Selective Hybrid Chaotic-Based Cipher for Real-Time Image Application

Moussa Farajallah
College of Information Technology
and Computer Engineering
Palestine Polytechnic University
Hebron, Palestine
Email: mousa_math@ppu.edu

Rawan Qumsieh
Master of Informatics
Palestine Polytechnic University
Hebron, Palestine
Email: Rawan.iq@gmail.com

Samer Isayed
Master of Informatics
Palestine Polytechnic University
Hebron, Palestine
Email: samers@ppu.edu

***Abstract*—Confusion and diffusion are the two main principles in encryption. Confusion is a process that drastically changes data from the input to the output. In order to make it right, we have to make the relation between the key and cipher-text as complex as possible. On the other hand, diffusion means that changing a single character of the input will change many characters of the output. In other words, we can say that the output bits should depend on the input bits in a very complex way, so if we change one bit in the plain-text, the cipher-text will change completely. Many chaos-based algorithms were implemented with a chaotic map called the Skew Tent Map (STM), which we address and evaluate in this paper. Our proposed hybrid encryption scheme combines both stream and block ciphering algorithms to achieve the required level of security with the minimum encryption time. The proposed chaos-based cryptosystem uses the STM as a substitution based on a lookup table and STM as a generator to change the byte position to achieve the required confusion and diffusion effects. There is no need to have the inverse or the reverse of the generator in our proposed cryptosystem. The robustness of the proposed cryptosystem was proven by the performance and security analysis, as well as the high encryption speed (throughput).**

Keywords–skew tent map; confusion; diffusion; chaos-based cryptosystem.

I. INTRODUCTION

Finding new channels to transmit data over the Internet is easy, but the main problem is how to ensure sending it safely. Cryptography is the way to transform data, so that it is hidden to all except those who are the intended recipients of the data. So, it mainly provides secure ways to exchange personal and secret information between others through the electronic world. Encrypting images in the electronic world is especially important, yet the basic way to encrypt an image is slow in comparison with other fields of encryption. Many researchers are working to find cryptosystems to transmit images in a secure and fast way. On the other hand, the redundancy between bytes of the images is higher than it is in texts, and so we need a strong encryption algorithm to remove this high correlation and all crypto problem resulting from this high redundancy. We chose to work with chaos theory as it has the most powerful and important property required in any cryptosystem that produces random behaviors. Also, chaotic maps can be used as symmetric or asymmetric encryption algorithms [1].

It has been shown by many researchers that chaotic cryptosystems are excessively sensitive to the changes of their control parameters. Furthermore they have a pseudo-random behaviour toward non-authorized parties [2]–[7], and depending on the experimental results in [8]–[12], chaos-based encryption achieved a better security than the classical encryption algorithms [8].

Fridrich introduced the first chaos-based encryption algorithm [13] [14]. In his algorithm, the diffusion effect was achieved by using a non-linear feedback register, while the confusion effect was achieved by using three different 2-D chaotic maps; the standard one, the Backer's and the 2-D cat map.

Masuda et al. [15] [16] considered two different chaotic maps, "key-dependent chaotic s-box and chaotic mixing transformation" [15]. To make their cryptosystem resident to differential and linear cryptanalysis, they estimated bounds for the differential and linear probabilities.

Chaos-based image encryption was proposed in [17], where the authors used two Piece Wise Linear Chaotic Map (PWLCM), the first during implementing the addition modulo 256 in the substitution process, and the second is used in the permutation process (degree of 8). The error propagation, the slow encryption speed were weaknesses in this algorithm.

Finally, a fast and secure cryptosystem was proposed by Zhang et al. [18], which appears to be robust and secure against attacks, and faster than other previously proposed cryptosystems .

Our paper is organized as follows: The directly relevant work is presented in the next section. Then our cryptosystem and the evaluation regarding the complexity of execution and the security is shown in Section 3 and Section 4. Finally, the conclusion is given in Section 5.

II. RELATED WORK

For real-time image encryption, being fast and secure is the most important thing to many scientists in the cryptanalysis field.

A. Fridrich Model

Fridrich proposed in 1997 a chaos-based encryption scheme [13]. This model of Fridrich became the core structure of most all chaos-based cryptosystems.

The Fridrich model as shown in Figure 1 is composed of two layers; the first layer is the confusion layer which uses the 2D Baker chaotic map to calculate the new positions of

Copyright (c) IARIA, 2016. ISBN: 978-1-61208-493-0

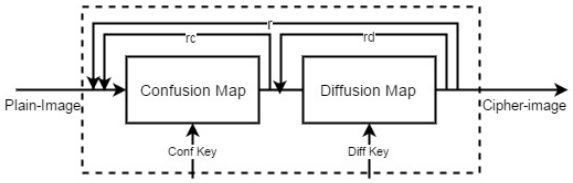


Figure 1. Fridrich image encryption architecture

each byte using(1)&(2), and the diffusion layer which is used to spread a single byte effect to the other bytes in the same block.

$$B(x,y) = (2x, \frac{y}{2}) \quad when\ 0 \le x < \frac{1}{2} \tag{1}$$

$$B(x,y) = (2x-1, \frac{y}{2} + \frac{1}{2}) \quad when\ \frac{1}{2} \le x \le 1 \tag{2}$$

After calculating the new position of the byte, the x_1 position will be occupied with the value of the first shuffled position, while the second shuffled value will be in x_2, and so on. Solak [19] broke Fridrich's algorithm using a chosen cipher-text attack, as he revealed some secret permutation from the algorithm.

B. Masuda Model

Masuda et. al. in [15], introduced a cryptosystem which uses the Finite State Tent Map (FSTM), which encrypts as shown by (3), and decrypts as shown by (4).

$$F_A(X) = \begin{cases} \lceil \frac{256}{A} \times X \rceil + 1 & 1 \le X < A \\ 256 & X = A \\ \lfloor \frac{256 \times (256-X)}{256-A} \rfloor & A < X \le 256 \end{cases} \tag{3}$$

$$F_A{}^{-1}(X) = \begin{cases} X_1 & X_1 \times (256-A) > A \times (256-X_2) \\ X_2 & X_1 \times (256-A) \le A \times (256-X_2) \end{cases} \tag{4}$$

where

$$X_1 = \left\lfloor \frac{A \times Y}{256} \right\rfloor \tag{5}$$

and

$$X_2 = 256 - \left\lfloor (1 - \frac{A}{256}) \times Y \right\rfloor \tag{6}$$

III. The Proposed Cryptosystem

Our proposed cryptosystem is based on a hybrid encryption scheme that combines both stream and block ciphering algorithms to achieve the required security level, with a minimum encryption time. Both stream and block ciphers in cryptography belong to the family of symmetric key ciphers in which we use the same key for both of the encryption and the decryption processes.

The stream cipher converts the plain-text bits directly into the cipher-text by XORing them with pseudo-random cipher bits, while block cipher encrypts fixed size blocks that contain a group of bits from the plain-text. Block encryption is more susceptible to cryptanalysis attacks than stream cipher because identical blocks of plain-text yield identical blocks of cipher-text [20]. The stream cipher has a higher speed of transformation and a low error rate, as an error that occurs in one bit will not affect the other bit. The block cipher has a high level of diffusion which any block effect will be spread into several blocks. On the other hand, the diffusion effect is low in the stream cipher, as all information of the plain-text is contained in a single cipher-text symbol. The block cipher has low encryption speed, as the entire block must be accumulated before the encryption or decryption process starts. Furthermore, the entire block here may corrupt due to an error in one bit.

A. Encryption Algorithm

Dividing the image into several numbers of blocks and encrypting block by block minimizes the error bits, so we divided our plain-text in the proposed algorithm into blocks with a predefined size of 256 bytes each (to use (3) in the permutation process as it does not map any block larger than 256 bytes). Our proposed algorithm encrypts the whole image using E_1 and E_2, where E_1 encrypts the odd blocks based on the FSTM proposed by Masuda et al. [15] as shown in Figure 1, while the diffusion and confusion effects are transferred between blocks using the Cipher-Block chaining mode (CBC) [21]. Equations (3) and (4) are implemented based on a look-up table to decrease the encryption time. The input of this look-up table will be the generated dynamic key from the implemented version of the used chaotic generator (see Section III-A) in addition to the byte from the plain-text as to be permuted or substituted.

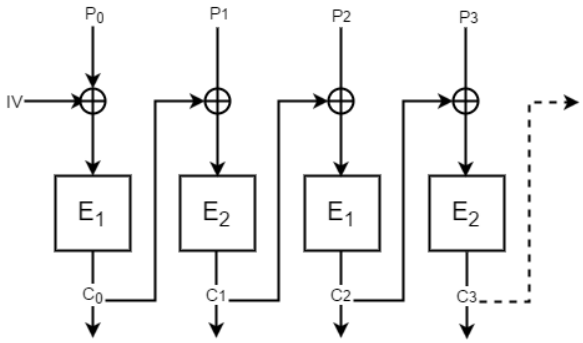


Figure 2. The proposed algorithm encryption process based on CBC mode

P_0 in Figure 2 represents the first plain block (B_0), while IV is the initial vector that is generated by the chaotic generator. C_0 is the resulting ciphered block that will be sent to the recipient side. E_1 is the proposed encryption algorithm which produces the confusion and diffusion based on slightly different look-up tables (LookupS to simulate (3) and (4) for substitution map, and LookupG to simulate (3) with small changes for the permutation map without needing the inverse map). Note that each map has different independent dynamic keys generated using the implemented chaotic generator:

- Substitution: our algorithm uses $C_{0,i} = LookupS(B_{0,i}, k_1)$ to encrypt the selected blocks from the plain image where $B_0 = B_{0,0}, B_{0,1}, B_{0,2}...B_{0,255}$ represents the first block pixels and $0 \le i \le 255$. While the decryption process of the ciphered block using the inverse look-up table as: $B_{0,i} = lookupS^{-1}(C_{o,i}, k_1)$.

Copyright (c) IARIA, 2016. ISBN: 978-1-61208-493-0

- Permutation: it uses $C_{0,x} = lookupG(C_{0,i}, k_2)$ to change the ciphered byte position in the block during the encryption process and uses the same table in the decryption side. The generated pre-defined look-up table for the permutation map based on (3) with a small modification of the first part by converting the ceil operation into floor one to be used as the generator.

The second block (and all even blocks) will be encrypted in our algorithm based on a Selective Stream Cipher Algorithm (SSCA). The SSCA is proposed to speed up the encryption process and increase the throughput of the encryption under the required security level. The selected encrypted bit of each pixel (MSB) is chosen as its contribution from the total information in the pixel is 2^7 which means that it has an effect equivalent to the remaining bits in the pixel. This MSB is XORed with the generated key bits from the used chaotic generator which gives 32-bits for each sample. Dividing the block size (256 bytes) by the sequence length (32 bits) will give us 2^3 calls to the chaotic generator while encrypting each block, which means that we XOR the MSB without reusing any key bit.

B. Chaotic generator

In the proposed cryptosystem, we implemented the chaotic generator proposed by El Assad et, al. [22] to avoid the weakness in the chaotic systems regarding periodicity generating sequences. It consists of two chaotic maps, i.e., the Skew Tent Map (STM) and the discrete Piece-Wise Linear Chaotic Map (PWLCM), in which are connected in parallel to generate the sequence values of 32-bit samples.

IV. Security and complexity analysis

A cryptosystem should be suitable and efficient for the target application, and it should offer the required security level. Analyzing the complexity of any cryptosystem is an important assessment factor, and researchers typically take this evaluation as the time of encryption/decryption. In this section we are using a more comprehensive measure to evaluate our proposed cryptosystem. The known theoretical attacks and the common statistical attacks are explained as well in this section.

A. Complexity analysis

The complexity of the algorithm used in the encryption method is an important factor which determines the time of performance. On the other hand, the performance can be determined by the running speed of the algorithm or the Encryption Throughput (ET) which can be calculated using (7), and the number of cycles needed to encrypt one byte, which is the CPU speed in Hertz divided by the ET in bytes as given in (8). The results for the encryption and decryption processes of our proposed cryptosystem are carried out using the Code::Blocks compiler of C programming on a PC with 2.30 GHz processor Intel $Core^{TM}$ i5-4200U CPU, 6GB RAM, and Windows 7, 64-bit operation system. Lena image (colored with the size of $512 \times 512 \times 3$ byte) is the image under test. The calculated time for the proposed cryptosystem is compared to the fastest chaos-based cryptosystems in the literature. To calculate the time, we calculated the average executions for the test images which are encrypted for 1000 different secret keys as shown in Table 1 for different image sizes 256, 512, and 1024, while Table 2 presents the running speed of the algorithm (throughput) in mega byte per second (MBps) and the number of cycles required to encrypt or decrypt one byte. Through those calculations, the number of encryption rounds is identified by the required security level.

$$ET = \frac{Image_{size}(Byte)}{Encryption_{time}(Second)} \quad (7)$$

$$Numberofcyclesperbyte = \frac{CPUSpeed_{(Hertz)}}{ET_{(Byte)}} \quad (8)$$

TABLE I. ENCRYPTION/DECRYPTION TIME OF DIFFERENT ALGORITHMS IN MILLISECOND

	Lena 256	Lena 512	Lena 1024
Proposed	1.385/1.315	4.965/5.009	18.845/19.256
Fouda [23]	3.98/4.19	15.58/16.77	62.32/67.08
Zhang 1 [18]	7.5/7.5	30/30	120/120
Zhang 2 [18]	7.5/8.25	30/33	120/132
Wang [24]	7.79/8.39	31.16/33.54	124.64/134.16
Akhshani [2]	14.4	57.6	230.4
Wong [25]	15.59/16.77	62.37/67.11	249.48/268.44
Kanso [26]	97.15	388	1554
Pareek [27]	160	920	5650
Farajallah [28]	6/5.8	24/23.2	96/92.8

As presented in Tables 1 and 2, our proposed cryptosystem is faster than other chaos-based cryptosystems, it is four times faster than the algorithms in [24] [18] and two times faster than [29]. As mentioned before, the cryptosystem had to achieve a high security level besides the encryption speed, so the speed isn't a sufficient assessment factor.

TABLE II. ENCRYPTION THROUGHPUT AND THE NUMBER OF CYCLES FOR EACH ENCRYPTED BYTE

	ET in MBps	Number of cycles per byte
Proposed	151.03	14.52
Fouda [23]	48.138/44.72	39.62/42.65
Zhang 1 [18]	25/25	122.07/122.07
Zhang 2 [18]	25/22.72	122.07/134.27
Wang [24]	24.06/22.35	122.85/132.24
Akhshani [2]	13.02	194.83
Wong [25]	12.03/11.18	245.7/26438
Kanso [26]	1.93	1121
Pareek [27]	0.39	2445
Farajallah [28]	31.25	94.60

B. Key space

Resisting brute force attack requires a large secret key, with at least 128 effective and independent bits. Depending on that fact, our proposed cryptosystem has a secret key with 169 bits. Moreover, the dynamic keys are changed for each new plain block for the substitution as well as the permutation in E_1. In E_2 all used dynamic bits are distinct and changeable for each new block.

C. Plain-text sensitivity attack

Depending on the diffusion definition, any change of a single bit of the plain-text, should statistically, change one bit out of two of the cipher-text, and similarly, if we change one bit of the cipher-text, then approximately one half of the plain-text bits should change.

In our proposed cryptosystem, two plain-text P_1 and P_2 were selected to be encrypted using the same secret key and have a difference in one bit in the first block. Most probably, the researchers chose the first bit in the image to be the different one, while in our scenario the chosen bit will be located in the beginning, in the middle, and at the end of the first block so as to get closer to the real application. The Unified Average Changing Intensity (UACI), which is calculated in (9) and the Number of Pixels Change Rate (NPCR) calculated using (10) are the two parameters used to measure any proposed cryptosystem's resistance to the plain-text sensitivity attack.

$$UACI = \frac{1}{L \times C \times P \times 255} \times \sum_{p=1}^{P} \sum_{i=1}^{L} \sum_{j=1}^{C} |C_1 - C_2| \times 100\% \quad (9)$$

$$NPCR = \frac{1}{L \times C \times P} \times \sum_{p=1}^{P} \sum_{i=1}^{L} \sum_{j=1}^{C} D(i,j,p) \times 100\% \quad (10)$$

where D(i,j,p) = 0 when it's the same value in C_1 and C_2 while it is 1 when it's different. And L is the height, C is the width and P is the depth of the image. Table 3 presents the results of the plain-text sensitivity attacks of our proposed cryptosystem, where the optimal value for UACI is 33.46% and for NPCR is 99.61% which are given in [30] [31].

TABLE III. THE UACI AND THE NPCR PLAIN-TEXT SENSITIVITY TESTS FOR THE PROPOSED CRYPTOSYSTEM

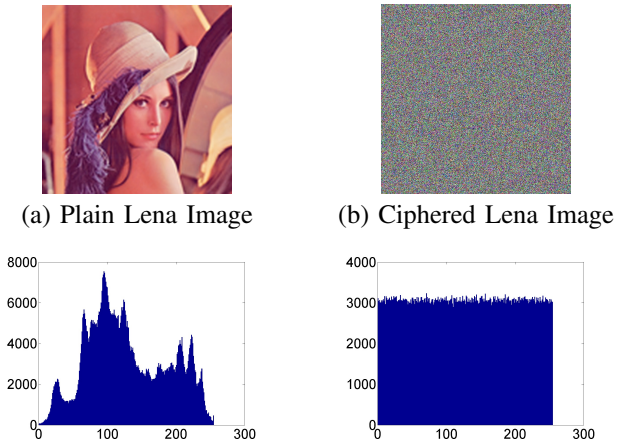
Image	UACI	NPCR
Lena 512	33.463968	99.605423
Baboon 512	33.462189	99.607487
Boat 512	33.462248	99.606874

D. Key sensitivity attack

Any slight change in the secret key will produce a completely different ciphered image [32], which means that any cryptosystem has to be resistant to this sensitivity attack. However, changing one bit in the key during decryption of the ciphered image will completely destroy the decryption process (it will completely fail). The testing scenario of the key sensitivity is similar to the plain-text sensitivity attacks: we have one plain-text P and two secret keys with a difference of one bit. First, P is encrypted using K_1 to obtain C_1. Then the same plain-text P is encrypted using K_2 to obtain C_2. Finally, previously mentioned equations for NPCR and UACI (9 and 10) are used to evaluate the key sensitivity attacks of the proposed cryptosystem. As shown in Table 4 which presents the average results of the key sensitivity attacks, our proposed cryptosystem results indicate that the proposed cryptosystem is very sensitive to one bit change in the secret key.

E. Histogram analysis

The graph which shows the number of pixels in an image at each different intensity value is called the histogram. For the encrypted image, it should be uniformly distributed as shown in Figure 3 to be strong against the statistical attacks, in which we can benefit from the most used bit in the image and its position. To ensure that the ciphered image pixels are



(a) Plain Lena Image (b) Ciphered Lena Image

(c) Histogram-plain image (d) Histogram-ciphered image

Figure 3. LENA IMAGE PLAIN AND CIPHERED WITH THEIR HISTOGRAM

TABLE IV. THE UACI AND THE NPCR KEY SENSITIVITY TESTS FOR THE PROPOSED CRYPTOSYSTEM

Image	UACI	NPCR
Lena 512	33.171848	99.609385
Baboon 512	33.343602	99.608161
Boat 512	32.531726	99.608082

uniformly distributed, we applied the chi-square test on the image histogram using (11).

$$\chi^2_{exp} = \sum_{i=0}^{Q-1} \frac{(o_i - e_i)}{e_i} \quad (11)$$

where Q is the number of levels (in this crypto is 256), o_i is the observed occurrence frequencies for each level in the ciphered image, while e_i is the expected one from the uniform distribution. Here $e_i = \frac{L \times C \times P}{256}$.

The obtained value of this test is close to 250, which meets the condition $\chi^2_{exp} < \chi^2_{th}(255, 0.05) = 293$. This result shows that the tested histograms are uniform and do not reveal any useful information for the statistical analysis.

F. Correlation analysis

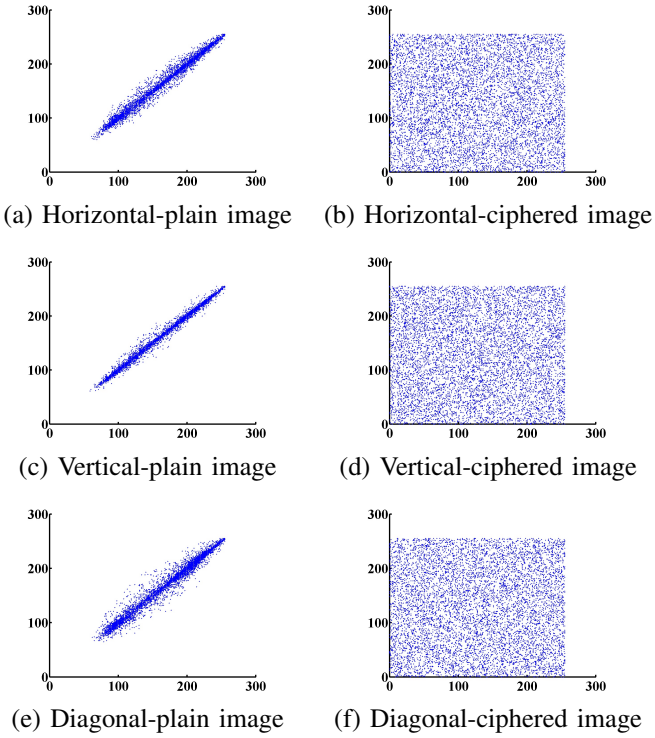
The pixels in the encrypted image should have as low redundancy and correlation values as possible, even though the adjacent pixels in the plain images are very redundant and correlated.

To determine the correlation in encrypted images, we calculate the correlation coefficient (r_{xy}) as in (12) between two horizontally, vertically and diagonally neighboring pixels [33] for 10000 randomly pairs (N).

$$r_{x,y} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (12)$$

where $cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}([x_i - E(x)]\,[y_i - E(y)])$, $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x - i - E(x))^2$, $E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i)$ and x,y are the pixel values of the two adjacent pixels in the tested image. Figure 4 shows the correlation results for the Lena

Copyright (c) IARIA, 2016. ISBN: 978-1-61208-493-0



(a) Horizontal-plain image (b) Horizontal-ciphered image

(c) Vertical-plain image (d) Vertical-ciphered image

(e) Diagonal-plain image (f) Diagonal-ciphered image

Figure 4. Correlation analysis of the plain and ciphered Lena image. Plain-Image Correlation Values: Horizontal Correlation=0.993077; Vertical Correlation=0.996988; Diagonal Correlation=0.988087. Cipher Correlation Values: Horizontal Correlation=0.009019; Vertical Correlation=0.008971; Diagonal Correlation=0.010765.

image and its corresponding cipher image, which is encrypted by our proposed cryptosystem.

V. Conclusion and Future Work

In this paper, we proposed a hybrid encryption scheme that has both block and stream cipher algorithms. This combination achieved a faster cryptosystem than the existing ones, in addition to preserving the required security level. The proposed chaos-based encryption method is a hybrid of block and stream ciphers. The block cipher uses odd plain text blocks which are implemented by a substitution layer from the FSTM and a permutation layer that is achieved by using the (FSTM) as a generator. The stream cipher level is applied by a selective cryptosystem to encrypt the MSB of each byte in the even plain text blocks. Our modified version of the STM used a novel method designed with a confusion and a diffusion layer in order to be simple, fast and robust against known attacks. Our proposed cryptosystem is the fastest of all chaos-based cryptosystems known to us, which was proved in the section on the security and complexity analysis. The selective encryption of the MSB bit requires improvement in future work in order to increase the security level while constantly increasing the encryption time.

References

[1] R. Tenny and L. S. Tsimring, "Additive mixing modulation for public key encryption based on distributed dynamics," Circuits and Systems I: Regular Papers, IEEE Transactions on, vol. 52, no. 3, 2005, pp. 672–679.

[2] A. Akhshani, A. Akhavan, S.-C. Lim, and Z. Hassan, "An image encryption scheme based on quantum logistic map," Communications in Nonlinear Science and Numerical Simulation, vol. 17, no. 12, 2012, pp. 4653–4661.

[3] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," Chaos, Solitons & Fractals, vol. 35, no. 2, 2008, pp. 408–419.

[4] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," Chaos, Solitons & Fractals, vol. 21, no. 3, 2004, pp. 749–761.

[5] F. Chiaraluce, L. Ciccarelli, E. Gambi, P. Pierleoni, and M. Reginelli, "A new chaotic algorithm for video encryption," IEEE Transactions on Consumer Electronics, vol. 48, no. 4, 2002, pp. 838–844.

[6] M. Farajallah, S. El Assad, and M. Chetto, "Dynamic adjustment of the chaos-based security in real-time energy harvesting sensors," in Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing. IEEE, 2013, pp. 282–289.

[7] F. Salam, J. E. Marsden, and P. P. Varaiya, "Chaos and arnold diffusion in dynamical systems," Circuits and Systems, IEEE Transactions on, vol. 30, no. 9, 1983, pp. 697–708.

[8] A. A. A. El-Latif, X. Niu, and M. Amin, "A new image cipher in time and frequency domains," Optics Communications, vol. 285, no. 21, 2012, pp. 4241–4251.

[9] B. Bhargava, C. Shi, and S.-Y. Wang, "Mpeg video encryption algorithms," Multimedia Tools and Applications, vol. 24, no. 1, 2004, pp. 57–79.

[10] J.-I. Guo et al., "A new chaotic key-based design for image encryption and decryption," in Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on, vol. 4. IEEE, 2000, pp. 49–52.

[11] S. Li, G. Chen, and X. Zheng, "Chaos-based encryption for digital image and video," Multimedia Encryption and Authentication Techniques and Applications, 2006, p. 129.

[12] I. Mansour, G. Chalhoub, and B. Bakhache, "Evaluation of a fast symmetric cryptographic algorithm based on the chaos theory for wireless sensor networks," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012, pp. 913–919.

[13] J. Fridrich, "Image encryption based on chaotic maps," in Systems, Man, and Cybernetics, 1997. Computational Cybernetics and Simulation., 1997 IEEE International Conference on, vol. 2. IEEE, 1997, pp. 1105–1110.

[14] ——, "Symmetric ciphers based on two-dimensional chaotic maps," International Journal of Bifurcation and chaos, vol. 8, no. 06, 1998, pp. 1259–1284.

[15] N. Masuda, G. Jakimoski, K. Aihara, and L. Kocarev, "Chaotic block ciphers: from theory to practical algorithms," Circuits and Systems I: Regular Papers, IEEE Transactions on, vol. 53, no. 6, 2006, pp. 1341–1352.

[16] N. Masuda and K. Aihara, "Cryptosystems with discretized chaotic maps," Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on, vol. 49, no. 1, 2002, pp. 28–40.

[17] D. Socek, S. Li, S. S. Magliveras, and B. Furht, "Short paper: Enhanced 1-d chaotic key-based algorithm for image encryption," in Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on. IEEE, 2005, pp. 406–407.

[18] W. Zhang, K.-w. Wong, H. Yu, and Z.-l. Zhu, "An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion," Communications in Nonlinear Science and Numerical Simulation, vol. 18, no. 8, 2013, pp. 2066–2080.

[19] E. Solak, C. Çokal, O. T. Yildiz, and T. Biyikoğlu, "Cryptanalysis of fridrich's chaotic image encryption," International Journal of Bifurcation and Chaos, vol. 20, no. 05, 2010, pp. 1405–1413.

[20] S. William, "Cryptography and network security: principles and practice," Prentice-Hall, Inc, 1999, pp. 62–90.

[21] W. F. Ehrsam, C. H. Meyer, J. L. Smith, and W. L. Tuchman, "Message

Copyright (c) IARIA, 2016. ISBN: 978-1-61208-493-0

verification and transmission error detection by block chaining," Feb. 14 1978, uS Patent 4,074,066.

[22] S. El Assad and H. Noura, "Generator of chaotic sequences and corresponding generating system," 2011, uS Patent 8,781,116 B2.

[23] J. A. E. Fouda, J. Y. Effa, and M. Ali, "Highly secured chaotic block cipher for fast image encryption," Applied Soft Computing, vol. 25, 2014, pp. 435–444.

[24] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," Applied soft computing, vol. 11, no. 1, 2011, pp. 514–522.

[25] K.-W. Wong, B. S.-H. Kwok, and W.-S. Law, "A fast image encryption scheme based on chaotic standard map," Physics Letters A, vol. 372, no. 15, 2008, pp. 2645–2652.

[26] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3d chaotic map," Communications in Nonlinear Science and Numerical Simulation, vol. 17, no. 7, 2012, pp. 2943–2959.

[27] N. Pareek, V. Patidar, and K. Sud, "Cryptography using multiple one-dimensional chaotic maps," Communications in Nonlinear Science and Numerical Simulation, vol. 10, no. 7, 2005, pp. 715–723.

[28] M. Farajallah, Z. Fawaz, S. El Assad, and O. Déforges, "Efficient image encryption and authentication scheme based on chaotic sequences," in The 7th International Conference on Emerging Security Information, Systems and Technologies, 2013, pp. 150–155.

[29] H. E.-d. H. Ahmed, H. M. Kalash, and O. F. Allah, "Encryption efficiency analysis and security evaluation of rc6 block cipher for digital images," in Electrical Engineering, 2007. ICEE'07. International Conference on. IEEE, 2007, pp. 1–7.

[30] Y. Wu, J. P. Noonan, and S. Agaian, "Npcr and uaci randomness tests for image encryption," Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT), 2011, pp. 31–38.

[31] F. Maleki, A. Mohades, S. M. Hashemi, and M. E. Shiri, "An image encryption system by cellular automata with memory," in Availability, Reliability and Security, 2008. ARES 08. Third International Conference on. IEEE, 2008, pp. 1266–1271.

[32] J.-R. Ohm, G. J. Sullivan, H. Schwarz, T. K. Tan, and T. Wiegand, "Comparison of the coding efficiency of video coding standardsincluding high efficiency video coding (hevc)," Circuits and Systems for Video Technology, IEEE Transactions on, vol. 22, no. 12, 2012, pp. 1669–1684.

[33] R. Munir, "Security analysis of selective image encryption algorithm based on chaos and cbc-like mode," in Telecommunication Systems, Services, and Applications (TSSA), 2012 7th International Conference on. IEEE, 2012, pp. 142–146.

Copyright (c) IARIA, 2016. ISBN: 978-1-61208-493-0