mathrm{y}-\mathrm{y}') \qquad (14)$$

Where P is the number of chaotic pair and the values of x and y, are in shifted and encrypted image.

V. STATISTICAL ANALYSIS

In order to analyze the information from the encrypted image, to evaluate the sensitivity against attacks, we have tested 3 types of images and got interesting values from the performance measurement methods in section IV, in Fig.5 the rows and columns correlation shown, they represent the distribution of pixels pair relocation, also the in Fig.6, pixels confusion of the 3 images appears clearly, one of the images that used in the previous work was Lena image, we used it in our proposed work for comparison purposes.

The comparison of performance measure are listed in table (1), it represent the statistical analysis and the sensitivity results, including the values of information entropy, NPCR, UACI, and correlation coefficient analysis of 3 images, we have selected various images according to its pixels distribution and intensity levels range, we used Lena image among these 3 images in order to compare the measurement between our proposed method and the previous work, while It was used in some previous research [5],[13], and [14], also we used the performance measures that considered better for comparison in the stated researches.



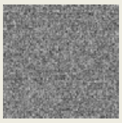
a. Original row/col correlation

b. Encrypted row/col correlation

Figure 5. Correlations of original (a) and encrypted image (b).

According to the results from table (1), it appear that the entropy from the finger print image look interesting while its original entropy was with very low 3.53197, and the encrypted images got 7.95100, that show high comparison about its original entropy value, as well as, the drone values. Regarding the results from Lena image, we have compared our results with some previous techniques and we got good ranking about the performance measure that used on the same image "Lena" as it shown in table (2). Regarding the values of the information entropy, NPCR, UACI, and correlation coefficient, it show the sensitivity against attack in encryption domain, the performance measures used tell whether the techniques add more robustness, they represent the enhancement field in term of higher sensitivity .

TABLE I. STATISTICAL ANALYSIS OF INFORMATION ENTROPY, NPCR, UACI, AND CORRELATION COEFFICIENT

Original Images		 Drone	 Lena	 Fingerprint
Information Entropy		7.12886	7. 56344	3.53197
Correlation Coefficient	Row	0.94494	0.96925	0.62021
	Col	0.93446	0.94157	0.72666
Encrypted Images		Drone 	Lena 	Fingerprint
Information Entropy		7.98932	**7.99522**	7.95100
Correlation Coefficient	Row	- 0.00456	- 0.00442	- 0.00751
	Col	- 0.00597	0.00135	- 0.00315
NPCR		99.59106	99.62310	99.64141
UACI		33.88725	33.95970	32.31850

The higher value of information entropy i.e. close to 8 means that the encrypted image has higher security against attack, in addition to the values from NPCR, while the higher percent indicate higher security according to the different of pixels, and regarding the UACI, the values usually considered weak if it's close to 0, meaning that there average difference look equal.

TABLE II. COMPARISON USING LENA IMAGE BETWEEN PREVIOUS WORK AND OUR PROPOSED METHOD.

Methods	**NPCR**	**UACI**	**Entropy**	**Correlation Coefficient**	
				Columns	**Rows**
MMC [14]	**99.5100**	**33.4500**	**7.9997**	**0.0030**	**0.0047**
CCML [13]	**25.0000**	**19.0000**	**Not used**	**0.0014**	**0.0036**
NPWLCM [23]	**99.6292**	**28.5050**	**7.9975**	**-0.0195**	**-0.0195**
3DCM [5]	**99.6048**	**33.5044**	**7.9890**	**0.0014**	**-0.0043**
Proposed Method	**99.62310**	**33.95970**	**7.99522**	**0.00135**	**- 0.00422**

VI. CONCLUSIONS AND FUTURE WORK

In this paper, images encryption techniques implemented using Matlab platform, which considered better platform for images and signal processing applications including Steganography, we have clarified the phases and the techniques that has been used in this method, we have showed the QRs keys generation phases during chaining steps in figures, and how it produce high security along encryption phases, also we showed that Fourier transform can be used for circular shifting and has been applied in every QR generation step, as well we as, the dynamic encoding using encoding dictionary. In our results we have explained the performance measure in various algorithms, we have evaluated our work by, information entropy, NPCR, UACI, and correlation coefficient values, these measurements are highly used in this field of work, we have compared our work with some previous works, also we explained the slight change in the results, and we clarified that these results are very good factors for higher security for the final encryption, and they are considered in case of any kind attack and reversible methods like brute force or even cryptosystems machine learning.

In future work, this method can be enhanced by producing QRs chain based on other chaos techniques by using Fourier transform too, i.e. using longer encoding vectors, while in our case each character encoded by 16-bit, this value can be increased, but we have to consider the chaotic complexity and randomness, also this work can be developed by extending the chain sequence and looping it in circular sequence, starting from the reshaped bar code vector until the last QR key.

In future work also, it will be very practical to perform cryptosystem machine learning but in term of finding the nearest pattern to the generated QRs key, this can be achieved by collecting huge number of images as a data set, as we explained in our work that the probability considered very high, one may decide to collect all probabilities to generate this data set, there is only one problem in this try, which is the shifting factor across the chained keys, so by giving try to test attacking this method we have to ignore shifting phase from the QRs generation phase in order to separate testing phases.

REFERENCES

[1] G Wen, H. & Yu, S. Eur. Phys. J. Plus (2019) "Cryptanalysis of an image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps" Springer Berlin Heidelberg.

[2] S. Lian., "A Block Cipher Based on Chaotic Neural Networks". Elsevier, Neurocomputing, vol. 72, pp. 1296-1301, 2009.

[3] Z. Hua, Y. Zhou, C.-M. Pun, and C. P. Chen, "2D Sine Logistic modulation map for image encryption," Information Sciences, vol. 297, pp. 80-94, 2015.

[4] Nepomuceno, Erivelton & Arias García, Janier & G, Nardo & Butusov, Denis & Tutueva, Aleksandra. (2019). Image encryption based on the pseudo-orbits from 1D chaotic map. Chaos. 29. 61101. 10.1063/1.5099261.

[5] Hossain, Md. Billal & Rahman, Md.Toufikur & Rahman, A & Islam, Sayeed. (2014). A new approach of image encryption using 3D chaotic map to enhance security of multimedia component. 2014 International Conference on Informatics, Electronics and Vision, ICIEV 2014. 1-6. 10.1109/ICIEV.2014.6850856.

[6] Pawan N. Khade and Prof. Manish Narnaware, “3D Chaotic Functions for Image Encryption", International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, PP 323-328, May 2012.

[7] Zhou Zhe, Yang Haibing, Zhu Yu, Pan Wenjie, Zhang Yunpeng, “A Block Encryption Scheme Based on 3D Chaotic Arnold Maps”, International Asia Symposium on Intelligent Interaction and Affective Computing, 2009.

[8] R.Gonzalez & R.Wood, “Digital Image Processing,” 3rd ed, Englewood Cliffs, NJ: Prentice Hall, 2007.

[9] W. A. H. Jumiawi and A. El-Zaart, "Image Spectrum Segmentation for Lowpass and Highpass Filters," 2018 4th International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Mangalore, India, 2018, pp. 327-332. doi: 10.1109/iCATccT44854.2018.9001919

[10] Roopashree.S, Sachin Saini, Rohan Ranjan Singh, “Enhancement and Pre-Processing of Images Using Filtering” International Journal of Engineering and Advanced Technology (IJEAT), Volume-1, Issue-5, June 2012.

[11] Revanna C R, Dr. C Keshavamurthy “A Secure Document Image Encryption Using mixed Chaotic System” International Journal of Computer Science and Information Security (IJCSIS), Vol. 15, No. 3, March 2017.

[12] Abdullah, Hikmat & Abdulkareem, Hamsa. (2017). Image encryption using hybrid chaotic map. 121-125. 10.1109/CRCSIT.2017.7965545.

[13] Sodeif Ahadpour, Yaser Sadra, “A Chaos-based Image Encryption Scheme using Chaotic Coupled Map Lattices”. International Journal of Computer Applications,Vol. (49), Number-2,2012,ISBN 973-93-8086931-6.

[14] Kamel Faraoun, “Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption”. The International Arab Journal of Information Technology, Vol. 7, No. 3,pp231-240, July 2011.

[15] Hadi H Abdulredha, Qassim Nasir, “Low Complexity High Security Image Encryption Based on Nested PWLCM Chaotic Map”. IEEE Internatonal conference for Internet Technology and Secure Transactions, ISBN 978-1-4577-0884-8, pp 220-225, Dec 2011.

[16] Som, Sukalyan & Kotal, Atanu & Mitra, A. & Palit, Sarbani & Chaudhuri, Bidyut. (2014). A chaos based partial image encryption scheme. 2014 2nd International Conference on Business and Information Management, ICBIM 2014. 58-63. 10.1109/ICBIM.2014.697093.

[17] Hennelly, Bryan & Sheridan, John. (2003). Optical image encryption by random shifting in fractional Fourier domains. Optics letters. 28. 269-71. 10.1364/OL.28.000269.

.