A New Approach of Image Encryption Using 3D Chaotic Map to Enhance Security of Multimedia Component

Md.Billal Hossain[1], Md.Toufikur Rahman[2], A B M Saadmaan Rahman[3], Sayeed Islam[4]
[1, 3, 4]# Electronics and Communication Engineering Department, MIU, Dhaka-1216, Bangladesh.
[2]# Electronics and Communication Engineering Department, KUET, Khulna-9203, Bangladesh.
[1]billal.0709018@gmail.com, [2]toufik0709023@gmail.com, [3]saadmaan.mist@gmail.com, [4]sayeed_nsu@live.com

Abstract—**Multimedia data contains text, audio, video, graphic, images and with the increasing use of multimedia data over internet, here comes a demand of secure multimedia data. Image encryption differs from other multimedia components encryption due to some intrinsic features, such as bulk data capacity and high correlation among pixels the earlier encryption techniques such as AES, DES etc. are not suitable for practical applications. The combination of chaotic theory and cryptography forms an important field of information security. The latest trend in image encryption is chaos based for some unique characteristics such as the sensitivity to initial conditions, non-periodicity, non-convergence, and control parameters. There are a lot of image encryption algorithms based on chaotic maps have been proposed some of them are time consuming and complex some have little key space. In this paper we proposed a non-linier 3D chaos based simple encryption technique where for the first time 3D chaos is used for position permutation and value transformation technique. We get average entropy of encrypted image 7.99, NPCR of 99.6% and UACI of 33.5%. We tabulate correlation coefficient value both horizontal and vertical position for cipher and original image and compare performance of our method with some existing methods. We also discuss about different types of attack, key sensitivity, and key space of our proposed approach.**

Keywords- Information security, image encryption, chaotic maps, logistic map, information entropy.

I. INTRODUCTION

The tremendous spreading out of the communication networks has evoked increased dependency on digitized information in our society. As a result information is more vulnerable to abuse now. Today the web is going towards multimedia data due to the development of network and multimedia technology. Multimedia data consist of image, audio, video, text, etc. The digital images become one of the most important information carriers which are helpful for biometric authentication, medical science, military, online personal photograph album, etc. [1]. Image encryption is different from text encryption [7]. Conventional cipher algorithms such as DES, IDEA, AES, 3DES etc. are not suitable for multimedia files due to public data capacity, strong pixel correlation and high redundancy which reduces the encryption performance [2]-[6].

Chaos theory was firstly used in the computer system by Edward Lorenz 1963. During the last decade chaos based cryptography has received considerable attention due to noise-like signal for unauthorized person, ergodicity, mixing and sensitivity to initial conditions, can be connected with those of good ciphers, such as confusion and diffusion [7][8]. In the research of information security and a lot of image encryption algorithms based on chaotic systems have been proposed [2]-[33]. There have been many image encryption algorithms based on chaotic maps like the Logistic map [12]-[16]. Higher dimension chaos functions are far more secure from cryptanalytic attacks [19].

There are two types of image encryption process called position permutation and value transformation. In position permutation technique, permute image position without changing pixel value of original image and in value transformation technique pixel value replaced by another pixel value without changing position. XOR operation is one of the most used value transformation technique which is used to create linier independency between two or more variable. The idea behind XOR Encryption is that it is impossible to reverse the operation without knowing the initial value of one of the two arguments. In order to improve the security performance of the image encryption algorithm, the concept of shuffling the positions of pixels in the plain-image and then changing the gray values of the shuffled image pixels is used.

In this work we proposed hybrid encryption technique by using pixel rotation and XOR based encryption technique using 3D chaos for secure and enhance multimedia communication. The Simulation Result presents performance of our method against different types of attack.

The rest of the paper is organized as follows. The proposed hybrid image encryption strategy is described in Section II. Section III includes the simulation result and security analysis. The comparison with some existing algorithm and discussion on our method is presented in Section IV. Section V concludes the paper.

II. HYBRID ENCRYPTION STRATEGY

There are five stages to complete the overall encryption process. They are:

a) 3D Chaos generation.

978-1-4799-5180-2/14/$31.00 ©2014 IEEE

b) Chaos Histogram Equalization.

c) Row Rotation.

d) Column Rotation.

e) XOR operation.

Figure 1 represents the overall encryption process where x (0), y (0), z (0), a, b, c, N1, N2, N3, N4, N5, N6 are the key. All stage operation described gradually in bellow.

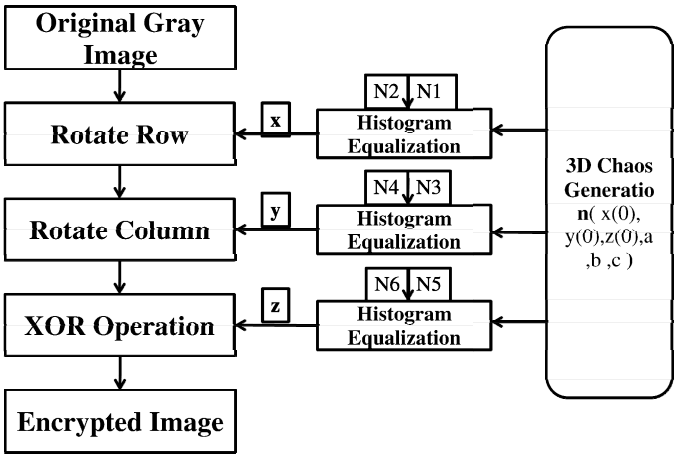

Figure 1. Hybrid Encryption Technique Using 3D Chaos.

A. 3D Chaos Generation

The logistic map is the simplest process of chaos generation given by an equation

$$x_{n+1} = \mu x_n(1 - x_n) \quad (1)$$

For $0< x_n <1$ and $\mu = 4$ is the condition to make this equation chaotic. Hongjuan Liu. et al proposed the 2D logistic map by using quadratic coupling for enhanced security [20] and its extended 3D version are proposed in [16] given by the following formula:

$$x_{n+1} = \gamma x_n(1 - x_n) + \beta y_n^2 x_n + \alpha z_n^3 \quad (2)$$

$$y_{n+1} = \gamma y_n(1 - y_n) + \beta z_n^2 y_n + \alpha x_n^3 \quad (3)$$

$$z_{n+1} = \gamma z_n(1 - z_n) + \beta x_n^2 z_n + \alpha y_n^2 \quad (4)$$

Here the above equations exhibit the chaotic behavior for $3.53<\gamma<3.81$, $0<\beta<0.022$, $0<\alpha<0.015$ and the initial value of x, y, z any value in-between 0 and 1. Presence of cubic, quadratic coupling and 3 constant terms make the 3D logistic map even more complicated and secure. Fig. 2 (a), (b), (c) shows the generated chaos sequences using the equation 2, 3, 4 and initial value of x(1)=0.2350; y(1)=0.3500; z(1)=0.7350; α=0.0125; β=0.0157; γ=3.7700.

B. Chaos Histogram Equalization

In Fig. 2 (d), (e) and (f) it is clear that histogram of x, y and z has non-uniform distribution. For higher security we need to equalize histogram. If a gray image with M×N dimension where M is the number of row and N is the number of column then equalizes histogram by following formula:

$$x = \big(integer(x \times N2)\big) mod\ N \quad (5)$$

$$y = \big(integer(y \times N4)\big) mod\ M \quad (6)$$

$$z = \big(integer(z \times N6)\big) mod\ 256 \quad (7)$$

Where,

N2, N4, N6 are a large random number generally greater than 10000. For the simplicity we also can consider N2, N4 and N6 are equal. Fig. 2 (g), (h) and (i) shows the equalized histogram by using N2=N4=N6= 100000, M=256, N=256.

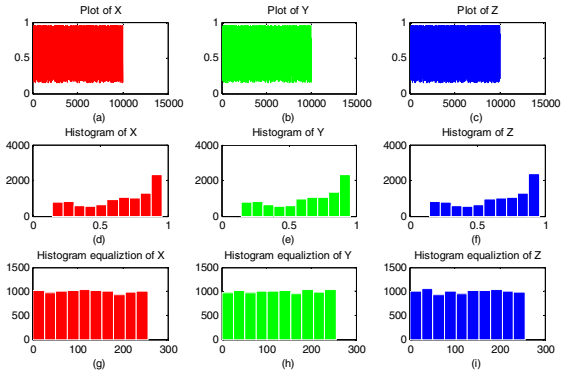

Figure 2. Histogram Equalization of 3D Chaos.

C. Row Rotation

For the purpose of image pixel permutation we introduce new approach rotation of row column. This rotation is same as like as a combination lock of a briefcase. For the rotation of row of a gray image have a dimension of M×N we need to select M number of chaos sequence. At first we generate a large random number N1 then select M number of chaos starting from index N1 and rotate row according to the value of chaos 'x' from Eq. 5. For enhance security we rotate left when the chaos is even and rotate right if the chaos value is odd.

D. Column Rotation

Column rotation is same as like as row rotation. For the rotation of row of a gray image have a dimension of M×N we need to select N number of chaos sequence. At first we generate a large random number N3 then select N number of chaos starting from index N3 and rotate row according to the value of chaos 'y' from Eq. 6.. For enhance security we rotate up when the chaos is even and rotate down if the chaos value is odd. After the rotation of row column the image becomes encrypted but the problem is unchanged histogram which can cause histogram attack. To protest this attack we need another step that changes the image pixel value.

E. XOR operation

The last step of this encryption process is XOR operation. XOR operation change the pixel value into new value and can't reverse without knowing chaos key. At first we generate a large random number N5 and convert M×N image into 1×MN image. After that we XOR the chaos (starting from index N5) and row-column shifted image and finally we get encrypted image.

978-1-4799-5180-2/14/$31.00 ©2014 IEEE

III. SIMULATION RESULT AND SECURITY ANALYSIS

For simulation purpose we use Lena, Peppers, Deblur and Mandrill image with a size 256 x 256 are used in our experimental. Due to the page limit, we highlight some of picture.

A. The Encryption Example

In order to confirm the algorithm's validity, the experiment has been taken. Set an image of size 256× 256 and the initial keys are:

x(1)=0.2350; y(1)=0.3500; z(1)=0.7350; α=0.0125; β=0.0157; γ=3.7700, N2=N4=N6=100000, N1=5000, N3=6000, N4=7000.

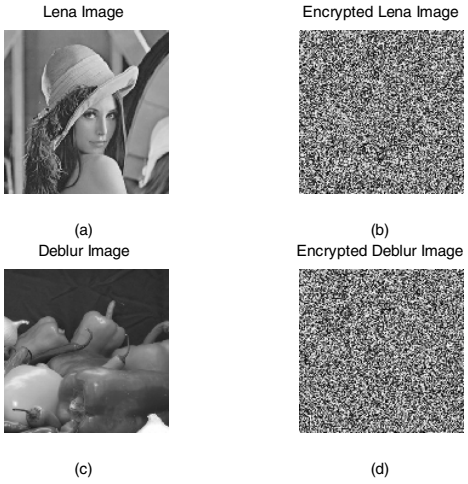

Figure 3. Encryption for Lena and Deblur image.

In Fig.3 shows the encryption example. Among them (a) Original Lena image, (b) Encrypted Lena image, (c) Original Deblur image and (d) Encrypted Deblur image. From the figure we can see that pixels are diffused properly and completely different from original image.

B. Statistical Analysis

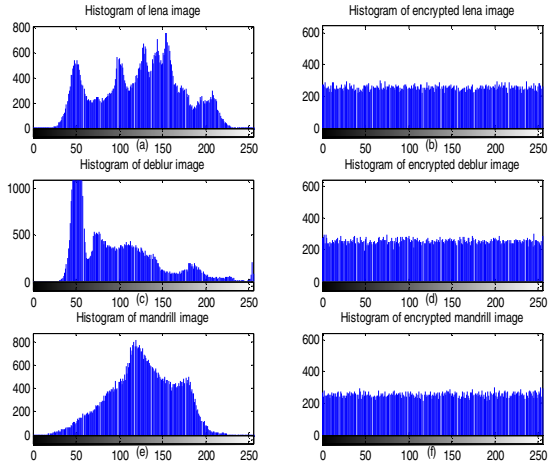

Figure 4. Histogram of original and Encrypted Lena, Deblur and Mandrill image.

Due to high correlation value between adjacent pixels statistical attacks are so serious for image encryption. Statistical analysis perform to demonstrates it's superior confuse and diffuse properties which strongly resist statistical attacks. In Fig. 4, it shows the histogram of original image and encrypted image. Among them Fig. 4(a) shows the histogram of original Lena image 4(b) shows the histogram of encrypted Lena image 4(c) and 4(d) for Deblur image and 4(e) and 4(f) for Mandrill image. From the Encrypted image histogram we can see that the entire pixel values are uniformly distributed which doesn't contain any information to the intruder.

C. Key Sensitivity Analysis

A Secure image encryption algorithm should be sensitive to the small change in decryption key even in single change of key. A good encryption algorithm should have highly sensitive to the key. For test sensitivity we encrypt Lena image with key1 (K1) and decrypted with slightly changed key (K2) and plotting their histogram which is shown in Fig. 5. Table-I represent the key we used for key sensitivity analysis.

TABLE I. LIST OF KEY USED FOR KEY SENSITIVITY ANALYSIS

Key1	**Key2**
x(1)=0.2350 y(1)=0.3500 z(1)=0.7350 α=0.0125 β=0.0157 γ=3.7700 N2=N4=N6=100000 N1=5000 N3=6000 N4=7000	x(1)=0.2350+1×10^{-17} y(1)=0.3500 z(1)=0.7350 α=0.0125 β=0.0157 γ=3.7700 N2=N4=N6=100000 N1=5000 N3=6000 N4=7000

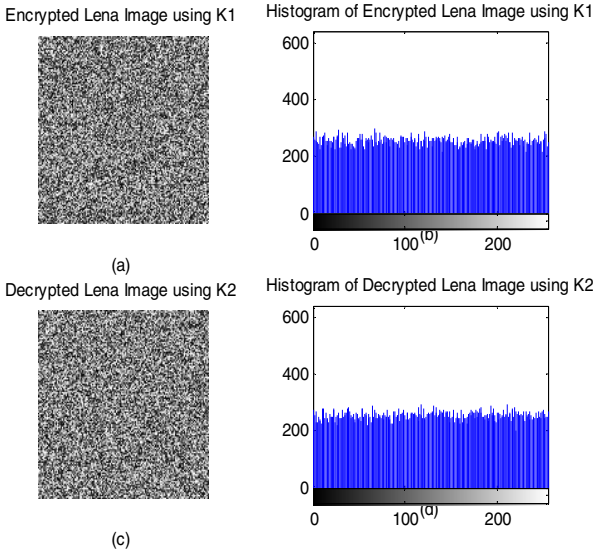

Figure 5. Key sensitivity of proposed algorithm.

D. Information and Entropy Analysis

The entropy H of a symbol source S can be calculated by following equation [21].

$$H(S) = -\sum_{i=0}^{N-1} P(S_i)\log_2 P(S_i) \quad (8)$$

Where $P(S_i)$ represents the probability of symbol S_i and the entropy is expressed in bits. If the source S emits 2^8 symbols with equal probability, i.e. $S = \{s1, s2. \ . \ . \ s256\}$, then the result of entropy is $H(S) = 8$, which corresponds to a true random source and represents the ideal value of entropy for message source S. The more the distribution of gray value is uniform, the greater the information entropy. If the information entropy of an encrypted image is significantly less than the ideal value 8, then, there would be a possibility of predictability which threatens the image security. However, the values of information entropy obtained for the case of images encrypted by the proposed algorithm are very close to the ideal value 8, the entropy values of the encrypted images are listed in Table II.

TABLE II. INRORMATION ENTROPY OF ENCRYPTED IMAGES FOR VARIOUS TEST IMAGE

Entropy Analysis of Image							
Lena		**Peppers**		**Mandrill**		**Deblur**	
Plain Image	Cipher Image	Plain Image	Cipher Image	Plain Image	Cipher Image	Plain Image	Cipher Image
7.4467	7.9890	7.5553	7.9896	7.2636	7.9895	7.0207	7.9887

E. Plain -text Sensitivity Analysis

If the cipher image is not sensitive in the changing of the plaintext then the cryptanalyst can get very useful information from the encrypted image. To check the sensitivity of the plain-text attacks, we use two criteria, NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity).

NPCR defined as a percentage of different pixels numbers between two cipher images and UACI defined as an average intensity of differences between two cipher images of M×N as defined in the following:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (9)$$

$$UACI = \frac{1}{M \times N} \sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{255} \times 100\% \quad (10)$$

Where, C1 and C2 are two different cipher images encrypted by using a different keys, where D (i , j) is defined as follows:

$$D(i,j) = \begin{cases} 1 \ if \ C1(i,j) \neq C2(i,j) \\ 0 \ if \ C1(i,j) = C2(i,j) \end{cases} \quad (11)$$

After calculations, we get the Average NPCR and UACI and tabulated in table-III for different test image. From table-III we can see that NPCR is about 99.6% with lowest value of 99.5880 % and UACI is about 33.5% with worst value of 33.5044% which is satisfactory for image encryption.

TABLE III. PLAIN TEXT SENSITIVITY ANALYSIS FOR VARIOUS TEST IMAGE

Plain Text Sensitivity Analysis				
Parameter	***Lena***	***Peppers***	***Mandrill***	***Deblur***
NPCR (%)	99.6048	99.5972	99.6368	99.5880
UACI (%)	33.5044	33.5189	33.6354	33.5170

F. Correlation Coefficient Analysis

In order to evaluate the encryption quality of the proposed encryption algorithm, the correlation coefficient is used calculate the correlation coefficients between two vertically, horizontally adjacent pixels of an encrypted image, the following equation is used [22].

$$\gamma = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (12)$$

$$D(x) = \frac{1}{M} \sum_{i=1}^{M} (x - \overline{x})^2 \quad (13)$$

$$Con(x,y) = \frac{1}{M} \sum_{i=1}^{M} (x - \overline{x})(y - \overline{y}) \quad (14)$$

Where M is the number of randomized pair and x, y is the values of pair of randomized image. In table-IV the results showed that the proposed method randomized the pixels in very good way. In Fig.6 shows the correlation for 256×256 Deblur image. Among them (a) Vertical correlation (b) horizontal correlation of original image and (c) (d) stands for encrypted image. From fig.6 we can see that though the original image is highly correlated to the adjacent pixel and values are distributed near the center but after encryption pixel values are uniformly distributed as a result lower the correlation value.

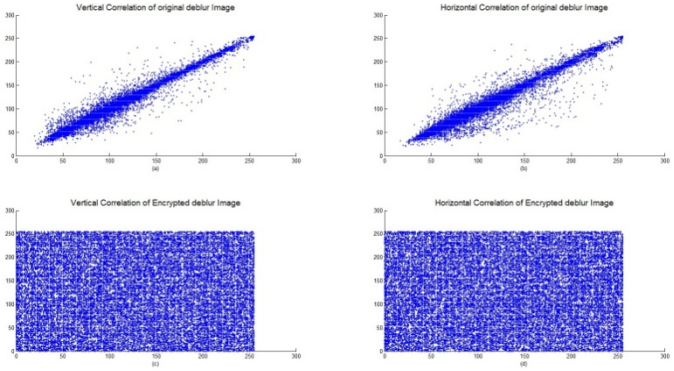

Figure 6. Correlation of original and encrypted Deblur image.

TABLE IV. CORRELATION COEFFICIENT FOR VARIOUS TEST IMAGE

Correlation Coefficient of Image								
position	***Lena***		***Peppers***		***Mandrill***		***Deblur***	
	Plain Image	Cipher Image	Plain Image	Cipher Image	Plain Image	Cipher Image	Plain Image	Cipher Image
Horizontal	0.9700	-0.0043	0.9315	-0.0024	0.8761	-0.0005	0.9838	0.0052
Vertical	0.9409	0.0014	0.9323	0.0084	0.8890	0.0032	0.9896	0.0006

G. Key Space Analysis

3D chaos is more key space then 1D and 2D chaos as a result provides higher security then others [31]. Again 3D linier chaos is less suitable then 3D non-linier chaos for security application. As a result we use non-liner 3D chaos for our algorithm.

Key space is the total number of different keys that can be used in the cryptographic system. There are total six initial conditions of chaotic map used in the algorithm and the initial conditions are $x_1, y_1, z_1, \alpha, \beta, \gamma$ used as secret keys of encryption with precision 10^{-14}. As a result, the key space size is $(10^{14})^6$ i.e. 10^{84}. Again we use eight random number $N1, N2, N3, N4, N6, N7, N8$ as a key. For those we use

precision of 10^5 then the key space size is $(10^5)^8$ i.e. 10^{40} as a result total key space size is larger than 10^{124}, which is large enough to resist the exhaustive attack. In section IV table VII, we compare this key space with respect to some other algorithm.

IV. COMPATIBILITY OF ALGORITHM

There is a lot of chaos based image encryption techniques proposed with their simulation result. In this section we highlight compatibility of our method to others with basis of some performance parameter. For test the performance Lena image of 256×256 is common slandered picture. We compare NPCR, UACI and Entropy of our method to other algorithm. From the table V we can see that NPCR and UACI which is better compare to the algorithm [24], [25], [29], [30], [18] and [32] and comparatively same with respect to [23], [26], [27]. In [18] and [32] which use 3D chaos for image encryption have poor performance and large number of round then our proposed method. Table VI shows the comparison of entropy among different method with ours. From that table we can conclude that entropy of our method is not bad with respect to other one and have a value near to the theoretical maximum value 8. Table VII stands for represent the key space superiority among different algorithm. From that table we can conclude that our proposed method have a largest key space than any other algorithm spatially with respect to [18] and [32]. In table VIII represents correlation coefficient superiority among different image encryption algorithms. From this table we can horizontal correlation coefficient of plain image is 0.9700 which is maximum then other and horizontal correlation value for cipher image is -0.0043 which is lowest compare to others and for vertical correlation it is not poor then others spatially with respect to [18] and [32].

TABLE V. PLAIN TEXT SENSITIVITY ANALYSIS FOR LENA IMAGE USING DIFFERENT METHOD

Method	NPCR (%)	UACI (%)
NPWLCM [23]	99.6292	28.5050
MMC [24]	99.5100	33.4500
CM and CF [25]	99.6000	33.5400
LIS and LM [26]	99.5956	33.6035
CEA [27]	99.6128	33.4420
CCML [29]	25.0000	19.0000
MCM [30]	41.9620	33.2500
3D Cat [18] (6 Round)	50.3000	25.2000
3D CBM [32] (5 Round)	99.6000	33.4000
Proposed Method	**99.6048**	**33.5044**

TABLE VI. RESULT OF ENTROPY ANALYSIS FOR ENCRYPTED LENA IMAGE USING DIFFERENT METHOD

Method	Entropy (Encrypted Image)
NPWLCM [23]	7.9975
MMC [24]	7.9997
LIS and LM [26]	7.9912
CEA [27]	7.9993
CM [28]	7.9891
MCM [30]	7.9968
Proposed Method	**7.9890**

TABLE VII. KEY SPACE COMPARISON AMONG DIFFERENT METHODS

Method	Key Space
NPWLCM [23]	2^{96}
MMC [24]	2^{230}
CM and CF [25]	2^{157}
LIS and LM [26]	10^{30}
CM [28]	10^{112}
CCML [29]	2^{203}
MCM [30]	2^{260}
3D Cat [18]	2^{36}
NCA [31]	10^{45}
3D CBM [32]	2^{128}
HC [33]	10^{70}
Proposed Method	$\mathbf{10^{124}}$

TABLE VIII. CORRELATION COFFICIENT COMPARISON AMONG DIFFERENT METHODS FOR LENA IMAGE

Method	Plain image		Cipher Image	
	Horizontal	Vertical	Horizontal	Vertical
NPWLCM [23]	0.9471	0.9665	-0.0159	-0.0195
MMC [24]	0.9537	0.9792	0.0047	0.0030
CM and CF [25]	0.9411	0.9702	-0.0003	0.0014
LIS and LM [26]	0.9603	0.9275	-0.0030	0.0085
CM [28]	0.9535	0.9616	0.0095	0.0106
CCML [29]	0.9341	0.9634	0.0014	0.0036
MCM [30]	0.9574	0.9399	0.0038	0.0028
3D Cat [18] (6 Iteration)	0.9176	0.9542	0.0118	0.0001
NCA [31]	0.92401	0.9561	-0.0158	-0.0653
3D CBM [32] (5 Round)	0.9765	0.9796	0.0445	0.0284
Proposed Method	**0.9700**	**0.9409**	**-0.0043**	**0.0014**

V. CONCLUSION

In this paper we proposed a 3D chaos based simple encryption technique with combination of position permutation techniques and value transformation techniques. Though pixel position permutation and XOR operation for value transformation is not a new concept for image encryption but to our knowledge, it is the first time that chaos has been used for position permutation. We can use this algorithm for low, medium and high security purpose by controlling its complexity. We can easily skip any step which reduces key size and complexity. A detailed statistical analysis on both stream generation system and the encryption scheme is given. However, we show by experimental results that our algorithm is sensitive to initial conditions and strong against the brute force attacks. Finally, after some tests like entropy analysis, statistical analysis and plain-text sensitivity, we show that our algorithm has a high security against different types of attacks. Experimental results, allow concluding that this algorithm outperforms existing schemes in term of security. Having a high throughput, the proposed system is ready to be applied in fast real time encryption applications and suitable for practical use in the secure transmission of multimedia information over the Web. The algorithm presented in this paper aims at the

image encryption; it is not just limited to this area and can be widely applied in other information security fields.

REFERENCES

[1] Srivastava, A., "A survey report on Different Techniques of Image Encryption". *International Journal of Emerging Technology and Advanced engineering. Vol. 2, pp. 163-167. 2012*

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

[3] Bhatnagar, G., & Wu, Q., "Chaos-Based Security Solution for Fingerprint Data During Communication and Transmission". *Instrumentation and Measurement, IEEE Transactions on, 61(4), 876-887. 2012.*

[4] Chang, C. C., Hwang, M. S., Chen, T. S., "A new encryption algorithm for image cryptosystems". *Journal of Systems and Software, 58(2), 83-91. 2001*

[5] Schneier B., "Applied Cryptography: Protocols, Algorithms, and Source Code in C", *John Wileyand Sons, New York, 1996.*

[6] Daemen J. and Rijmen V., "The Design of Rijndael: AES - The Advanced Encryption Standard", *Springer-Verlag New York, Berlin, 2002.*

[7] Kwok H. and Tang W., "A Fast Image Encryption System Based on Chaotic Maps With Finite Precision Representation," *Chaos, Solitons and Fractals, vol. 32, no. 4, pp. 1518-1529, 2007.*

[8] L. Kocarev., "Chaos-Based Cryptography: A Brief Overview". *IEEE Circuits and Systems, 1(3):6–21, 200.*

[9] J. C. Yen and J. I. Guo, "A new image encryption algorithm and its VLSI architecture." *in Proceedings of IEEE workshop on signal processing systems, pp. 430–437, 1999.*

[10] J. C. Yen and J. I. Guo, "A new chaotic key-based design for image encryption and decryption." *in Proceedings of IEEE International Symposium on Circuits and Systems, Vol.4, pp. 49–52, 2000.*

[11] L. Zhang, X. Liao, X. Wang, "An image encryption approach based on chaotic maps." *Chaos, Solitons and Fractals, vol. 24, no. 3, pp. 759–765, 2005.*

[12] C. Dongming, Z. zhiliang, Y. Guangming, "An Improved Image Encryption Algorithm Based on Chaos." in Proceedings of IEEE *International Conference for Young Computer Scientists, pp. 2792-2796, 2008.*

[13] A. N. Pisarchik, N. J. Flores-Carmona and M. Carpio-Valadez, "Encryption and decryption of images with chaotic map lattices." *Chaos Journal, American Institute of Physics, vol. 16, no. 3, pp. 033118-033118-6, 2006.*

[14] Li Xiongjun , Peng Jianhua , Xv Nin, "A Image Encryption Algorithm Based on Two-dimensional Chaotic Sequence" , *Journal of Image and Graphics , 2003 , 8(10) : pp. 1172-1177.*

[15] N. K. Pareek, V. Patidar, K. K. Sud, "Image encryption using chaotic logistic map." *Image and Vision Computing, vol. 24, no. 9, pp. 926–934, 2006.*

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

[17] Y. Mao, S. Lian, and G. Chen, "A novel fast image encryption scheme based on 3D chaotic Baker maps." *International Journal of Bifurcation and Chaos, vol. 14, no. 10, pp. 3616–3624, 2004.*

[18] G. Y. Chen, Y. B. Mao, C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps." *Chaos Solitons and Fractals, vol. 21, no. 3, pp. 749-761, 2004.*

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

[20] Hongjuan Liu, Zhiliang Zhu, Huiyan Jiang, Beilei Wang, "A Novel Image Encryption Algorithm Based on Improved 3D Chaotic Cat Map", *The 9th International Conference for Young Computer Scientists, 2008.*

[21] X. Tao, X. F. Liao, G. P. Tang, "A novel block cryptosystem based on iterating a chaotic map." *Physics Letter A, vol. 349, no. 1-4, pp. 109-115, 2006.*

[22] Min L. and Li T., "A chaos –based data encryption algorithm for image/video,". *Int. Conf. on Multimedia and information technology, pp 172-175, 2010.*

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

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

[25] A. Masmoudi, M.S. Bouhlel anf W. Puech, "A New Image Cryptosystem Based On Chaotic Map And Continued Fractions" *18th European Signal Processing Conference (EUSIPCO-2010),Aalborg, Denmark, pp 1504-1508, August 2010.*

[26] Hazem Mohammad Al-Najjar, "Digital Image Encryption Algorithm Based on a Linear Independence Scheme and the Logistic Map". *in Proceedings of ACIT-2011*

[27] Abir Awad and Dounia Awad, "Efficient Image Chaotic Encryption Algorithm with No Propagation Error". *ETRI Journal, Volume 32, Number 5, pp 774-783, October 2010.*

[28] Musheer Ahmad, M. Shamsher Alam, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping". *International Journal on Computer Science and Engineering, Vol.2 (1), 2009, pp 46-50.*

[29] Sodeif Ahadpour, Yaser Sadra, "A Chaos-based Image Encryption Scheme using Chaotic Coupled Map Lattices". *International Journal of Computer Applications,Vol. (49), Number-2,2012,ISBN 973-93-80869-31-6.*

[30] S.Behnia, A.Akhshani, H.Mahmodi, A.Akhavan, "A novel algorithm for image encryption based on mixture of chaoticmaps", *ELSEVIER Chaos, Solitons & Fractals,Volume 35, Issue 2, pp 408–419, January 2008.*

[31] H. Gao, Y. Zhang, S. Liang, D. Li, "A new chaotic algorithm for image encryption", *ELSEVIER Chaos, Solitons & Fractals, Volume 29, Issue 2, July 2006, pp 393–399.*

[32] Y. Maa, G. Chen, S. Lian, "A Novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps", *International Journal of Bifurcation and Chaos, Vol. 14, No. 10 (2004), pp 3613-3624*

[33] T. Gaoa, Z. Chenb, "A new image encryption algorithm based on hyper-chaos", *ELSEVIER Physics Letters A, Volume 372, Issue 4, pp 394–400, 21 January 2008.*

978-1-4799-5180-2/14/$31.00 ©2014 IEEE