

A Novel Image Encryption Scheme Based on Different Block Sizes for Grayscale and Color Images

Omar Reyad
Sohag University, Egypt
Emails: ormak4@yahoo.com

M. A. Mofaddel
Sohag University, Egypt
mmofaddel@hotmail.com

W. M. Abd-Elhafiez
Sohag University, Egypt
w_a_led@yahoo.com

Mohamed Fathy
Sohag University, Egypt
mohamed_fathy@yahoo.com

Abstract—In this paper, two image encryption schemes are proposed for grayscale and color images. The two encryption schemes are based on dividing each image into blocks of different sizes. In the first scheme, the two dimension (2D) input image is divided into various blocks of size $N \times N$. Each block is transformed into a one dimensional (1D) array by using the Zigzag pattern. Then, the exclusive or (XOR) logical operation is used to encrypt each block with the analogous secret key. In the second scheme, after the transformation process, the first block of each image is encrypted by the corresponding secret key. Then, before the next block is encrypted, it is XORed with the first encrypted block to become the next input to the encrypting routine and so on. This feedback mechanism depends on the cipher block chaining (CBC) mode of operation which considers the heart of some ciphers because it is highly nonlinear. In the case of color images, the color component is separated into blocks with the same size and different secret keys. The used secret key sequences are generated from elliptic curves (EC) over a binary finite field \mathbb{F}_{2^m} . Finally, the experimental results are carried out and security analysis of the ciphered images are demonstrated that the two proposed schemes had a better performance in terms of security, sensitivity and robustness.

I. INTRODUCTION

With the great progress in Internet technology and the maturation of digital image processing techniques, various applications of digital images are commonly widespread and are still continuously and rapidly increasing in the future. Although, a potential information security risk is still and always exist during the transmission operation of digital images over an opened (unsecured) networks. Naturally, the security of multimedia content such as plainimages attracts more and more attention from cryptographers points of view and leads to the importance of image encryption technology in many applications.

Image encryption principles is different from that of text due to some intrinsic features of images such as bulk data capacity, high redundancy, strong correlation among adjacent pixels, and so forth. The traditional of various encryption algorithms that is based on number theory such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) and the RSA cryptosystem, are found to have the weakness of low-level efficiency when the image is becoming bulky and large [1], [2]. Consequently, these algorithms are not fully suitable for

the encryption of such kind of large sized data, especially for a real-time communication scenarios.

In many situations, the color images are commonly used and frequently transmitted over the Internet and through wireless communication networks, because, they contain more abundant information than the grayscale images. Though some encryption algorithms for grayscale images can be easily extended and modulated to handle color images, it consumes more running time due to additional information required to represent the Red, Green and Blue (RGB) color image components. So, the need to develop a secure encryption algorithm for color images has attracted growing attentions in recent years [3], [4].

In this paper, we proposed a new encryption scheme based on segment the image into blocks of size $N \times N$, in order to increase the security level of the cipherimages and the resistance against known-plaintext and chosen-plaintext attacks.

The paper is organized as follows. In Section II, the preliminaries of EC and CBC mode are discussed. In Section III, given a background about the current image encryption schemes. In Section IV, the description of the proposed schemes are presented. In Section V, presented the experimental results and discussion while conclusions are given in Section VI.

II. PRELIMINARIES

A. Elliptic Curve over a Binary Finite Field

The field \mathbb{F}_{2^m} is called a binary finite field and it can be viewed as a vector space of dimension m over the field \mathbb{F}_2 which consists of two binary elements $\{0, 1\}$. A non-supersingular elliptic curve E over a binary field \mathbb{F}_{2^m} is defined by an equation taking the form

$$y^2 + xy = x^3 + ax^2 + b \quad (1)$$

where the parameters $a, b \in \mathbb{F}_{2^m}$ with $b \neq 0$. The set $E(\mathbb{F}_{2^m})$ consists of all the points $(x, y), x \in \mathbb{F}_{2^m}, y \in \mathbb{F}_{2^m}$, which satisfy the defining equation given in (1), together with a special point O called the point at infinity. These set of points form an abelian group with respect to the arithmetic of elliptic curve addition rules over this abelian group [5].

B. The Chaos-Driven ECPRNG

The Chaos-Driven Elliptic Curve Pseudo-random Number Generator (C-D ECPRNG) is considered to be the EC-Linear Congruential Generator [6] driven by a chaotic map and is presented in [7] for the prime finite field \mathbb{F}_p . Such specific modification improves randomness of the sequence generated and increases its periodicity. The C-D ECPRNG for a given seed point $G(x, y) \in E(\mathbb{F}_{2^m})$ as the secret key, is defined as the following sequences of points generated by EC-points addition operation:

$$U_i = [i(1 + b_i)]G \oplus U_0 \\ = \begin{cases} [i]G \oplus U_0 & \text{if } b_i = 0 \\ [2i]G \oplus U_0 & \text{if } b_i = 1 \end{cases}, i = 1, 2, \dots \quad (2)$$

where $U_0(x, y) \in E(\mathbb{F}_{2^m})$ is the "initial value" and b_i is the random bits generated by a chaotic map Φ

$$b_i = \begin{cases} 0 & \text{if } \Phi^i(s) \in S_0 \\ 1 & \text{if } \Phi^i(s) \in S_1 \end{cases}, i = 1, 2, \dots \quad (3)$$

where the state space $S = [0, 1]$ is the interval and $S_0 = [0, 0.5]$, $S_1 = (0.5, 1]$ are two subsets of the interval equal to 0.5 [8].

C. The CBC Mode of Operation

In cipher block chaining (CBC) mode, the encryption of a block not only depends on the key but also on the previous blocks [9]. The encryption process is context-dependent operation. This means that the same size blocks in different contexts are encrypted differently. The receiver can confirm that the cipher block has been changed because the decryption process of a manipulated cipher block does not work.

The CBC mode uses a fixed initialization vector (IV) which can be made public. Then, the plainimage is decomposed into blocks of length n . If Alice encrypts the sequence b_1, \dots, b_n , of plainimage blocks of length n using the key k , then she sets

$$C_0 = IV, \quad C_j = E_k(C_{j-1} \oplus B_j), \quad 1 \leq j \leq n \quad (4)$$

She obtains the cipher block

$$C = C_1 \dots C_n \quad (5)$$

In general, the CBC mode of operation encrypts the same plainimage differently with different initialization vectors. Moreover, the encryption of a plainimage block depends on the preceding plainimage blocks. Therefore, if the order of the cipherimage blocks is changed or if the cipherimage blocks are replaced, then the decryption process becomes very hard or even impossible.

III. LITERATURE REVIEW

Pareek et al. [3] proposed a new approach for color image encryption based on chaotic logistic maps. An external secret key of 80-bit length and two chaotic logistic maps are employed. Eight different operation-types are used to encrypt the image pixels. In [10], Huang and Nien proposed a color image cryptosystem using multi-chaotic systems, which is composed of two shuffling stages parameterized by chaotically generated sequences. But, it is found that this method cannot resist known-plaintext attack and chosen-plaintext attack [11]. Liu and Wang [12] designed a stream-cipher algorithm based on one-time keys and robust piecewise linear chaotic maps in order to get high security and improve the dynamical degradation. The initial conditions were generated by the Message Digest hash function (MD5) of the mouse positions. In [13], Patidar et al. have designed a fast loss-less symmetric color image cipher based on the widely used substitution-diffusion principle which utilized chaotic logistic maps. In [14] Rhouma et al. have proposed an approach for color image encryption based on one-way coupled-map lattices (OCML). An external secret key of 192-bit length was used to generate the initial conditions and parameters of the OCML by making algebraic transformations to the secret key. Liu and Wang [15] applied a bit-level permutation and high-dimension piecewise linear chaotic map to encrypt color image. The chaotic Chen system was employed to confuse and diffuse the red, green and blue components simultaneously. In [16], Ye has proposed an efficient image encryption scheme based on generalized Arnold map and generalized Bernoulli shift map. The proposed scheme can shuffle the plainimage efficiently in the permutation process. In [17], a new color image encryption algorithm was presented based on Logistic map, which is used to encrypt the red, green and blue components of color image at the same time and make the three components affect each other.

It is found that most of the chaos-based cryptosystems for color images usually employ the low dimensional and single chaotic system which leads to some fundamental drawbacks such as insufficient key space and weak security function. Moreover, the red, green and blue components are unchanged when only pixel shuffle is used.

Algorithm 1 First Encryption Scheme

- 1) Read gray/color image.
 - 2) Divide image into blocks with size $N \times N$.
 - 3) Convert 2D image block to 1D block array by using Zigzag pattern.
 - 4) Encrypt each 1D block array with its analogue secret key using XOR operation.
 - 5) Repeat step 3 and 4 for each block and for each color component (R, G and B).
-

IV. THE PROPOSED IMAGE ENCRYPTION SCHEMES

In this section, two encryption schemes for grayscale and color images are proposed. The first scheme is described in

algorithm 1 (Scheme 1) and it starts with reading the grayscale or color image, then, divide it into blocks of size $N \times N$. Here, we divide the image into blocks of sizes 8×8 , 16×16 and 32×32 . Then, we convert each 2D plain block to 1D block array by using Zigzag pattern. The resulted block arrays are encrypted with its analogue secret key using the XOR operation. We repeat the encryption operation until the end of the plainimage blocks.

The second scheme starting the same way, but, the plainimage block is XORed with the previous encrypted image block before it is in turn encrypted according to the CBC mode given in Section II-C. In the second scheme which described in algorithm 2 (Scheme2), the encryption of each image block depends on all the previous blocks. In other words, each image block is used to modify the encryption of the next block. So, each cipherimage block is dependent not just on the plainimage block that generated it, but, on all the previous plainimage blocks.

Algorithm 2 Second Encryption Scheme

- 1) Read gray/color image.
- 2) Divide the image into blocks with size $N \times N$.
- 3) Convert 2D image block to 1D block array by using Zigzag pattern.
- 4) Encrypt the first 1D block array with its analogue secret key using XOR operation.
- 5) The resulting encrypted block from previous step is again XORed with the next plain block.
- 6) Repeat step 5 for each next block and for each component.

TABLE I
CORRELATION COEFFICIENT FOR GRAYSCALE IMAGES.

	Block Size	Gray Image	Horizontal	Vertical	Diagonal
Scheme1	8×8	Lena1	-0.110731	0.019723	0.064634
		Brain1	-0.078563	0.027462	0.068747
		Brain2	-0.080802	0.020420	0.059806
	16×16	Lena1	-0.003129	0.030368	0.054511
		Brain1	0.001796	0.019956	0.047490
		Brain2	-0.001519	0.019827	0.044745
	32×32	Lena1	0.015067	-0.013705	-0.008321
		Brain1	0.006978	-0.006833	-0.013169
		Brain2	0.009111	-0.007917	-0.005091
Scheme2	8×8	Lena1	-0.007554	-0.002917	-0.002976
		Brain1	-0.008014	0.004825	-0.001519
		Brain2	0.015339	0.010465	-0.006979
	16×16	Lena1	0.001588	0.010809	-0.004753
		Brain1	0.002683	0.004188	0.000231
		Brain2	-0.001019	0.040991	-0.009674
	32×32	Lena1	0.008448	0.005313	-0.002331
		Brain1	-0.000296	0.002431	-0.002793
		Brain2	0.002351	-0.011532	-0.001332

V. EXPERIMENTAL RESULTS

In this section, the performance of the two proposed schemes is analyzed by using different security test measures. These measures are taken as follows: key space analysis,

TABLE II
CORRELATION COEFFICIENT FOR COLOR IMAGES.

	Block Size	Color Image	Horizontal	Vertical	Diagonal
Scheme1	8×8	Lena2	-0.082513	0.037293	0.068243
		Lena	-0.078532	0.036584	0.063751
		Peppers	-0.049236	0.037812	0.031654
	16×16	Lena2	0.010421	-0.000204	0.045462
		Lena	0.012032	-0.000660	0.042805
		Peppers	0.011683	-0.002831	0.031449
	32×32	Lena2	0.019763	-0.009177	-0.012030
		Lena	0.018391	-0.011639	-0.012637
		Peppers	0.011303	-0.011811	-0.004381
Scheme2	8×8	Lena2	-0.005078	0.009510	0.000686
		Lena	-0.011888	-0.002805	0.005339
		Peppers	0.007140	-0.000409	0.005576
	16×16	Lena2	-0.004184	-0.002763	0.007892
		Lena	-0.003383	0.005404	0.007359
		Peppers	0.002886	0.001597	0.001081
	32×32	Lena2	0.004221	-0.004797	0.001803
		Lena	0.005993	-0.003371	-0.005426
		Peppers	0.003712	-0.010077	-0.004915

statistical analysis including histogram analysis and computing the correlation coefficients of adjacent pixels, information entropy analysis, test security against differential attack including calculating the number of pixel change rate (NPCR) and unified average changing intensity (UACI). The used grayscale images are (brain1 and brain2) with size 256×256 and (lena1) with size 512×512 . Also, the color images (lena and peppers) with size 256×256 and (lena2) with size 512×512 are used and the security analysis of the cipherimages is carried out.

A. Histogram Analysis

To prevent the leakage of information, it is important to ensure that cipherimage does not have any statistical resemblance with its original plainimage. A robust encryption scheme should always generate a cipherimage of uniform histogram for any plainimage. In this work, the histograms are plotted for grayscale/color plain and ciphered images. Figs. 1(a – c) and Figs. 2(a – c) display the histogram of the grayscale and color images (Fig. 1(a) and Fig. 2(a) and the corresponding cipherimages (Fig. 1(b, c) and Fig. 2(b, c)), respectively. From these figures, one can clearly notice that the histograms of the ciphered image are fairly uniform and significantly different about those of the original image. The statistical feature of the original images is enhanced in such a manner that the cipherimages had a uniform level distribution and good balance property.

B. Correlation Analysis

It is known that two adjacent pixels in every plainimage are highly correlated vertically, horizontally and diagonally. This could be the property of any ordinary image. The maximum value of correlation coefficient test is 1 and the minimum value is 0. A robust image encryption scheme versus statistical attack should have a correlation coefficient value of 0. Results of horizontal, vertical and diagonal directions are obtained as shown in Table I for different grayscale images and Table

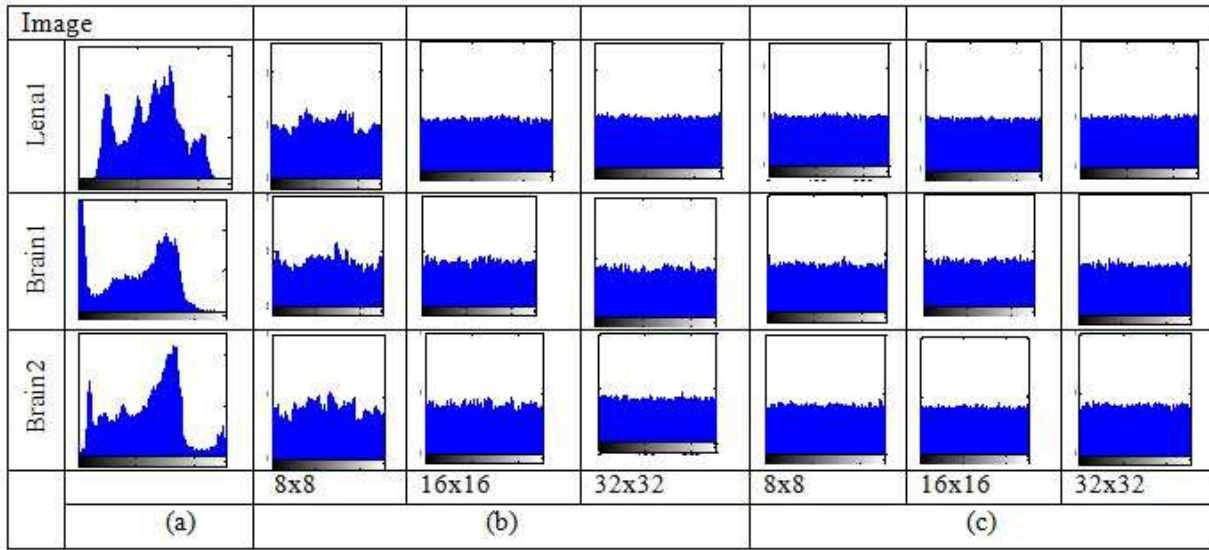


Fig. 1. Histogram of a) Original image, b) Scheme1 encrypted image, c) Scheme2 encrypted image, for different grayscale images.

II for different color images. These results demonstrate that there is negligible correlation between the two adjacent pixels in the cipherimages, even when these two adjacent pixels in the plainimage are highly correlated. Also, it is comparable to the correlation coefficient values presented by references [10], [14], [18], [19], [20] and [21] as shown in Table III.

C. Entropy Analysis

Entropy is defined to show the degree of uncertainties in the system. It is well known that the entropy $H(m)$ of a message source m can be calculated as:

$$H(m) = - \sum_{i=0}^{255} P(m_i) \log_2 P(m_i) \quad (6)$$

where $P(m_i)$ represents the probability of symbol m_i . For all the considered cipherimages shown in Fig. 3(b, c) and Fig. 4(b, c), the number of occurrence of each grayscale and color images is recorded and the probability of occurrence is computed for grayscale images and color images with different block sizes, respectively. Table IV and V indicates the various values of the entropies for the encrypted images by the presented schemes. It can be noted that the entropy of the cipherimages are very near to the theoretical value of 8 indicating that all the pixels in the encrypted images occur with almost equal probability. Therefore, the information leakage in the proposed encryption schemes is negligible, and it is secure against the entropy-based attack. Also it is comparable to the entropy values presented by references [12], [14], [18] and [22] as shown in Table VI.

D. Sensitivity Analysis

In order to avoid the known-plaintext attack, the changes in the cipherimage should be significant even with a minor

TABLE III
COMPARISON OF CORRELATION COEFFICIENT FOR LENA COLOR IMAGE

Scheme	Horizontal	Vertical	Diagonal
Original Lena image	0.958853	0.980061	0.943422
The proposed scheme1	0.017363	-0.011263	-0.012563
The proposed scheme2	-0.011888	-0.002805	0.005331
Ref. [10]	0.1257	0.0581	0.0504
Ref. [14]	0.0681	0.0845	0.0046
Ref. [18]	-0.00124	0.00176	0.00193
Ref. [19]	-0.00368	0.00014	-0.02298
Ref. [20]	0.0042	0.0033	0.0024
Ref. [21]	-0.0018	0.00033	0.00427

change in the plainimage. If one small change in the plainimage can cause a significant change in the cipherimage, with respect to diffusion and confusion properties, then the differential attack actually loses its efficiency and becomes practically useless. To quantify this requirement, two common measures are used here: number of pixels change rate (NPCR) and unified average changing intensity (UACI) [23]. We have tested the NPCR and UACI with the proposed encryption schemes to assess the influence of changing a single pixel in the plainimages on the cipherimages. From the obtained results, we have found that the average values of the percentage of pixels changed in cipherimages is greater than 99.65% for NPCR and 33.46% for UACI for the two proposed encryption schemes. This implies that the proposed schemes is very sensitive with respect to minor changes in the plainimage as shown in Table VII and Table VIII.

E. Key Space Analysis

The key space that is being used for encryption must be large enough to make the brute-force attack infeasible [24]. The key sequences generated using the elliptic curve generator over the field \mathbb{F}_2 had high periodicity so that the

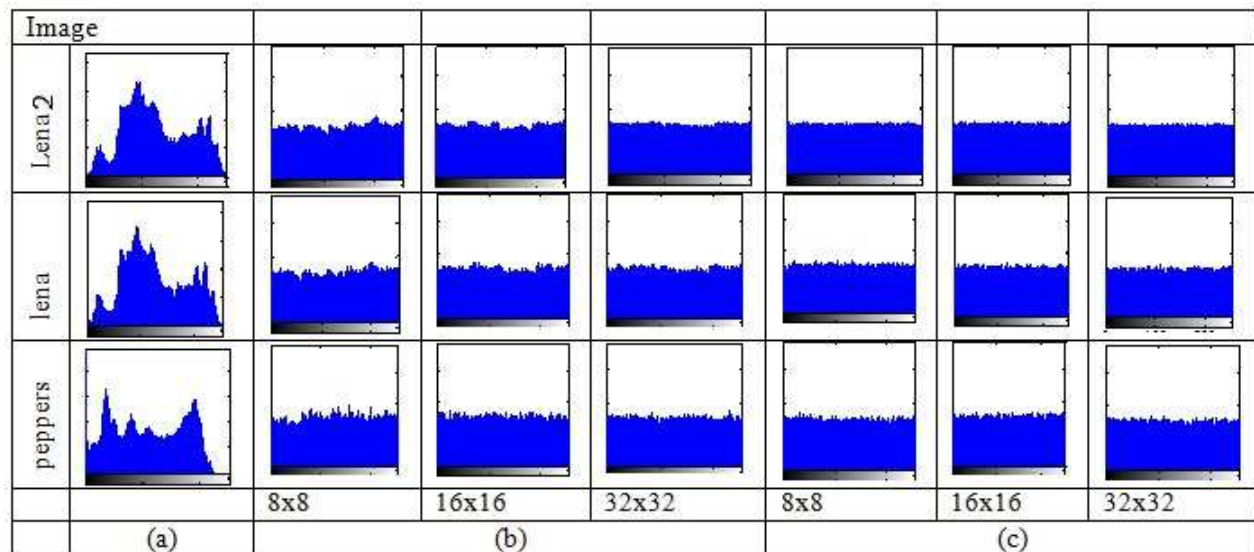


Fig. 2. Histogram of a) Original image, b) Scheme1 encrypted image, c) Scheme2 encrypted image, for different color images.

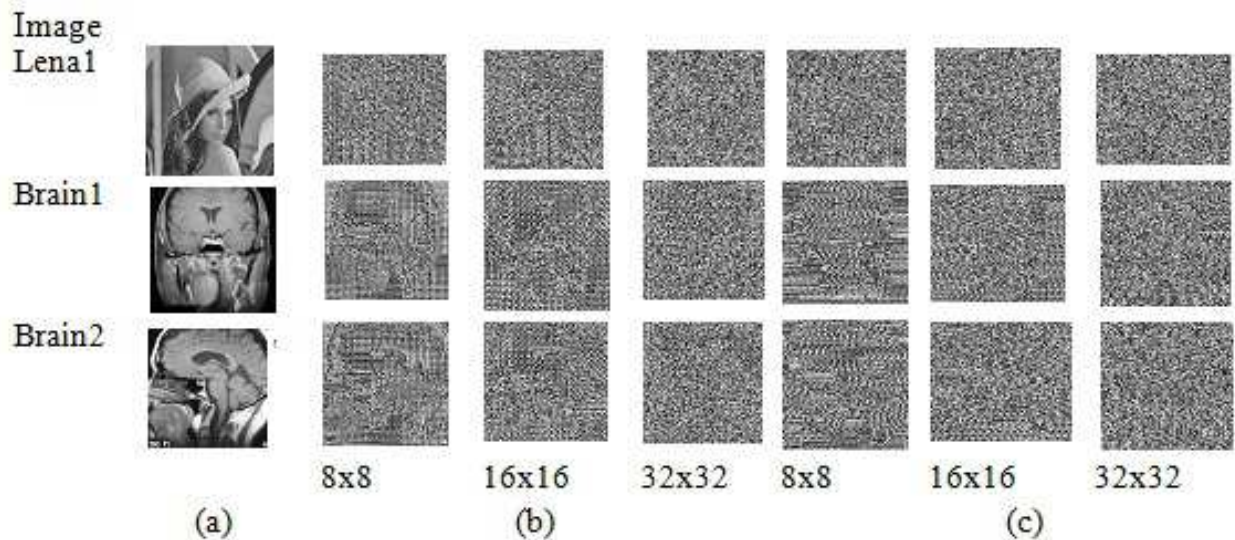


Fig. 3. Show the a) Original image, b) Scheme1 encryption image, c) Scheme2 encryption image, for different grayscale images.

cipherimages are secure. In addition, the used chaos-driven elliptic curve pseudo-random key sequence generator has a flexible, moderately large key space, which comprises of the following parameters:

- 1: The secret key of the chaotic generator (if the precision is 10^{-14} , then, the size of the key space for initial condition and control parameter is 2^{93}),
- 2: Possible elliptic curves and the base point,
- 3: The external secret user's key of CBC mode.

Then, the total number of possible keys is the size of the key space and is equal to the product of the above parameters. It is to be noted that unless all the above elements of the key space are known to the attacker, decryption using brute force attack is difficult. Even if the proposed schemes are hacked,

after number of iterations and using different keys, the attacker is able to view only one single part/block of the image.

VI. CONCLUSION

Image encryption algorithms play a vital role in the security of digital images and is considered one common method to protect the image information. In this paper, we presented two encryption schemes for grayscale/color images based on split the image into sub-blocks of different sizes $N \times N$ to increase the image security. Each block is transformed into a one dimensional (1D) array by using the Zigzag pattern. Then, the XOR logical operation is used to encrypt each block with the analogous secret key. In the second scheme, after the transformation process and before the next block

is encrypted, it is XORed with the first encrypted block to become the next input to the encrypting routine and so on. This feedback mechanism depends on CBC mode of operation which considers highly nonlinear.

The results show that lower correlation and higher entropy resulted by using smaller block sizes. Also, the results showed that the correlation between image elements was significantly decreased by using the second proposed scheme (Scheme2) with block size 16×16 and 32×32 .

TABLE IV
ENTROPY VALUES FOR GRAYSCALE IMAGES.

	Block Size	Gray Image	Entropy
Scheme1	8×8	Lena1	7.987895
		Brain1	7.986050
		Brain2	7.983381
	16×16	Lena1	7.99897
		Brain1	7.99643
		Brain2	7.996091
32×32	Lena1	7.999046	
	Brain1	7.99747	
	Brain2	7.998037	
Scheme2	8×8	Lena1	7.99914
		Brain1	7.99747
		Brain2	7.99782
	16×16	Lena1	7.999268
		Brain1	7.99768
		Brain2	7.99842
	32×32	Lena1	7.999294
		Brain1	7.998186
		Brain2	7.998090

TABLE V
ENTROPY VALUES FOR COLOR IMAGES.

	Block Size	Color Image	Entropy
Scheme1	8×8	Lena2	7.9974
		Lena	7.99653
		Peppers	7.994405
	16×16	Lena2	7.99854
		Lena	7.99764
		Peppers	7.99764
	32×32	Lena2	7.99942
		Lena	7.99869
		Peppers	7.99871
Scheme2	8×8	Lena2	7.99973
		Lena	7.99903
		Peppers	7.99873
	16×16	Lena2	7.99978
		Lena	7.99902
		Peppers	7.99890
	32×32	Lena2	7.99976
		Lena	7.99897
		Peppers	7.99876

REFERENCES

- [1] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcat. Chaos*, vol. 8, 1998, pp. 1259–1284.
- [2] L. Zhang, X. Liao and X. Wang, "An image encryption approach based on chaotic maps," *Chaos Solitons Fract.*, vol. 24, 2005, pp. 759–765, doi:10.1016/j.chaos.2004.09.035.
- [3] N. K. Pareek, V. Patidar and K. K. Sud, "Image encryption using chaotic logistic map," *Image Vision Comput.*, vol. 24, 2006, pp. 926–934, doi:10.1016/j.imavis.2006.02.021.

TABLE VI
COMPARISON OF ENTROPY VALUE FOR LENA COLOR IMAGE.

Scheme	Entropy
The proposed scheme1	7.998137
The proposed scheme2	7.999034
Ref. [12]	7.985467
Ref. [14]	7.975033
Ref. [18]	7.989633
Ref. [22]	7.9870

TABLE VII
NPCR AND UACI OF GRAYSCALE IMAGES

	Block Size	Gray Image	NPCR (%)	UACI (%)
Scheme1	8×8	Lena1	99.5712	27.3573
		Brain1	99.5947	30.4378
		Brain2	99.6005	28.8077
	16×16	Lena1	99.6784	28.9233
		Brain1	99.6503	32.1215
		Brain2	99.6708	30.3371
	32×32	Lena1	99.6093	33.4635
		Brain1	99.5966	32.2349
		Brain2	99.6113	30.6637
Scheme2	8×8	Lena1	99.5853	28.6517
		Brain1	99.6259	31.8237
		Brain2	99.6015	30.2017
	16×16	Lena1	99.6105	28.5656
		Brain1	99.6230	31.9521
		Brain2	99.5761	30.3085
	32×32	Lena1	99.6124	28.6939
		Brain1	99.6337	31.8058
		Brain2	99.6425	30.2723

TABLE VIII
NPCR AND UACI OF COLOR IMAGES

	Block Size	Color Image	NPCR (%)	UACI (%)
Scheme1	8×8	Lena2	99.6093	33.4635
		Lena	99.7339	31.2896
		Peppers	99.7014	33.3449
	16×16	Lena2	99.6093	33.4635
		Lena	99.6515	31.0247
		Peppers	99.6383	32.2480
	32×32	Lena2	99.6093	33.4635
		Lena	99.6358	30.4976
		Peppers	99.5854	32.2896
Scheme2	8×8	Lena2	99.6093	33.4635
		Lena	99.6114	30.3397
		Peppers	99.6164	32.1348
	16×16	Lena2	99.6093	33.4635
		Lena	99.5885	30.4506
		Peppers	99.6276	32.3855
	32×32	Lena2	99.6093	33.4635
		Lena	99.6007	30.4142
		Peppers	99.5905	32.0023

- [4] O. Reyad and Z. Kotulski, "Pseudo-Random Sequence Generation from Elliptic Curves over a Finite Field of Characteristic 2," In: *Federated Conference on Computer Science and Information Systems, FedCSIS, ACSIS*, vol. 8, pp.991–998, IEEE, 2016.
- [5] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York 2009.
- [6] O. Reyad and Z. Kotulski, "On Pseudo-random Number Generators Using Elliptic Curves and Chaotic Systems," *J. Appl. Math. Inf. Sci.*, vol. 9, 2015, pp. 31-38.
- [7] O. Reyad and Z. Kotulski, "Statistical Analysis of the Chaos-Driven

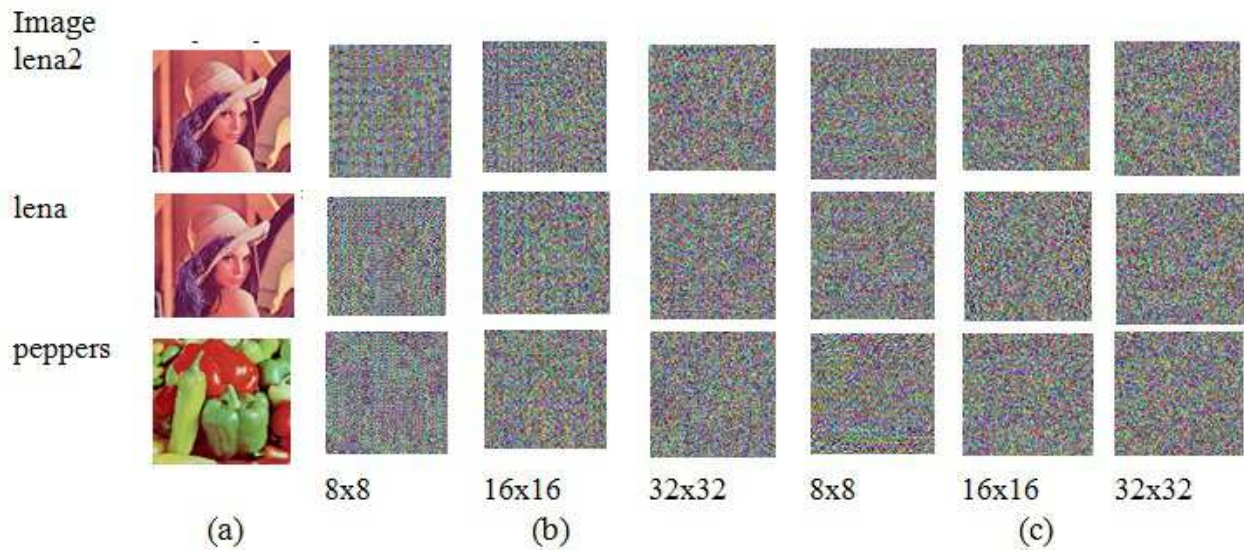


Fig. 4. Show the a) Original image, b) Scheme1 encryption image, c) Scheme2 encryption image, for different color images.

TABLE IX
COMPARISON OF NPCR AND UACI FOR LENA COLOR IMAGE.

Scheme	NPCR (%)	UACI (%)
The proposed scheme1	99.6023	30.339
The proposed scheme2	99.6514	33.463
Ref. [10]	99.52	26.7933
Ref. [14]	99.5843	33.3755
Ref. [17]	99.6358	33.4428
Ref. [18]	42.7519	13.2874
Ref. [19]	99.7915	49.2191
Ref. [20]	99.2173	33.4055
Ref. [21]	99.9654	33.5720
Ref. [25]	99.6062	33.8981

Elliptic Curve Pseudo-random Number Generators," *In: Z. Kotulski, et al. (eds.) CSS 2014. CCIS*, vol. 448, Springer, Heidelberg, 2014, pp. 38–48.

[8] J. Szczipanski, Z. Kotulski, "Pseudorandom number generators based on chaotic dynamical systems," *Open Systems & Information Dynamics*, vol. 8, 2001, pp. 137–146.

[9] B. Schneier, *Applied cryptography (2nd ed.): protocols, algorithms, and source code in C*, John Wiley & Sons, Inc. New York, NY, USA 1995.

[10] C. K. Huang and H. H. Nien, "Multi chaotic systems based pixel shuffle for image encryption," *Opt. Commun.*, vol. 282, 2009, pp. 2123–2127.

[11] E. Solak, R. Rhouma and S. Belghith, "Cryptanalysis of a multi-chaotic systems based image cryptosystem," *Opt. Commun.*, vol. 283, 2010, pp. 232–236.

[12] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. Appl.*, vol. 59, 2010, pp.3320–3327.

[13] V. Patidar, N. K. Pareek and K. K. Sud, "A new substitution diffusion based image cipher using chaotic standard and logistic maps," *Commun Nonlinear Sci Numer Simulat*, vol. 14, 2009, pp. 3056–3075.

[14] R. Rhouma, S. Meherzi and S. Belghith, "OCML-based colour image encryption," *Chaos Soliton Fract.*, vol. 40, 2009, pp. 309–318.

[15] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, 2011, pp. 3895–3903.

[16] R. Ye, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism," *Opt. Commun.*, vol. 284, 2011, pp. 5290–5298.

[17] X. Wang, L. Teng and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process*, vol. 92, 2012, pp. 1101–1108.

[18] W. Xiangjun, B. Chenxi and K. Haibin, "A new color image cryptosystem via hyperchaos synchronization," *Commun Nonlinear Sci Numer Simulat*, vol. 19, 2014, pp. 1884–1897.

[19] W. Xiangjun, L. Yang and K. Jrgen, "A New Color Image Encryption Scheme Using CML and a Fractional-Order Chaotic System," *PLOS ONE*, vol. 10, 2015, doi:org/10.1371/journal.pone.0119660.

[20] X. Wei, L. Guo, Q. Zhang, J. Zhang and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyperchaotic system," *J. Syst. Software*, vol. 85, 2012, pp. 290–299.

[21] H. Liu, A. Kadir and Y. Niu, "Chaos-based color image block encryption scheme using S-box," *Int. J. Electron. Commun.*, vol. 68, 2014, pp. 676–686.

[22] S. Liu, J. Sun and Z. Xu, "An improved image encryption algorithm based on chaotic system," *J. Comput.*, vol. 4, 2009, pp. 1091–1100.

[23] Y. Wu, J. P. Noonan and S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption," *IEEE Transl. J. of Selected Areas in Telecommunications (JSAT)*, pp. 31–38, April 2011.

[24] T. Gao and Z. Chen, "Image encryption based on a new total shuffling algorithm," *J. Chaos, Solit. and Fract.*, vol. 38, 2008, pp.213–220.

[25] A. Kadir, A. Hamdulla and WO. Guo, "Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN," *Optik*, vol. 125, 2014, pp. 1671–1675.