Efficient Chaotic Tent Map-based Image Cryptosystem

Mohammed A. AlZain
Department of Information Technology
College of Computers and Information Technology
Taif University, P.O. Box 888, Al-Hawiya-Taif, 21974, KSA

Osama S. Faragallah
Department of Information Technology
College of Computers and Information Technology
Taif University, P.O. Box 888, Al-Hawiya-Taif, 21974, KSA

ABSTRACT
This paper presents an efficient chaotic image encryption cipher that is designed with the aim of improving the security and enhancing the encryption efficiency. In this paper, a chaotic tent map (CTM) is utilized to build a new digital chaotic image cryptosystem. The characteristics of CTM are very suitable for the design of encryption schemes. The security estimation of the proposed CTM-based image cryptosystem against brute-force, statistical, and differential attacks is investigated from strict cryptographic viewpoint. Experimental tests are performed with detailed analysis confirming the high security of the proposed CTM-based image cryptosystem.

General Terms
Security, Image Encryption.

Keywords
Symmetric encryption, Chaos, Encryption quality, Tent map, and Security analysis.

1. INTRODUCTION
The field of encryption is becoming very important in the present era in which information security is of utmost concern. Security is an important issue in communication and storage of text, images, audio and video. Encryption has several applications in Internet communication, multimedia systems, medical imaging, telemedicine, military communication, pay-TV, and confidential video conferencing, etc. In this regard, a variety of encryption schemes have been proposed to mask the multimedia data streams, such as DES (Data Encryption Standard) [1-2], optical encryption [3-7], IDEA (International Data Encryption Algorithm) [8-9] and RSA [9].

The intrinsic characteristics of images make traditional algorithms such as DES, IDEA and RSA not suitable for practical image encryption to some intrinsic features of multimedia such as bulk data capacity and high redundancy, which are troublesome for traditional encryption [10-12]. Moreover these encryption schemes require extra operations on compressed multimedia data thereby demanding long computational time and high computing power. In real-time communications, due to their low encryption and decryption speeds, they may introduce significant latency [13-14]. Currently, chaotic maps have been considered as a way to solve such problems [15-18].

The characteristics of the chaotic maps have attracted the attention of cryptographers since it has many fundamental properties such as ergodicity, sensitivity to initial condition and system parameter, and mixing property, etc [19-21].

Most properties are related to some requirements such as mixing and diffusion in the sense of cryptography. Therefore, chaotic cryptosystems have more useful and practical applications.

The close relationship between chaos and cryptography makes chaos based cryptographic algorithms as natural candidates for secure communication and cryptography. Chaos based encryption techniques are considered good for practical use as these techniques provide a good combination of speed, high security, complexity, reasonable computational overheads and computational power etc. In this paper, we propose a new image encryption algorithm based on a chaotic tent map which is a symmetric encryption algorithm.

We examine its implementation for digital images, providing its encryption quality estimation, and security analysis with respect to brute-force, information entropy, cipher cycle, statistical, and differential attacks. Experimental results for security analysis show that the proposed CTM-based image cryptosystem has satisfactory security, which makes it a potential candidate for encryption of multimedia data such as images, audios and even videos.

The rest of the paper is organized as follows. In Section 2, the cryptosystem is presented. Section 3 is devoted to experimental results. Section 4 analyzes the security of the cryptosystem. Finally, some comments and conclusions are given in Section 5.

2. DESCRIPTION OF THE CRYPTOSYSTEM

2.1 Chaotic Tent Map and its Analysis
One of the simplest chaos functions that have been studied recently for cryptography applications is the tent map [22]:

$$T(x)=\begin{cases} r\,x & x>0.5 \\ r(1-x) & x\le 0.5 \end{cases} \quad (1)$$

Define an iterative map by

$$X_{n+1}=T(x_n) \quad (2)$$

where $0 \le r \le 2$, $X_n \in [0,1]$. The tent map is constructed from two straight lines, which makes the analysis simpler than for truly nonlinear systems. The graph of the tent map function is plotted using MATLAB software and is given in Fig. 1.

Although the form of the tent map is simple and the equation involved is linear, for certain parameter values, this system can display highly complex behavior and even chaotic phenomena. Figs. 2-4 show the simulation of the tent map. The simulation results include three portions. It is described as follows: let the initial value: x0=0.3, loop iteration =30. The parameter r can be divided into three segments, which can be examined by experiments on the following conditions:

1. When $r \in [0,1]$ as shown in Fig. 2, the calculation results come to the same value after several iterations with no chaotic behavior.

2. When $r \in [1,1.4]$, the system appears periodicity, as shown in Fig. 3.
3. While $r \in [1.4,2]$, it becomes a chaotic system with periodicity disappeared as shown in Fig. 4, so it can be used for image cryptosystems.

Also, we use MATLAB software to graph the bifurcation diagram of the tent map as shown in Fig. 5.

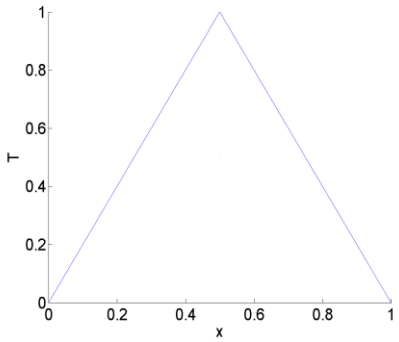


Fig. 1: The graph of the tent map

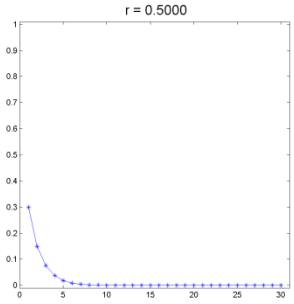


Fig.2: Iteration property when r=0.5

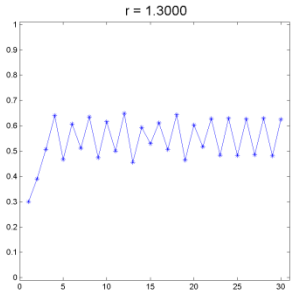


Fig. 3: Iteration property when r=1.3

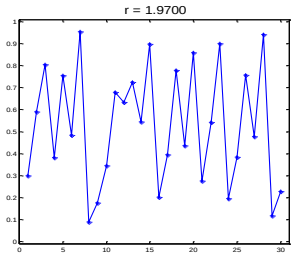


Fig. 4: Iteration property when r=1.97

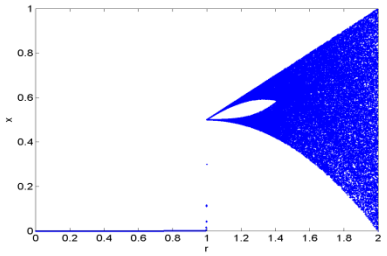


Fig. 5: The bifurcation diagram of the tent map

2.2 Encryption and decryption

Here, we propose a new approach for image encryption using chaotic tent map. The chaotic tent map is used as the core of the scheme to achieve the security requirements. In order to transform the plainimage to the cipherimage we do the following algorithm.

1. Convert the plainimage into binary, and then divide it into a series packet in length of 128-bit. If the length of the last packet is less than 128, fulfill it with 0.
2. Give initial value X_0 and control parameter r; calculate the chaotic sequence of the tent map according to equation (1), the chaotic sequence $X_n \in [0,1]$. Mapping xn into the range of [1.4,2], hence generate sequence a , which is chosen as the parameter of equation (3)
3. Calculate the secret key K_n from the following formula:

$$K_n = floor(K_{n-1} * a + K_{n-1})^2 \quad (3)$$

$K_n \in [0,1]$, L is the number of possible gray levels

4. Convert K_n into binary, and then obtain the intermediate cipherimage C_n by carrying out the XOR operation with The plainimage P_n through the following formula:

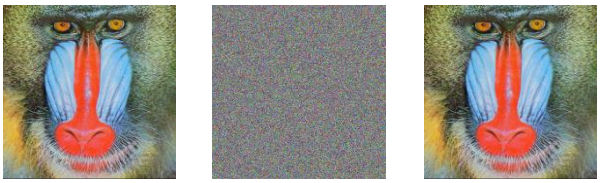
$$C_n = (P_n \oplus (K_n \bmod L)) \quad (4)$$

5. Quit out, if clear images are all encrypted, else get the next packet and return to step 2.

The decryption algorithm is a reverse process of the encryption algorithm. After converted into binary, ciphered image will be carried out the XOR operation with decryption sequences, which could be obtained after the reverse process of the encryption algorithm, and then the decrypted image will be obtained.

3. EXPERIMENTAL RESULTS

Results of some experiments are given to prove its efficiency of application to digital images. We use several images that are homogenous, grayscale, true color, containing repeated patterns, high and/or low frequency components as the original images (plainimages). As shown, the encrypted images (cipherimage) regions are totally invisible. The visual inspection of Figs. 6-8 shows the possibility of applying the proposed scheme successfully in both encryption and decryption. Also, it reveals its effectiveness in hiding the information contained in them.



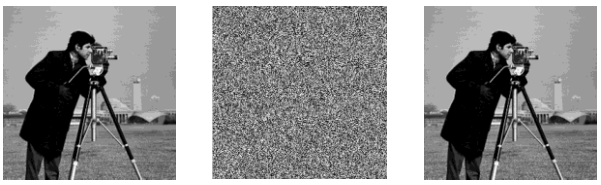
a) Original image b) Encrypted image c) Decrypted image

Fig. 6: Application of the proposed cipher to Baboon.gif of size 512x512

4. SECURITY ANALYSIS

The security of an image cryptosystem is determined by its confusion and diffusion capabilities. It is usually evaluated by the following quantitative measures [23-25].

4.1 Statistical Analysis



a) Original image b) Encrypted image c) Decrypted image

Fig. 8: Application of the proposed cipher to Cameraman.tif of size 128x128

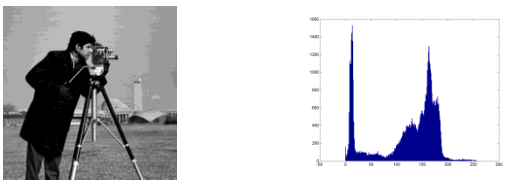
It is well-known that the statistical analysis on cipherimage is of crucial importance for a cryptosystem. In fact, an ideal cipher should be robust against any statistical attacks. In order to evaluate the security of image cryptosystems, the following statistical tests are usually performed.

4.1.1 Histogram

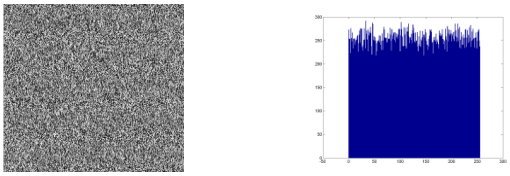
The histogram of the cipherimage is plotted to see whether it is sufficiently uniform. A good image encryption scheme should always generate a cipherimage of uniform histogram for any plainimages. We have calculated and analyzed the histograms of the several encrypted images as well as its original images that have widely different content. One typical example among them is shown in Fig. 9.

The original-image with the size 256x256 is shown in Fig.9 (a) and the histogram of the original-image is shown in Fig. 9(b). Fig. 9(c) is the encrypted image and Fig. 9(d) is the histogram of the encrypted image.

It is clear that the histogram of the encrypted image is fairly uniform and significantly different from the respective histograms of the original image and hence does not provide any clue to employ any statistical attack on the proposed image encryption procedure.



(a) The original-image (b) The histogram of the original-image;



(c) The encrypted image (d) The histogram of the encrypted image

Fig. 9: The original-image , the encrypted image , and the histogram for each one

4.1.2 Correlation of adjacent pixels

In addition to the histogram analysis, we have also analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plainimage/cipherimage respectively. The procedure is as follows: First, randomly select 1000 pairs of two adjacent pixels from an image. Then, calculate their correlation coefficient using the following two formulas:

$$\mathrm{cov}(x,y) = E(x - E(x))(y - E(y)), \quad (5)$$

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \quad (6)$$

where x and y are grey-scale values of two adjacent pixels in the image. In numerical computations, the following discrete formulas were used:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (7)$$

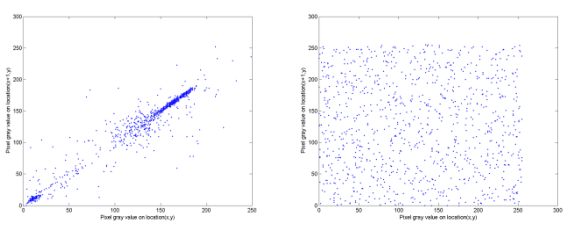
$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2, \quad (8)$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)), \quad (9)$$

Fig. 10 shows the correlation distribution of two horizontally adjacent pixels in plainimage cipherimage for the proposed cipher. The correlation coefficients are 0.9661 and -0.0233, respectively for both Lena plainimage and cipherimage, which are far apart. Similar results for diagonal and vertical directions were obtained as shown in Table 1. It is clear that from the Fig. 9 and Table 1 that there is negligible correlation between the two adjacent pixels in the cipherimage. However, the two adjacent pixels in the plaintext are highly correlated.

Table 1. Correlation coefficient of two adjacent pixels in original and encrypted Cman image

Direction	Plainimage	Cipherimage
Horizontal	0.9661	-0.0233
Vertical	0.9508	-0.0674
Diagonal	0.9168	0.0280



(a) (b)

Fig. 10: Two horizontally adjacent pixels Correlation in plainimage/cipherimage, respectively

4.1.3 Information entropy analysis

Information theory is the mathematical theory of data communication and storage founded in 1949 by C.E. Shannon [26]. Modern information theory is concerned with error-correction, data compression, cryptography, communications systems, and related topics. To calculate the entropy H (m) of a source m, we have:

$$H(m) = \sum_{i=0}^{2^N-1} P(m_i) \log_2 \frac{1}{P(m_i)} \; bits \qquad 10$$

where p (mi) represents the probability of symbol mi and the entropy is expressed in bits. Let us suppose that the source emits 2^8 symbols with equal probability, i.e., after evaluating Eq. (9), we obtain its entropy H (m) = 8, corresponding to a truly random source. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security.

Let us consider the ciphertext of image encryption using the proposed block cipher, the number of occurrence of each ciphertext block is recorded and the probability of occurrence is computed. The entropy is as follows:

$$H(m) = \sum_{i=0}^{255} P(m_i) \log_2 \frac{1}{P(m_i)} = 7.9974 \approx 8 \qquad 11$$

The value obtained is very close to the theoretical value of 8. This means that information leakage in the encryption process is negligible and the encryption system is secure upon the entropy attack.

4.2 Resistance against Differential attack

In order to resist differential attack, a tiny alteration in the plainimage should cause a substantial change in the cipherimage. This is a measure of the plainimage sensitivity which can be obtained using the following procedures. A plainimage is first encrypted to a cipher-image C1. Then a pixel in the plainimage is randomly selected to have a tiny change, e.g., add/subtract 1 to/from its decimal value, or toggle the least significant bit. The modified image is encrypted using the same key to generate a new cipher-image C2. The two cipher-images are then compared quantitatively using the following measures [27]:

1. Number of pixels change rate (NPCR): It counts the percentage of different pixels between the cipher-images C1 and C2, using the following equation:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \qquad 12$$

where D(i, j) is a binary value, W and H are width and height of the cipherimage, respectively. The pixel values at position (i, j) of C1 and C2 are denoted as C1(i, j) and C2(i, j), respectively. If C1(i, j) = C2(i, j), D(i, j) =1; otherwise, D(i, j) = 0.

2. Unified average changing intensity (UACI): This is a measure of the average intensity of differences between the cipher-images C1 and C2, as defined by:

$$UACI = \frac{1}{W \times H} \left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255} \right] \times 100\%, \qquad 13$$

Tests have been performed on the proposed algorithm, about one-pixel change influence on a 256 grayscale image of size .We obtained NPCR= 99.62% and UACI=31.23%. The results show that a swiftly change in the original image will result in a significant change in the ciphered image, so the algorithm proposed has a good ability to anti differential attack.

4.3 Sensitivity Analysis

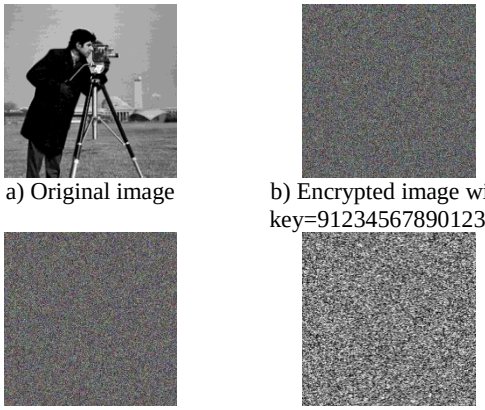
An ideal encryption procedure should be sensitive with respect to both the secret key and plainimage. The proposed CTM-based image cryptosystem has high key and plaintext sensitivities. This means that a slight change in the key or in the plaintext will causes great changes in the ciphertext. These properties make various sensitivity-based (differential) attacks difficult. To prove the robustness of the proposed CTM-based image cryptosystem, we will employ sensitivity analysis with respect to both key and plaintext.

4.3.1 Key Sensitivity Analysis

An encryption scheme has to be key-sensitive, meaning that a tiny change in the key will cause a significant change in the output. Assume that a 16-character (128-bit) ciphering key is used. For testing the key sensitivity of the proposed CTM-based image cryptosystem, we have performed the following steps:

1. First, a 2562x256 image is encrypted using the test key "9123456789012345".
2. Then, the least significant bit of the key is changed, so that the original key becomes, say "9123456789012346" in this example, which is used to encrypt the same image.
3. Finally, the above two ciphered images, encrypted by the two keys, are compared.

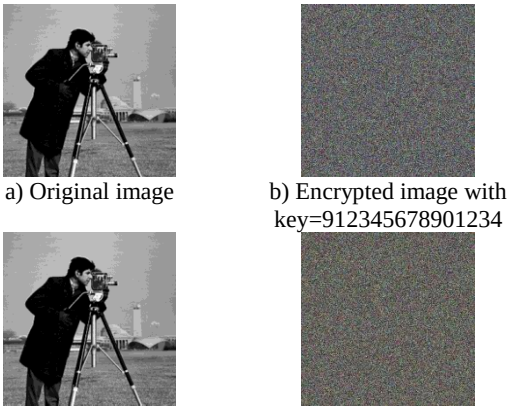
The result of key sensitivity analysis shows that changing one bit in encryption key will result in a completely different cipherimage by more than 99% in terms of pixel grey scale values. Fig. 11 shows the test results. High key sensitivity is required by secure cryptosystems, which means that the cipherimage cannot be decrypted correctly although there is only a slight difference between encryption and decryption keys. This guarantees the security of the proposed CTM-based image cryptosystem against brute-force attacks.



a) Original image
b) Encrypted image with key=9123456789012345
c) Encrypted image with key=9123456789012346
d) Difference image between (b) and (c)

Fig. 11: Key sensitive test result 1 with the proposed CTM-based image cryptosystem

So, when a 16-character key is used to encrypt an image while another trivially modified key is used to decrypt the ciphered image, the decryption also completely fails. Fig. 12 has verified this and clearly shows that the image encrypted by the key "9123456789012345" is not correctly decrypted by using the key "9123456789012346", which has also only one bit difference between the two keys. It is clear that the decryption with a slightly different key fails completely and hence the proposed CTM-based image cryptosystem is highly key sensitive.



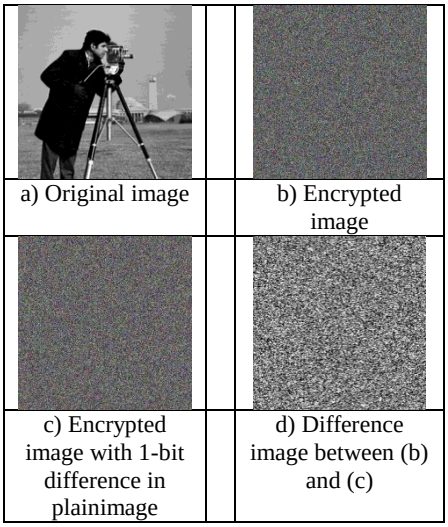
a) Original image
b) Encrypted image with key=912345678901234
c) Decrypted image with key=9123456789012345
d) Decrypted image with key=9123456789012346

Fig. 12: Key sensitive test result 2 with the proposed CTM-based image cryptosystem

4.3.2 Plain image Sensitivity Analysis

In general, the opponent may make a slight change such as modifying only one pixel of the original image, and then observes the change of the result. In this way, he may be able to find out a meaningful relationship between the plainimage and the cipherimage. If one minor change in the plainimage can cause a significant change in the cipherimage, then this differential attack would become very inefficient and practically useless. In order to avoid the known-plaintext and the chosen-plaintext attacks (differential attacks), the changes in the cipher image should be significant even with a small change in the original one. According to the proposed CTM-based image cryptosystem, this small difference should be diffused to the whole ciphered data. They can in fact be reflected by .

A desirable property for the proposed CTM-based image cryptosystem is that it is highly sensitive to small change in the plainimage (single bit change in plainimage). The average pixel differences of some well-known images are computed for the two encrypted images whose plainimages have only one-bit change. The results are tabulated in Table 2. It can be observed that the values are very close to the expected value of pixel difference on two randomly generated images (99.609375%). Fig. 23 shows an example of two enciphered images from two plainimages with only 1-bit difference generated using the proposed CTM-based image cryptosystem. The original and encrypted images are shown in Figs. 13(a) and (b), respectively, Fig. 13(c) is the encrypted image with only one-bit change in the original image (a), while (d) is the difference-image between the two encrypted images: (b) and (c). As can be seen, most of the pixels in Fig. 13(d) are nonzero, which means that the difference between image (b) and image (c) is big enough. Thus, the proposed CTM-based image cryptosystem has high plainimage sensitivity.



a) Original image
b) Encrypted image
c) Encrypted image with 1-bit difference in plainimage
d) Difference image between (b) and (c)

Fig. 13: Plaintext sensitivity test with the proposed CTM-based image cryptosystem

Table 2. Pixel difference between encrypted images with 1-bit difference in their plainimages

Image	Pixel difference (mean NPCR)
Lena	99.6123%
Cman	99.6378%
House	99.67846%
Barbara	99.66252%

5. CONCLUSION

In this paper, a new scheme for image encryption named CTM-based image cryptosystem that based on chaotic tent map. The chaotic tent map is chosen, for certain parameter values, this proposed CTM-based image cryptosystem can display highly complex behavior and even chaotic phenomena. The security analysis of the proposed CTM-based image cryptosystem confirms a high security level. Experiments show the proposed CTM-based image cryptosystem is promising for image encryption.

6. REFERENCES

[1] National Bureau of standards. "Data Encryption Standard," Federal Information processing standards Publication 46, US Government Printing Office, Washington, D.C., 1977.

[2] NIST Computer Security Division's (CSD) Security Technology Group (STG) (2013). "Block cipher modes", Cryptographic Toolkit. NIST. Retrieved April 12, 2013.

[3] Ahmad M. Elshamy, Ahmed N. Z. Rashed, Abd El-Naser A. Mohamed, Osama S. Faragallah, Yi Mu, Saleh A. Alshebeili and F. E. Abd El-Samie, "Optical Image Encryption Based on Chaotic Baker Map and Double Random Phase Encoding," IEEE/OSA Journal of Lightwave Technology, vol. 31(15), pp. 2533-2539, 2013.

[4] Chen J, Zhu Z, Liu Z, Fu C, Zhang L, Yu H., "A novel double-image encryption scheme based on cross-image pixel scrambling in gyrator domains," Opt. Express, vol. 22, pp. 7349-7361, 2014.

[5] Ahmad M. Elshamy, Fathi E. Abd El-Samie, Osama S. Faragallah, Sayed M. Elshamy, Hala S. El-sayed, S. F. El-Zoghdy, Ahmed N. Z. Rashed, Abd El-Naser A. Mohamed, and Ahmad Q. Alhamad, "Optical Image Cryptosystem Using Double Random Phase Encoding and Arnold's Cat Map," Optical and Quantum Electronics, vol. 48(3):212, pp. 1-18, 2016, Springer.

[6] Chen W, Chen X, Sheppard CJR. "Optical color-image encryption and synthesis using coherent diffractive imaging in the Fresnel domain," Opt. Express, vol. 20, pp. 3853-3865, 2012.

[7] P.C. Mogensen and J. Gluckstad, "Phase-only optical encryption," Opt. Lett. 25, 566-568, 2000.

[8] W. Stallings., "Cryptography and Network Security: Principles and Practice," Prentice-Hall, New Jersey, 1999.

[9] A. Menezes, P. van Oorschot and S. Vanstone, "Handbook of Applied Cryptography," CRC Press, New York, 1997.

[10] B. Furht and D. Socek, "A Survey of Multimedia Security," Technical Report, pp. 1-24, August 21, 2003.

[11] S. Tosun and W. C. Feng, "Lightweight Security Mechanisms for Wireless Video Transmission," In Proc. IEEE Int. Conference on Information Technology: Coding and Computing, pp. 157–161, 2001.

[12] Mohamed Amin, Osama S. Faragallah, Ahmed A. Abd El-Latif, "A Chaotic Block Cipher Algorithm for Image Cryptosystems," Communications in Nonlinear Science and Numerical Simulation, vol. 15(1), pp. 3484–3497, 2010.

[13] B. Furht and D. Socek, "Multimedia Security: Encryption Techniques," In IEC Comprehensive Report on Network Security, International Engineering Consortium, Chicago, IL, pp. 335-349, 2004

[14] B. Preneel and M. Csapodi, "Cryptographic Algorithms: Basic Concepts and Applications to Multimedia Security," Appeared in Proceedings of the Design Automation Day on Cellular Computing Architectures for Multimedia and Intelligent Sensors, European Conference on Circuit Theory and Design (ECCTD 1997), 1997.

[15] Heba M. Elhoseny, Hossam E. H. Ahmed, Alaa M. Abbas, Hassan B. Kazemian, Osama S. Faragallah, Sayed M. El-Rabaie, Fathi E. Abd El-Samie, "Chaotic encryption of images in the fractional Fourier transform domain using different modes of operation," Signal, Image and Video Processing Journal, vol. 9(3), pp. 611-622, 2015.

[16] Ensherah A. Naeem, Mustafa M. Abd Elnaby, Naglaa F. Soliman, Alaa M. Abbas, Osama S. Faragallah, Noura Semary, Mohiy M. Hadhoud, Saleh A. Alshibeili, and Fathi E. Abd El-Samie, "Efficient Implementation of Chaotic Image Encryption in Transform Domains," Journal of Systems and Software, vol. 97, pp. 118-127, 2014.

[17] Osama S. Faragallah, "An Efficient Block Encryption Cipher Based on Chaotic Maps for Secure Multimedia Applications," Information Security Journal: A Global Perspective, vol. 20(3), pp. 135-147, 2011.

[18] Osama S. Faragallah, "Digital Image Encryption Based on the RC5 Block Cipher Algorithm," Sensing and Imaging: An International Journal, vol. 12(3), pp. 73-94, 2011, Springer.Shiguo Lian, "Multimedia Content Encryption: Techniques and Applications," Taylor & Francis Group, LLC, 2009.

[19] Ljupco Kocarev, Zbigniew Galias and Shiguo Lian, "Intelligent Computing Based on Chaos," Springer Publisher, 2009.

[20] Shiguo Lian , Jinsheng Sun, Zhiquan Wang, "A chaotic stream cipher and the usage in video encryption," Chaos, Solitons and Fractal, vol. 34, pp. 851-859, 2009.

[21] Ljupco Kocarev, Zbigniew Galias and Shiguo Lian(editors). Intelligent Copmuting based on chaos. Springer publisher, 2009.

[22] Mohamed Amin, Osama S. Faragallah, Ahmed A. Abd El-Latif," Chaos-based hash function (CBHF) for cryptographic applications", Chaos, Solitons & Fractals (2009), doi:10.1016/j.chaos.2009.02.001.

[23] G. Chen, Y. Mao, C.K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps". Chaos, Solitons & Fractals vol. 21(3), pp. 749–61, 2004.

[24] Hossam El-din H. Ahmed, Hamdy M. Kalash, Osama S. Faragallah, "Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Images," Journal of Optical Engineering, vol.45, 2006.

[25] Nawal El-Fishawy, Osama M. Abu Zaid, "Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms," International Journal of Network Security, vol. 5(3), pp. 241-251, Nov. 2007.

[26] C.E. Shannon, "Communication theory of secrecy systems," Bell System Technical Journal, vol. 28, No. 4, pp. 656-715, October 1949.

[27] S. Behnia, A. Akhshani, A.Akhshani, H. Mahmodi, A. Akhavan, "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps". Physics Letters A vol. 36(6), pp. 391-396, 2007.