SECURE STRATEGY FOR OPTICAL IMAGE ENCRYPTION SYSTEM BASED ON AMPLITUDE MODULATION, PHASE MODULATION AND MODIFIED LOGISTIC MAP

Ahmed M. Elshamy[1], Aziza I. Hussein[2,3], Hesham F. A. Hamed[4], M. A. Abdelghany[4], and Hamdy M. Kelash[5]

[1]Department of Network and Security, College of Information Technology,
Fujairah University, Fujairah, UAE
[2]Department of Computer & Systems Engineering, Faculty of Engineering,
Minia University, Minia, Egypt
[3]Electrical & Computer Engineering Department,
Effat University, Jeddah, KSA
[4]Department of Communication & Electronics, Faculty of Engineering,
Minia University, Minia, Egypt
[5]Department of Computer Science and Engineering,
Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt

ABSTRACT

This paper presents an optical image encryption system based completely on amplitude modulation, phase modulation in the discrete Fourier transform and modified chaotic logistic map. Amplitude modulation and phase modulation are accomplished by the use of spatial light modulator (SLM). SLMs are normally used to control incident light in amplitude-best, phase-best or the mixture (amplitude-phase). The random amplitude modulation based on a chaotic Baker map is carried out in time domain, while the random phase modulation is accomplished in the frequency domain. In this paper, we proposed a technique to regulate and enhance protection in a chaotic logistic map method leading to increased variety of key space of the logistic map. This causes our encryption system to become exceptionally sturdy against brute pressure. An exhaustive analysis of the proposed encryption system is undergone and shows positive results in encryption metrics when compared to several different photo encryption techniques. The analysis demonstrates the highly valued security and immunity to noise of the photograph encryption. The proposed modified logistic map with amplitude and phase modulation is suitable for real-time application.

KEYWORDS

Image Encryption, Fourier Transform, Security, Chaotic Logistic Map, Chaotic Baker Map

1. INTRODUCTION

Technological advances in internet connectivity have led to a massive increase in transmitted data over the internet, including media sharing, photos, videos and social networking. Therefore, it has emerged as a major concern to maintain the security of this data. The prime method of ensuring

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 101–116, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81808

the safety of this data is through the process of encryption. There are many encryption methods, but websites, as well as their users, will always prefer the most efficient encryption systems that still protect them against unauthorized hackers. Thus it is essential to understand and improve upon the most recent proposed techniques in order to guarantee the safety of different types of data, including the most important, such as private conversations and official records.

There are a few chaos strategies in picture encryption and phase modulation encryption techniques in the optics field proposed by researchers. Picture encryption strategies have been a particular focus to fulfill the demand of photoprotection in digital and electric conversation systems. Chaos encryption techniques are essential for increasing verbal exchange protection. Unauthorized hackers attempt to intercept the original data in the course of the transmission from the sender to the receiver via wired or wireless media. Chaotic systems are high in randomness and sensitivity of the initial conditions of the transmission. These properties make chaotic systems ideal for implementation of a cipher, which is needed for encryption and decryption in the encryption technique. Despite encryption systems being well built and implemented, there remains the possibility of hacking of any system. The goal is to minimize this opportunity, and in an effort to do so, unique chaotic logistic map techniques were proposed.

In reference [1], the Logistic chart is implemented aimed at the chaotic mapping, for optical orthogonal occurrence department multiplexing system (OFDM) in the time and frequency domains in a fast Fourier remodel. In [2-4], authors proposed cozy orthogonal frequency-department-multiplexing passive optical community (OFDM-PON) primarily based on the chaos scrambling in the OFDM frequency domain. Amongst them, chaotic Logistic maps based totally on pseudorandom quantity generator PRNGs were proposed [5-6]. In [7], authors proposed a picture encryption gadget primarily based on the changed logistic map, compressive ghost imaging and coordinate sampling. The cipher text may be received by discrete cosine remodel (DCT). Multichannel random discrete fractional Fourier remodel with arbitrary increment coefficients and fractional remodel kernel features has been proposed with the aid of Kang [8]. In [9], the novel model offered by implementing the chaotic Logistic map in embedded structures using the synchronization phenomenon of discrete fractional logistic maps have been proposed. A logistic chaotic map and a multichannel arbitrary unconnected fractional Fourier convert was proposed [10]. In [11], presented a photograph encryption system founded on the unconnected manifold parameter and coupled Logistic maps. A new data encryption approach based on the location substitution, shuffling and a selection manner is proposed [12]. A unique shade photo encryption set of rules based totally on the Logistic map and double random section encoding by rapid Fourier transform has been offered through the way of Huang [13].

In [14], they proposed optical chaos based totally on confusion (Arnold cat map) and diffusion (logistic map) encryption algorithms, which confuse the connection among the authentic photograph and encrypted image. [15] offered an encryption approach for photo based on chaos blending, which reduces the encryption time manner, in contrast to unique chaotic maps. In [16], a grayscale photograph encryption device based on chaotic Baker map and optical segment modulation in frequency area was offered by means of Discrete Fourier transformation. The authentic image randomized with the aid of chaotic baker map first. After this, it is transformed to optical signs by means of optical emitter, like an optical source, to transform it from electrical sign to optical signal, and encrypt it via phase modulation. This follows two phase modulation, one in time domain and one in Fourier area and finally, transformed by way of CCD virtual digital camera to virtual layout to show it on the laptop.

In [17], a hybrid encryption device based on Arnold cat map and optical phase encryption in frequency area by way of discrete Fourier remodel was presented. The original image is randomized through Arnold cat map first, and then it is transformed to optical signal via an optical emitter inclusive of optical source to convert it from electric signal to optical sign.

However, it encrypts through section modulation with the aid of applying two-phase modulation on it, one in the time domain and one in Fourier area. It detects it by means of CCD virtual camera to transform it to digital format to show it on the computer. Within the decryption technique, it applies the conjugate of two random phase modulation to the optical signal to decrypt the photo, after that it converts the optical signal to electrical sign with the aid of optical detector and randomized with the aid of chaotic Arnold's cat map to get the authentic picture, and then accomplish chaotic Arnold's cat map decryption.

In [18], an encryption method for color photo founded entirely on twofold arbitrary part modulation is described as well as the shade indexed map as the preprocessing cover for altering the color image from three components (RGB) to at least one aspect. [19] presented a video encryption approach primarily based on Henon chaotic map and the optical segment modulation. The Henon chaotic map may be applied digitally, then it demonstrates a second technique optical section modulation optically. The implementation of the proposed method used two classes of video encryption absolutely and permutation encryptions. In [20], there is contrast among numerous encryption technique based on the chaos map and the optical section modulation.

In this paper, the picture is passed through a confusion and diffusion procedure. We compared between special encryption approaches to decide which technique is most appropriate for use in communication network structures for relaxed and efficient transmission. To confirm the validity of the proposed encryption device, numerical Matlab simulation, and cryptanalysis consequences are done.

The structure of the current study is arranged as follows:

Phase II clarifies some preliminary knowledge of several encryption techniques. Phase III gives the proposed encryption techniques. Segment IV presents the high-quality metrics, performance evaluation. In the end, the belief and destiny guidelines are drawn in phase V.

2. Literature Review of Image Encryption Techniques

2.1. Logistic Map

Chaotic maps may be classified into three degrees: 1-D map, 2-D maps, and 3-D [21]. The Logistic map has been considerably utilized for chaotic cryptosystems and released as a paradigm for the dynamics of a population. It includes a maximum of the chaotic traits and an example of a 1D map [22]. This chaotic logistic map is determined by way of refer to (1).

$$Z_m = \beta Z_{m-i}(I - Z_{m-i}) \tag{1}$$

Where (0, 1) and β are bifurcation parameters. When 3.57 ≤ β ≤ 4 the machine is in chaotic conduct. The chart in Fig. 1 demonstrates the bifurcation of Logistic Map as indicated by β. Its value explores and determines the conduct of the chaotic logistic map.

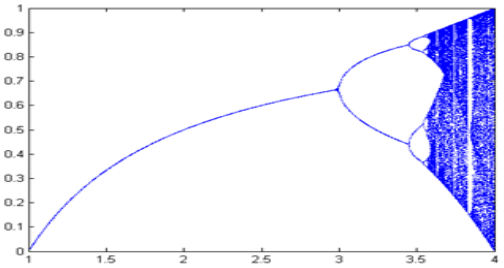


Figure 1. Logistic map chart.

2.2. Baker Map

The chaotic Baker map encryption approach in a photo processing network called a device of encryption. It's a primarily confusion-based device that accomplishes the scrambling of a four-sided matrix photograph M × M dimension by using converting places for pixels founded off a stealthy key.

Baker map of the discretized is represented by $B(v_1,\ldots\ldots,v_k)$, wherever the arrangement of k integers, $v_1,v_2,\ldots\ldots,v_k)$ is selected as where every integer v_i divisions M, and $M_i = v_1 + \ldots\ldots\ldots + v_i$. The pixel at indices (l, s), with $M_i \le l \le M_i + v_i$ and $0 \le s \le M$ is mapped to [23]:

$$B_{(n_1,\ldots\ldots\ldots,n_k)}(l,s) = \left[\frac{M}{v_i}(l - M_i) + s \bmod \frac{M}{v_i}, \frac{v_i}{M}(s - s \bmod \frac{M}{v_i}) + M_i\right] \tag{2}$$

This technique is applied to the subsequent phases:

1. The rectangular matrix M × M is split into ok squares of thickness VI and quantity of factors M.
2. Each factor in the rectangle are rearranged to a row within the permuted rectangle. Rectangles are decided upon from right to left beginning with top rectangles, and then lower ones.
3. The examination starts off read out inside each rectangle, from the lowest left nook in the direction of upper elements.

Fig. 2 suggests an instance for the chaotic Baker map for (M × M) rectangular matrix (M = eight), where the name of the game key S = [2, 4, 2].

2.3. Optical Phase Modulation

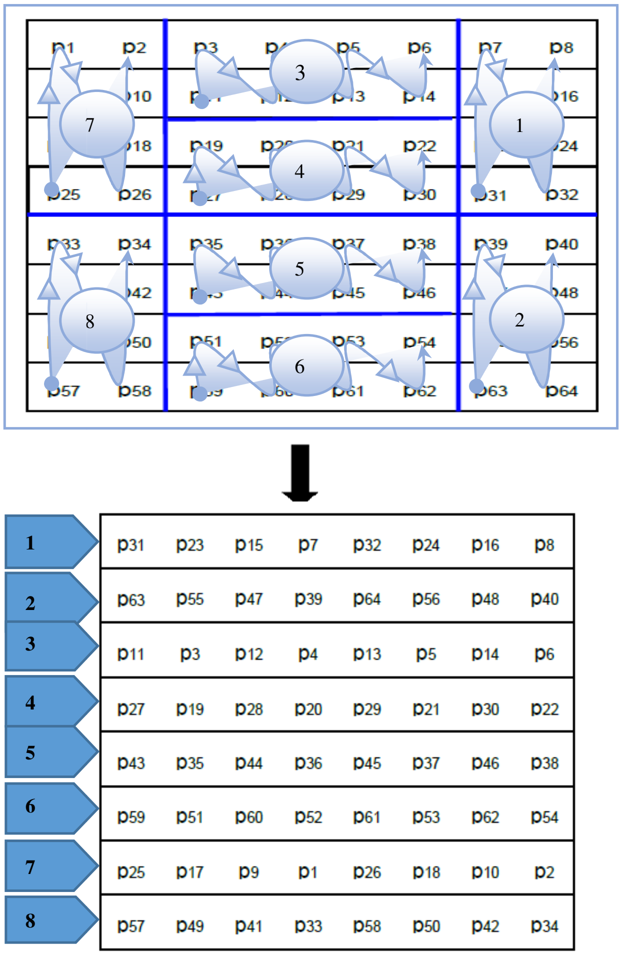
Optical segment modulation was proposed as an optical encryption method in 1997 via Refregier and Javidi known as Double Random phase Encryption (DRPE). DRPE used two random segment mask presented as keys. This encryption approach carried out in pure optical conversation systems, by means of generating optical original signal from laser generator and making use of first phase modulation through Spatial Light Modulator (SLM1) and passing it via first unique lens to convert the signal in frequency domain and observe 2nd phase modulation through SLM2 and bypass it via lens2 to transform lower back signal in time area and retrieve it with the aid of Charge Coupled Device (CCD) as visible in Figure 3.

$\varphi(x,y)$ Coded image, $f(x,y)$ present inventive image, $\delta_n(x,y)$ first amplitude mask in the time domain (first key), $\delta_m(\gamma,\mu)$ and second phase mask in the frequency domain [16].

$$\delta_n(x,y) = \exp[2i\pi n(x,y)] \tag{3}$$

$$\delta_m(x,y) = \exp[2i\pi m(x,y)] \tag{4}$$

$$DFT\,\delta_m(x,y) = \delta_m(\gamma,\mu) = \exp[2i\pi m(\gamma,\mu)] \tag{5}$$



1	p31	p23	p15	p7	p32	p24	p16	p8
2	p63	p55	p47	p39	p64	p56	p48	p40
3	p11	p3	p12	p4	p13	p5	p14	p6
4	p27	p19	p28	p20	p29	p21	p30	p22
5	p43	p35	p44	p36	p45	p37	p46	p38
6	p59	p51	p60	p52	p61	p53	p62	p54
7	p25	p17	p9	p1	p26	p18	p10	p2
8	p57	p49	p41	p33	p58	p50	p42	p34

Figure 2. Chaotic Baker map randomization for 8 × 8 matrices with a secret key S= [2, 4, 2].

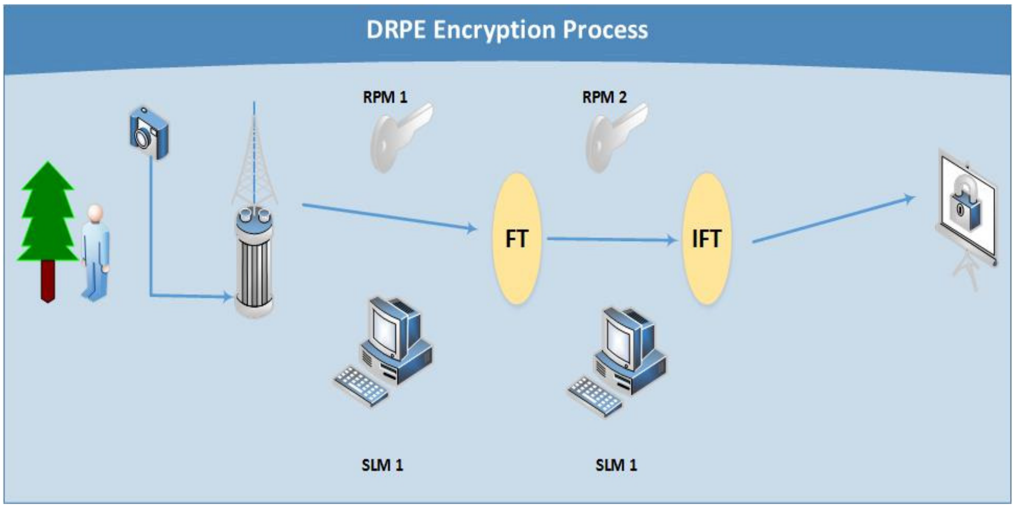


Figure 3. Fully encryption technique with double phase modulation.

Encryption process for the grayscale image in two dimensions is defined as follows:

$$\varphi(x,y) = FT^{-1}\{FT\{f(x,y)\delta_n(x,y)\} * \{\delta_m(\gamma,\mu)\}\} \tag{6}$$

Equation (6) the symbol (*) denotes convolution.

But, in decryption process to do away with first and second segment modulation it has to use conjugate of first and second section mask, as it is applied in the time domain and in the frequency domain. Decryption system algorithm is illustrated as follows:

$$f(x,y) = FT^{-1}\{FT\{f(x,y)\delta^*_n(x,y)\} * \{\delta^*_m(\gamma,\mu)\}\} \tag{7}$$

In first and second phase masks (*) present conjugate of the mask.

$$\delta_n^*(x, y) = \exp\left[-2i\pi n(x, y)\right] \tag{8}$$

$$\delta_m^*(\gamma, \mu) = \exp\left[-2i\pi n(\gamma, \mu)\right] \tag{9}$$

3. THE PROPOSED IMAGE ENCRYPTION TECHNIQUE

The one-dimensional Logistic chaotic encryption set of rules is an easy cipher technique, the modified chaotic equations are carried out to scramble and unscramble pixels sequentially. The proposed encryption method based on random amplitude modulation followed on chaotic Baker rework map (BT) in the time domain by way of first SLM (key 1), random section encryption in frequency area by means of 2nd SLM (key 2) and modified Logistic transformation map (MLT). Changed Logistic map is a development of logistic map where a polynomial time period is $(1-2Z_{m-i})^2$ supplementary. The modified Logistic map equation may be as follows:

$$Z_m = \beta\, Z_{m-i}(I - Z_{m-i})\,(I - 2Z_{m-i})^2 \tag{10}$$

Where $Z_m \in$ (0, 1), $\beta \in$ (0, 16), the initial value Z_0 =0.3.

When $\beta \in$ (0, 4.2), the system seems as episodic behavior.

When $\beta \in$ (4.2, 6.5), the system seems as deprived of chaotic behavior.

When $\beta \in$ (6.5, 16), the system is now chaotic behavior.

The changed Logistic map reveals that it is going to have precise chaos characteristics due to the enhanced extensive variety of β (key space variety) from traditional range (3.57 - four) to (6.5 - 16) as visible in Figure 4, which rise key space and may be beneficial for image cryptosystems.

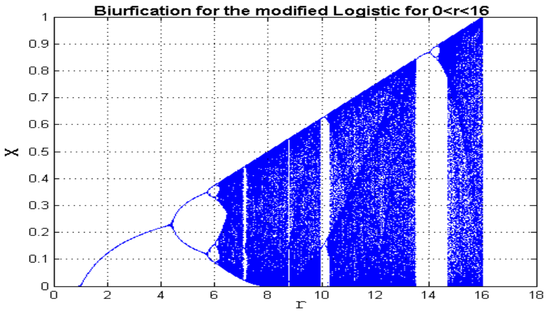


Figure 4. The modified Logistic map.

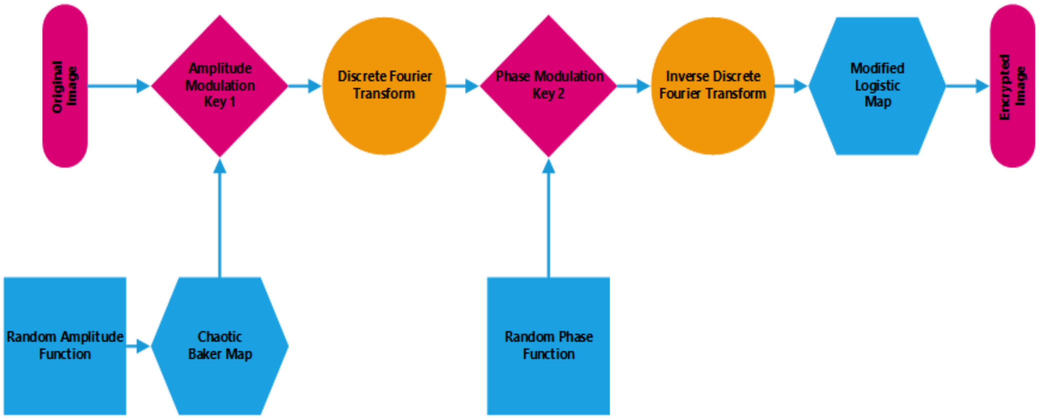

Original Image
Amplitude Modulation Key 1
Discrete Fourier Transform
Phase Modulation Key 2
Inverse Discrete Fourier Transform
Modified Logistic Map
Encrypted Image
Random Amplitude Function
Chaotic Baker Map
Random Phase Function

Figure 5. The proposed encryption technique block diagram.

The series steps for the encryption process are:

1. Randomize the pixels positions of amplitude masks by chaotic Baker map, this step completed digitally.

2. Trade the picture into an optical signal by way of laser beam generator (LED).

3. Follow amplitude modulation by first SLM (key 1) to the optical sign (authentic photograph) in time area using $BT\ \delta_n(x, y)$.

4. Convert it to Fourier domain by the first lens and apply section modulation by using SLM (Key 2).

5. Convert it to time area via the second lens and scramble pixels by using modified Logistic map (key three).

6. Retrieve the encrypted picture through CCD digital camera or convert it to electrical sign by means of detectors and display it on computer.

The encryption procedure is defined mathematically as:

$$\vartheta(x, y) = MLT\ \{FT^{-1}\{FT\{f(x, y)\ (BT\,\delta_n(x, y))\}*\{\delta_m(\gamma, \mu)\}\}\} \quad (11)$$

$\vartheta(x, y)$ Is the proposed encrypted image. MLT is denoted as the modified Logistic transform.

The original image $f(x, y)$ randomized by $BT\ \delta_n(x, y)$ chaotic baker map for amplitude masks. After this, it is transformed to optical sign with the aid of optical emitter, like optical supply, to transform it from electric signal to optical signal and encrypt it with the aid of section mask modulation, the end result scrambled by using changed Logistic map.

The decryption procedure is defined mathematically as

$$f(x,y) = IMLT\{FT^{-1}\{FT\{f(x,y)\ (IBT\delta_n^{*}(x,y))\}*\{\delta_m^{*}(\gamma,\mu)\}\}\} \qquad (12)$$

$IMLT$ consult with inverse modified Logistic transform and IBT check with the inverse Baker map. The conjugate of two amplitude and segment modulations are applied to the optical signal to decrypt the photograph, after that convert the optical sign to electric sign via optical detector and randomized via the changed Logistic map to get the original picture.

4. Encryption Quality Metrics and Analysis

Several Matlab simulation tests have been completed to research the proposed encryption approach, which has been applied to the Lena, Peppers and Baboon photos as shown in Fig. 6 to compare the proposed technique with a Logistic map, Baker map and DRPE in overall performance and noise immunity. These pics database specifications which were utilized in simulation experiments are defined in Table I.

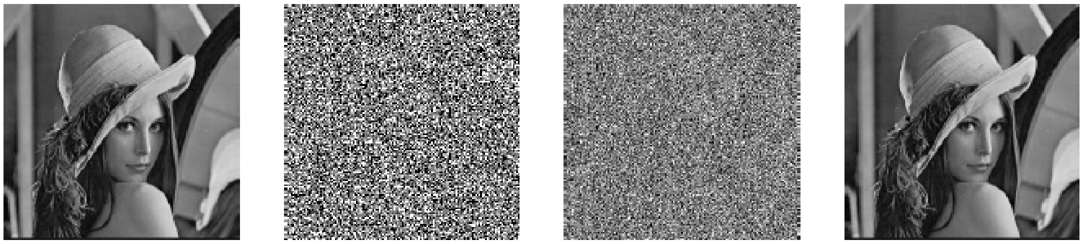
Table 1. Images database specifications

Encryption technique	**Lena**	**Peppers**	**Baboon**
Color	Grayscale	Grayscale	Grayscale
Dimensions	512×512	512×512	512×512
Bit depth	8	8	8
Image type	Bitmap	Bitmap	Bitmap

(a) (b) (C)

Figure 6. (a) Lena, (b) Peppers, and (c) Baboon images.

Visible inspection is a critical metric of photograph encryption, but it isn't sufficient to determine the robustness of proposed algorithm [23].



a. Original image

b. Amplitude and phase modulation

c. Modified Logistic map Encryption

d. Decrypted image

Figure 7. Visual inspection for Lena image.

It's clear that the cryptograph pictures are absolutely unrecognizable and do well to hide the information of the original photos. Therefore, the anticipated encryption set of rules is suitable from visual inspection factor of view [24].

4.1. Histogram Analysis

A grayscale picture is given the very best depth value L (for a picture with eight bits/ pixel L=255). The intensity degree histogram (grey) is described as a characteristic h(g) which is the same as value the number of pixels within the photo (or inside the region of the hobby) that have a depth equal to g, for every depth degree g ϵ [0 … L] [25].

$$h(g)= Ng \tag{12}$$

Where Ng present within the photograph is the number of pixels inside the location of hobby that have the intensity identical tog. Histogram evaluation is used to ensure factors: the first factor is that the original photograph and encrypted picture ought to be absolutely different, 2nd point is that the unique picture and the decrypted photo are much like every different. From Figure. 8 it's clear that all encryption techniques fulfilled the terms of histogram evaluation but Baker map encryption method no longer fulfills the terms because the histogram of the encrypted image is identical to histogram of the unique picture.

4.2. Correlation Coefficient Analysis

This evaluation applied among authentic sample photograph and encrypted sample photograph is used as a metric to evaluate the encryption method. This metric can be calculated as the subsequent equation [26]:

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{13}$$

In which x and y are the gray-scale standards of pixels on the equal directories in the apparent and cipher snap shots. In arithmetical calculations, the subsequent distinct formulations can be used.

$$E(x) = \frac{1}{L}\sum_{i=1}^{L} x_i \tag{14}$$

$$D(x) = \frac{1}{L}\sum_{i=1}^{L} (x_i - E(x))^2 \tag{15}$$

$$\operatorname{cov}(x,y)=\frac{1}{L}\sum_{i=1}^{L}(x_i-E(x))(y_i-E(y)) \qquad (16)$$

Where L is the quantity of pixels worried within the scheming. The nearer value of r_{xy} is to 0, the better the incomparability of the encryption procedure.

Table II. demonstrates values of correlation coefficient parameters for all encryption techniques. The power of encryption technique increases the lower the value of correlation coefficient and near 0. Table II. Clarifies that the best correlation coefficient value appears in the proposed approach in comparison to other encryption techniques.

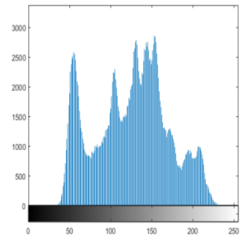
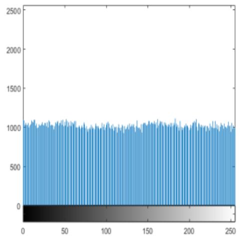
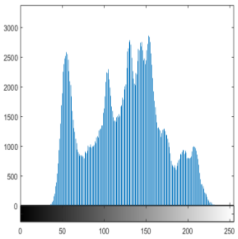
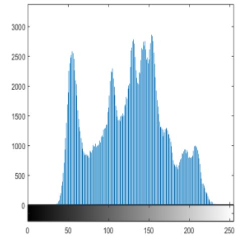
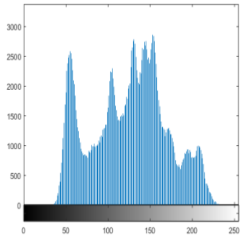
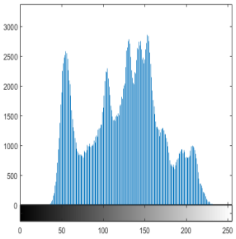
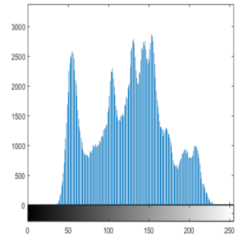
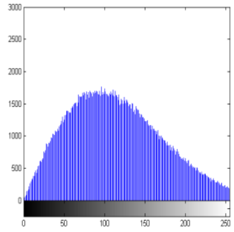
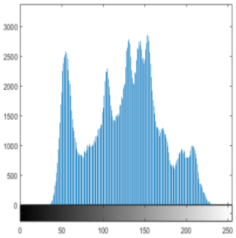
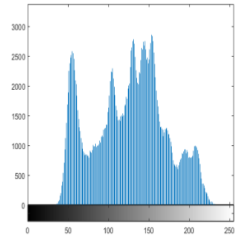
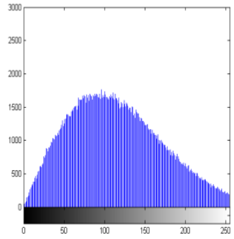
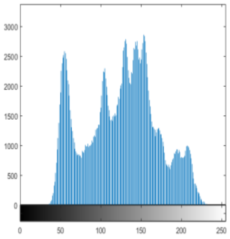
Techniques	**Original sample image**	**Encrypted sample image**	**Decrypted sample image**
(a) Logistic Map			
(b) Baker Map			
(c) DRPE			
(d) Proposed Technique			

Table 2. Correlation coefficient analysis between all encryption techniques including the proposed one.

Encryption Technique	Lena	Peppers	Baboon
Logistic map	-0.0154	-0.0165	-0.0291
Baker map	0.0014	0.0098	0.0118
DRPE	0.0016	0.0063	0.0057
Proposed Technique	0.0005	0.0028	0.0001

4.3. Maximum Deviation Analysis

This analysis measures how massive a deviation there may be between the histogram of unique pattern photograph and histogram of the encrypted image via the nature of encryption approach. Ideally, this should be maximum or an excessive value. Table III. Demonstrates that the maximum deviation value appears within the proposed encryption approach when compared to other encryption strategies.

Table 3. Maximum deviation analysis of all encryption techniques including the proposed one.

Encryption Technique	Lena	Peppers	Baboon
Logistic map	0.4860	0.3913	0.5223
Baker map	0	0	0
DRPE	0.8569	0.8550	0.8457
Proposed Technique	1	0.8766	0.8563

4.4. Irregular Deviation Analysis

Abnormal deviation analysis is based on measuring the extent of the deviation through encryption on the encrypted photograph. Higher efficacy of the encryption technique is indicated by low value of these parameters. The abnormal deviation DI is calculated by the following equation:

$$H_D(i) = \left| H(i) - M_H \right| \tag{17}$$

Where H(i) present histogram value of absolute difference matrix between original and encrypted images, MH is the main value of this histogram.

$$D_I = \frac{\sum_{i=0}^{255} H_D(i)}{M \times N} \tag{18}$$

Table IV. Demonstrates that the proposed technique in this metric analysis is lower than other encryption techniques.

Table 4. Irregular deviation analysis of all encryption techniques including the proposed one.

Encryption Technique	Lena	Peppers	Baboon
Logistic map	0.6877	0.5695	0.6932
Baker map	0.9552	0.8364	1
DRPE	0.6707	0.7318	0.7307
Proposed Technique	0.3876	0.3603	0.3592

4.5. Encryption Time Analysis

Encryption time analysis, one of the key parameters for measuring encryption system time, is the time needed for encryption procedure from beginning till giving up. However, internet encryption must consume the least time possible for encryption technique to be used in programs like video conference and live television. Table V. demonstrates the lowest time appears inside the DRPE encryption method, more so than different encryption strategies. However, the proposed encryption approach has a small encryption time which does not exceed 2 seconds.

Table 5. Encryption process time (sec) for all encryption techniques including the proposed one.

Encryption Technique	Lena	Peppers	Baboon
Logistic map	0.8046	0.9058	0.9082
Baker map	0.8764	0.8872	0.9704
DRPE	0.6593	0.6025	0.5367
Proposed Technique	1.1365	1.1211	1.0727

4.6. Noise Immunity

Noise immunity evaluation is one of the most essential metrics to determine if this encryption approach is suitable to use in any verbal exchange gadget. An evaluation of the authentic sample picture and decrypted photograph inside the height sign to noise ratio shows the presence of additive white Gaussian noise with variance 0.01. PSNR is expressed as the following equation:

$$MSE = \frac{1}{XY} \sum_{x=1}^{X} \sum_{y=1}^{Y} \left| f(x, y) - \hat{f}(x, y) \right|^2 \tag{19}$$

Wherever X and Y are the picture magnitudes. $f(x, y)$ and $\hat{f}(x, y)$ denote the innovative and the decrypted pictures, correspondingly.

$$PSNR = 10 \log_{10} \left(\frac{\text{Max Intensity of Image}}{MSE} \right) \tag{20}$$

Table VI. demonstrates that the proposed approach is the best in terms of electricity immunity to noise in comparison to different encryption techniques. Table VI indicates that our proposed approach shows desirable results to be used in all fashions of verbal exchange systems.

Table 6. PSNR (dB) values for all encryption techniques including the proposed one.

Encryption Technique	Lena	Peppers	Baboon
Logistic map	18.5646	17.8999	18.7482
Baker map	8.1517	9.9379	8.8715
DRPE	18.5640	17.9016	18.7461
Proposed Technique	28.0129	30.4805	28.3508

5. CONCLUSION

In this paper, a unique image encryption technique based on randomized pixel positions, amplitude modulation and phase modulation is proposed. The proposed approach based on the modified Logistic chaotic map and modified amplitude modulation increases complexity. Also, the implementation of the proposed technique used numerous keys. Both of these factors increase the solidity of encryption, thus making it exceptionally strong against unauthorized attackers. The proposed technique accomplished excellent evaluation outcomes in correlation coefficient, maximum deviation, irregular deviation, encryption time and immunity to noise. All results indicate the suitability of the proposed encryption technique in ideal conversation networks.

REFERENCES

[1] L. Zhang, Bo Liu, X. Xin, Qi Zhang, J. Yu, and Y wang. (2013). Theory and Performance Analyses in Secure CO-OFDM Transmission System Based on Two-Dimensional Permutation. Journal of Lightwave Technology, VOL 31, pp74-80.

[2] L. Zhang, X. Xin, Bo Liu, and Y Wang. (2011). Secure OFDM-PON Based on Chaos Scrambling. IEEE Photonics Technology, VOL 23, pp 998-1000.

[3] M. Bi, X. Fu, X. Zhou, Lu Z., G. Yang, X. Yang, S Xiao, and W Hu. (2017).A Key Space Enhanced Chaotic Encryption Scheme for Physical Layer Security in OFDM-PON. IEEE Photonics Journal, VOL 9, pp 1-10.

[4] W. Zhang, C. Zhang, C. Chen, H. Zhang, W. Jin, and Kun Qiu. (2017). Hybrid Chaotic Confusion and Diffusion of Physical Layer Security in OFDM-PON. IEEE Photonics Journal, VOL 9, pp 1-7.

[5] S. Chen, T. Hwang, and Wen-Wei Lin. (2010). Randomness Enhancement Using Digitalized Modified Logistic Map. IEEE Transactions on Circuits and Systems, VOL 57, pp 996-1000.

[6] Lingfeng Liu, Suoxia Miao, Hanping Hu, Yashuang Deng. (2015). Pseudorandom bit generator based on nonstationary logistic maps. IET Information Security, VOL 10, pp 87-94.

[7] Xianye Li, Xiangfeng Meng, Xiulun Yang, Yongkai Yin, Yurong Wang, Xiang Peng, Wenqi He, Guoyan Dong, and Hongyi Chen. (2016). Multiple-Image Encryption Based on Compressive Ghost Imaging and Coordinate Sampling. IEEE Photonics Journal, VOL 8, pp 1-11.

[8] Xuejing Kang, Feng Zhang, and Ran Tao. (2015). Multichannel Random Discrete Fractional Fourier Transform. IEEE Signal Processing, VOL 22, pp 1340-1344.

[9] P. Harsha. (2017). A Novel Micro-architecture using a Simplified Logistic Map for Embedded Security. IEEE Embedded Systems, VOL 9, pp 41-44.

[10] Guo Cheng Wu, Dumitru Baleanu. (2014). Chaos synchronization of the discrete fractional logistic map. Signal Processing Elsevier Journal, VOL 102, pp 96-99.

[11] Liansheng Sui, Kuaikuai Duan, Junli Liang. (2015). Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps. Optics Communications Elsevier Journal, VOL 343, pp 140-149.

[12] Manish Kumar, Sunil Kumar, Rajat Budhiraja, M.K. Das, Sanjeev Singh. (2016). A cryptographic model based on the logistic map and a 3-D matrix. Journal of Information Security and Applications Elsevier Journal, VOL 32, pp 47-58.

[13] Huiqing Huang, Shouzhi Yang. (2017). Colour image encryption based on logistic mapping and double random-phase encoding. IET Image Processing Journal, VOL 11, pp 211-216.

[14] Yiyuan X., Jiachao Li, Zhoufan K., Yushu Z., Xiaofeng L., and Yong L., "Exploiting Optics Chaos for Image Encryption-then-Transmission," IEEE JLT, VOL 34, No. 22, PP. 5101-5109, NOVEMBER VOL 15, pp 2016.

[15] Yannick A, Alain T. (2016). Image encryption by chaos mixing. IET Journal Image Processing, VOL10, No. 10, pp 742-750.

[16] Ahmed M. Elshamy, Ahmed N., Abd El-Naser A., Osama S. Faragallah, Yi Mu, Saleh A., Fathi E. (2013). Optical Image Encryption based on Chaotic Baker Map and Double Random phase Encoding. Light Wave Technology Journal- IEEE, Vol 31, No. 15, pp. 2533-2539.

[17] Ahmad M. Elshamy, Fathi E. Abd El-Samie, Osama S. Faragallah, Elsayed M. Elshamy, Hala S. El-sayed, S. F. El-zoghdy, Ahmed N. Z. Rashed , Abd El-Naser A. and Ahmad Q. Alhamad. (2016). Optical Image Cryptosystem Using Double Random Phase Encoding and Arnold's Cat Map. Optical and Quantum Electronics-Springer Journal, VOL 48, No. 3, pp. 1-18.

[18] Ahmed M. Elshamy, Aziza I. Hussein, Hesham F. A. Hamed, M. A. Abdelghany, Hamdy M. Kelash, and Ahmad Q. Alhamad. (2016). Optical Cryptosystem for Color Image Based on Double Random Phase Encryption in Discrete Fourier Domain and Color Indexed Map. IJCSIS, VOL 14, No. 8, pp. 763-780.

[19] Ahmed M. Elshamy, Aziza I. Hussein, Hesham F. A. Hamed, M. A. Abdelghany, Hamdy M. Kelash, and Ahmad Q. Alhamad. (2017). Secure Implementation for Video Streams Based on Fully and Permutation Encryption Techniques. IJCIS- IEEE Conference, PP. 50-55.

[20] Ahmed M. Elshamy, Aziza I. Hussein, Hesham F. A. Hamed, M. A. Abdelghany, and Hamdy M. Kelash. (2018). Image Encryption Techniques Based on Chaos Maps and Two Random Phase Modulation in Discrete Fourier Transform. Wulfenia Journal, VOL 25, No. 2, PP. 81-90.

[21] N.K. Pareek, Vinod Patidar, and K.K. Sud.(2005). Cryptography using multiple one-dimensional chaotic maps. Commun. Nonlinear Sci.umer. Simul. VOL 10, pp. 715-723.

[22] Z. Yun-peng, L. Wei, C. Shui-ping, Z. Zheng-jun, N. Xuan, and D. Weidi.(2009). Digital image encryption algorithm based on chaos and improved DES. Systems, Man and Cybernetics, IEEE Int. The conference, pp. 474-479.

[23] Y. Honglei , W. Guang-shou, W. Ting , L. Diantao, Y. Jun, M. Weitao, F. Y. Shaolei and M. Yuankao. (2009). An image encryption algorithm based on two-dimensional baker map. in Proc. ICICTA.

[24] Rajinder Kaur, Er. Kanwalpreet Singh. (2013). Comparative Analysis and Implementation of Image Encryption Algorithms. IJCSMC, VOL. 2, Issue. 4, pg.170 – 176.

[25] Nidhi Sethi. (2012). A New Image Encryption Method using Chirikov and Logistic Map. International Journal of Computer Applications (0975 – 8887), VOL 59– No.3.

[26] Sudip G., Sambaran H, Santi P, Hafizur R. (2015). A new algorithm for grayscale image histogram computation. INDICON IEEE conference.

[27] Fangjun H., JiwuH., Yun Q. (2016). New Framework for Reversible Data Hiding in Encrypted Domain. IEEE SPS Journal, VOL 11, No. 12, pp 2777-2789.

Authors

Ahmed M. ELShamy received his Bachelor’s degree in Electronics and Electrical Communication Engineering, 2010, his graduation project got best project in the level of EGYPT in Communication Engineering Field, 2010. He completed his Masters in Electronics and Electrical Communication Engineering from the University of Menofiah, Egypt, 2014.

He is currently Lecturer in Information Technology College at Fujairah University, Fujairah-UAE. Moreover, he is working in Fujairah e-Government as a Network and Security Specialist. He had many publications in international journals and conferences, his research interests include Network Security for its Analysis and Enhancement, Multimedia Security, Digital Encryption, Optical Encryption, Image Processing, Chaos Theory, authentication and Communications Networks. He has worked for various conferences at different levels from reviewer to organizer-chairman.

Aziza I. Hussein received her Ph.D. degree in Electrical & Computer Engineering from Kansas State University, USA in 2001 and the M.Sc. and B.Sc. degrees from Assiut University, Egypt in 1989 and 1983, respectively.

She joined Effat University in Saudi Arabia In 2004 and established the first Electrical and Computer Engineering program for women in the country and taught related courses. She was the head of the Electrical and Computer Engineering Department at Effat University from 2007-2010. She was the head of Computer and Systems Engineering Department, Faculty of Engineering, Minia University, Egypt from 2011-2016. Currently she is the head of the Electrical & Computer Engineering Department at Effat University Saudi Arabia.

Her research interests include microelectronics, analog/digital VLSI system design, RF circuit design, high-speed analog-to-digital converters design and wireless communications.ziza I. Hussein received her Ph.D. degree in Electrical & Computer Engineering from Kansas State University, USA in 2001 and the M.Sc. and B.Sc. degrees from Assiut University, Egypt in 1989 and 1983, respectively.

Her research interests include microelectronics, analog/digital VLSI system design, RF circuit design, high-speed analog-to-digital converters design and wireless communications.

Hesham F. A. Hamed was born in Giza, Egypt, in 1966. He received the B.Sc. degree in electrical engineering, the M.Sc. and Ph. D. degrees in electronics and communications engineering from EL-Minia University, EL-Minia, Egypt, in 1989, 1993,and 1997 respectively. He currently is the dean of faculty of engineering ,Minia University. He was a Visiting Researcher at Ohio University, Athens, Ohio. From 1989 to 1993 he worked as a Teacher Assistant in the Electrical Engineering Department, EL-Minia University. From 1993 to 1995 he was a visiting scholar at Cairo University, Cairo, Egypt. From 1995 to 1997 he was a visiting scholar at Texas A&M University, College Station, Texas (with the group of VLSI). From 1997 to 2003 he was an Assistant Professor in the Electrical Engineering Department, EL-Minia University. From 2003 to 2005 he was Associate Professor in the same University. He has published more than 80 papers. His research interests include analog and mixed-mode circuit design, low voltage low power analog circuits, current mode circuits, nano-circuits design, and FPGA.

Mahmoud A. Abdelghany was born in Saudi Arabia in 1979. He received the B.S. (Electrical Engineering) and the Master of Science (Communication Engineering) degrees from Minia University in 2000 and 2005, respectively and PhD degree from Kyushu University, Japan in 2011. He had been a post-doctoral research fellow with the Radio-Frequency Integrated Circuits (RFIC) & Microwave Communication Devices Laboratory, Kyushu University, Japan from October 2013 to April 2014. In December 2011, he joined the Electrical Engineering Department, Faculty of Engineering, Minia University as an assistant professor. In February 2017, he joined the Electrical Engineering (Communication and computer Engineering) Department, Faculty of Engineering, Nahda University as an assistant professor. His current research interests include the study and design of RF CMOS System LSI and low-power, low-noise and highly linear CMOS RF front-end architectures. Dr. Mahmoud is a member of the Institute of Electrical and Electronics Engineers (IEEE).

Hamdy Kelash received the B.Sc. and M.Sc degrees in Computer Science and Engineering from Menoufia University, Menouf, Egypt, in 1971 and 1979,also he received PhD from France in 1985. respectively. He is currently Full Professor with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University. His current research interests include network security, cryptography, internet security, multimedia security, image encryption, watermarking, steganography, data hiding, medical image processing, and chaos theory.