Improving Image Encryption Using 3D Cat Map and Turing Machine

Nehal A. Mohamed
Dept. of Computer Science
Faculty of Information System,
MUST University
6th October, Egypt

Mostafa A. El-Azeim
Dept. of Computer Science
Faculty of Information System,
AASTMT
Heliopolis, Egypt

Alaa Zaghloul
Dept. of Computer Science
Faculty of Information System,
MUST University
6th October, Egypt

***Abstract*—Security of data is of prime importance. Security is a very complex and vast topic. One of the common ways to protect this digital data from unauthorized eavesdropping is encryption. This paper introduces an improved image encryption technique based on a chaotic 3D cat map and Turing machine in the form of dynamic random growth technique. The algorithm consists of two main sections: The first does a preprocessing operation to shuffle the image using 3D chaotic map in the form of dynamic random growth technique. The second uses Turing machine simultaneous with shuffling pixels' locations to diffuse pixels' values using a random key that is generated by chaotic 3D cat map. The hybrid compound of a 3D chaotic system and Turing machine strengthen the encryption performance and enlarge the key space required to resist the brute force attacks. The main advantages of such a secure technique are the simplicity and efficiency. These good cryptographic properties prove that it is secure enough to use in image transmission systems.**

Keywords—chaotic 3D cat map; brute force attacks; Dynamic random growth technique; Turing machine; key space

I. INTRODUCTION

Up-to-date development and progress in the means of multimedia industry and the ways of communications have made studies focus on creating new schemes to enhance the security of transmission and storing multimedia data over open channels including the Internet and wireless networks. In mean times, multimedia data were transmitted over computer networks can be audio, image, and other multimedia types. During that, the images can be considered one of the most usable forms of information. These images often contain private or confidential information and sometimes they associated with financial interests [1, 2]. Security of digital image has become more and more important because of the advances in communication technology and multimedia technology. Three different ways to protect these digital images from unauthorized eavesdropping are cryptography, steganography and watermarking. Among these three techniques, cryptography has become one of the major tools to provide a high level of security. Image encryptions have applications in various fields including Internet communication, multimedia systems, medical imaging, telemedicine and military communication. As a result, the security for images, it needs to be hidden from unauthorized access to decode by transferring the multimedia data into an entirely different format, protected from unauthorized change, and available to an authorized entity, when it is needed. Although the three previously mentioned requirements have not changed, they now have some new dimensions. Not only should images be confidential, when it is stored in the computer; there should also be a way to maintain its confidentiality when it is transmitted from one computer to another. "Fig. 1" presents a diagrammatic view of general encryption-decryption mechanism.

The primary essence of this paper would be the protection of images. The high efficiency of any cryptographic algorithm is the most important criterion by which the robustness of encryption is measured. Traditional image encryption algorithms, for instance, private key encryption standards (DES and AES) faces problems when used to encrypt large images and therefore, its efficiency becomes low and weak, public key standards such as Rivest Shamir Adleman (RSA), and the family of elliptic-curve-based Encryption (ECC), as well as the international data encryption algorithm (IDEA) requires a great computational time and super computers when used in encrypting real-time images, may not be the most desirable candidates for image encryption, especially for fast and real-time communication applications because of Cryptographic algorithms that use less time are much more preferable for encrypting such real-time images. Also, some encryption schemes may be run very slowly, and this increases the degree of security features, yet they would be of little use when dealing with real-time images [3].

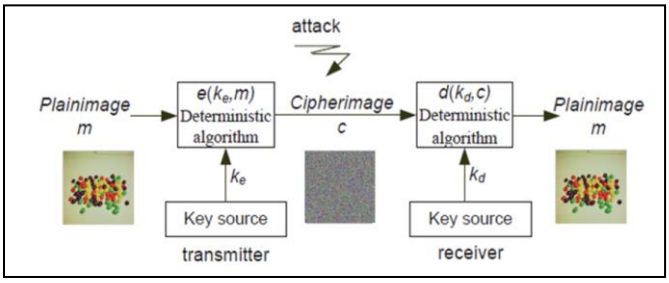

Fig. 1. General Encryption-Decryption Mechanism

In the last decade, chaos-based encryption techniques are considered suitable for practical applications since they have a perfect combination of speed, high security, complexity, reasonable computational overheads, and computational power. Moreover, chaos-based and other dynamical systems based algorithms have many important properties such as the

sensitive dependence on initial conditions and system parameters, pseudorandom properties, ergodicity, and non-periodicity [4].

Some chaos image encryption schemes have developed in recent years. In [5] proposed a new image encryption algorithm based on 3D chaotic map; this algorithm does not use the whole chaotic numbers, but only utilizes partial elements as running key. In chaotic sequence, those used elements keep certain interval, which is determined by the current ciphertext. Due to ciphertext closely related to plaintext, running-key is indirectly related with plaintext. In [6], shuffles the RGB layers by using 3D Cat map and standard map, and finally, the image is encrypted by performing XOR operation on the shuffled image and diffusion template. In [7], suggested a novel image encryption algorithm based on a three dimensional (3D) chaotic map; the design of the proposed algorithm based on three phases. In phase I, the image pixels are shuffled according to a search rule based on the 3D chaotic map. In phases II and III, 3D chaotic maps are used to scramble shuffled pixels through mixing and masking rules, respectively.

In this paper, an encryption algorithm for digital images which based on chaotic 3D cat map and the Turing machine is proposed. As cat map is weakness and has some common drawbacks that are: 1) periodic, and 2) can be easily cracked By chosen plaintext attack, we use cat map in another more secure way, which has benefits of mixing and sensitivity to initial conditions and parameters, to overcome these former defects; through calculating an intermediate parameter based on the blue layer of the image. The intermediate parameter is used as the initial parameter of a chaotic map to generate a random key stream. Consequently, the generated key streams are dependent on the plaintext image, which can resist the chosen plaintext attack [8]. The 3D chaotic map with random choose of initial conditions and parameters are used to generate three discrete chaotic sequences with high sensitivity by iterations. Two of the sequences are then used to design a two-dimensional permutation by calculating new coordinates of each pixel of the image and shuffle it. Then elements of the third one affect the behavior of the other two sequences through effect the initial values of the chaotic system for the further encryption process, which increases the sensitivity of plaintext images of the scheme. Both theoretical and computer simulations show that the algorithm is secure enough to use in image transmission system.

Organize other sections of this paper as follows: Section 2 introduces a chaotic 3D cat map; Section 3 discusses Turing machine; Section 4 shows the proposed image encryption and decryption schemes; Sections 5 and 6 present the experiment results and security analysis; Section 7 presents time complexity; finally, Section 8 concludes this paper.

II. The Chaotic 3D Cat Map

Arnold's cat map is a discrete-time dynamical system. Specifically, it is a kind of cut-out transformation, is originally introduced into traverse theory by Arnold and so-called Arnold transformation [9]. Arnold cat transformation is a classical encryption algorithm. Mathematically, Arnold's cat map is given by "(1)":

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1 \qquad (1)$$

In the process of image encryption, the use of Arnolds Cat Map provides extra security, as it approaching higher randomness. The above 2D cat map is now generalized by producing two new parameters, p and q into "(1)", which increase key spaces to resist brute-force attacks and longer averaged period lengths improve map randomness [10] to resist statistical attacks, as follows "(2)":

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod N \qquad (2)$$

To increase the security of the Arnold's cat map, the generalized 2D cat map is extended to a 3D discrete chaotic map by introducing six control parameters; $a_X, a_Y, a_Z, b_X, b_Y, b_Z$, a three-dimensional cat map can be presented as the following formula "(3)":

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{pmatrix} = A \begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix} \bmod 1 \qquad (3)$$

where

$$A = \begin{pmatrix} 1 + a_X a_Z a_Y & a_Z & a_Y + a_X a_Z + a_X a_Y a_Z b_Y \\ b_Z + a_X b_Y + a_X a_Z b_Y b_Z & a_Z b_Z + 1 & a_Y a_Z + a_X a_Y a_Z b_Y b_Z + a_X a_Z b_Z + a_X a_Y b_Y + a_X \\ a_X b_X b_Y + 1 & b_X & a_X a_Y b_X b_Y + a_X b_X + a_Y b_Y + 1 \end{pmatrix}$$

One can be easily verified that det $A = 1$, which means the 3D discrete cat map is a $1-1$ map and the sensitivity to initial conditions and parameters are kept unchanged. By simply setting $a_X = b_X = 1, a_Y = b_Y = 2, a_Z = b_Z = 3$, one gets

$$A = \begin{pmatrix} 7 & 3 & 17 \\ 23 & 10 & 56 \\ 4 & 1 & 10 \end{pmatrix}$$

Through numerical calculations, three eigenvalues of the above A are $\sigma 1 = 25.1314, \sigma 2 = 0.0215, and \sigma 3 = 1.8470$. It verified that the leading Lyapunov exponent is strictly positive since and given by $\ln \sigma 1$. Consequently, the corresponding 3D cat map is higher chaotic with properties of mixing and sensitivity to initial conditions and parameters of it.

III. Turing Machine

A Turing machine deals with a sequential tape having only three symbols: 0, 1, * . In this example the machine will take a binary number delimited by two * , and increment it by 1.

For example, if it reads * 1111 0110 * it should give * 1111 0111 * . If it reads * 0001 0011 * it should give * 0001 0100 * . If it reads * 1111 1111 * it should give * 0000 0000

$*$. And so on. "Fig. 2" presents the flow diagram of the encryption algorithm.

There are four ways to represent Turing Machine which are be from either right-to-left, or right-to-left inverse, or left-to-right, or left-to-right inverse.

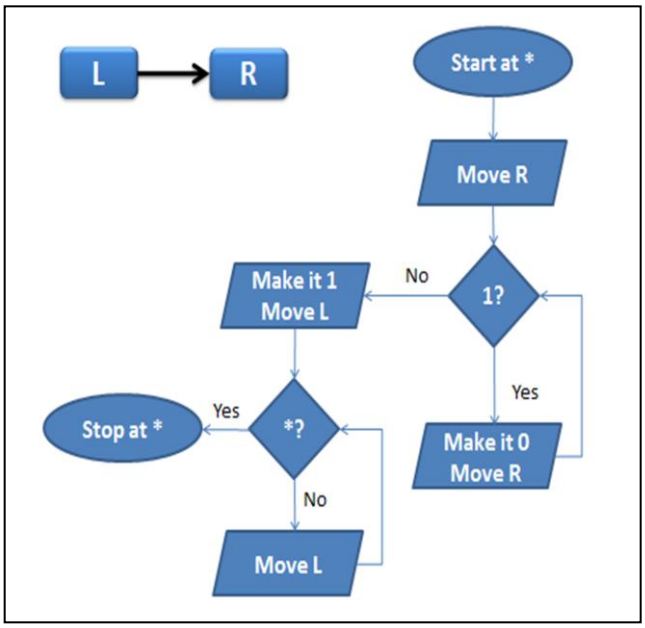

Fig. 2. Flow Diagram of Process of Left-to-Right Turing Machine

IV. Details of the Proposed Method

A. The proposed encryption scheme

In the proposed method, three pseudorandom discrete variables of 3D chaotic cat map are adopted to permute color image $O(i, j)$ of size $I \times J$ using the formula of "(3)". The presented method is a combination of two essential operations, permutation and substitution. "Fig. 3" gives the flow diagram of the encryption algorithm. The procedure of our encryption scheme is described as follow:

1) For 3D cat map "(3)", as shown in [10], choose at random three initial value (x_0, y_0, z_0) and six control parameters $(a_x, a_y, a_z, b_x, b_y, b_z)$, which are served as secret keys.

2) Before, presenting theses intrinsic processes, a preprocess operation is performed which use three initial values (x_0, y_0, z_0) to iterate the 3D chaotic map n_c times to avoid the harmful effect of the initial values, where n_c is a present integer and served as a secret key, too. Assign the last three outputs (x_0, y_0, z_0) from "(3)", to be new initial values of a 3D discrete cat map.

3) Permutation Operation: In this procedure, a 3D cat map is still used. This process can be achieved through the following steps:

a) The plain image is divided into three basic layers (red, green and blue), each of them divided into four sub-blocks which are equal in size, then rotate the first three sub-images 90 degree where the 1^{st} sub-image is rotated 90 degree twice times, the 2^{nd} sub-image is rotated 90 degree triple times, and the 3^{rd} sub-image is rotated 90 degree only once time.

b) We apply a 3D discrete chaotic cat map on red and green layers for each sub-image, while blue layer for all blocks is still unchanged.

c) While we iterate a chaotic 3D cat map for n_C times; where $n_C = 1, 2, ..., 204$, we get three pseudorandom chaotic key stream values (x_1, y_1, z_1), where x_1 and y_1 are used to calculate a new position (s,d) corresponding to the present pixel $O(i, j)$ using output of "(3)".

d) The chaotic sequence S_Z is produced using the pseudorandom chaotic key stream value z_1 which is generated by "(3)". In order to avoidance fleeting effects, neglect the first 200 values resulting from iterating 3D cat map.

e) Let [8]:

$$low_j = floor\left(x_{200+j} \times 10^{14}\right) \bmod \frac{N}{8} + \frac{N}{2} + (j-1)\frac{N}{8}; j = 1, 2, 3, 4. \quad (4)$$

f) Calculate sum for the original blue layer of each block; since S_B^{ij} represents the pixels' values of blue layer B at position (i, j) to affect the resulted values of a 3D separate chaotic cat map.

g) Perform the confusion procedure to the lower part of the size $low_i \times low_i$ of each of the four sub-images of the plain-image using 3D chaotic map respectively. "This is the so called [8] dynamic random growth technique, since the size of the lower part of each block of the plaintext image permuted by 3D chaotic map is random."

h) Operate confusion operation to the whole each sub-block by 3D chaotic map.

4) Substitution Operation: In this procedure, the pixels' values are altered by performing Turing machine on each block of the four sub-images. This process can be achieved through the following steps:

a) While confusing pixels' values in permutation process, performing Turing machine (TM) either from left-to-right or vice versa.

b) We convert every pixel value to a binary number B of 8 bit lengths.

c) Turing machine works as if pixel value equals 1 converts it to 0 until reached to the 1^{st} pixel value equals 0, then converts it to 1 and the rest of bits still un-changed, as introduced in "Fig. 2".

$$O(m,n) = TM\left(O(s,d)\right) \quad (5)$$

$$O(s,d) = TM\left(O(m,n)\right) \quad (6)$$

d) After applying Turing machine for red and green layers of each sub-image, we get R' and G'.

e) To enhance the security of encryption process, apply a bit exclusive OR, using the following formula:

$$G' = R' \oplus G' \quad (7)$$

$$B' = G' \oplus B \quad (8)$$

f) After applying Permutation- Substitution Operation on all sub-blocks in the three layers we combine these sub-blocks into one block for each layer then combine this layer to construct cipher image.

B. The proposed decryption scheme

The decryption process is the inverse process of the corresponding encryption scheme. "Fig. 4" gives the flow diagram of the decryption algorithm.

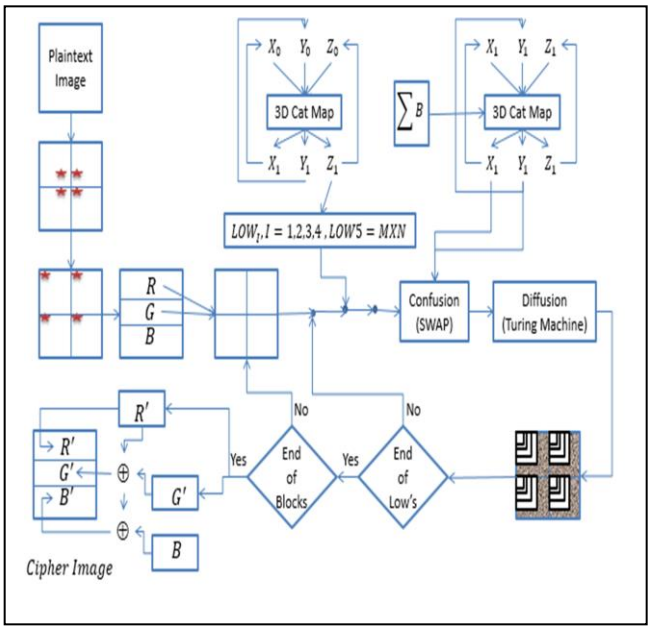

Fig. 3. Flow Diagram of Process of the Introduced Encryption Scheme

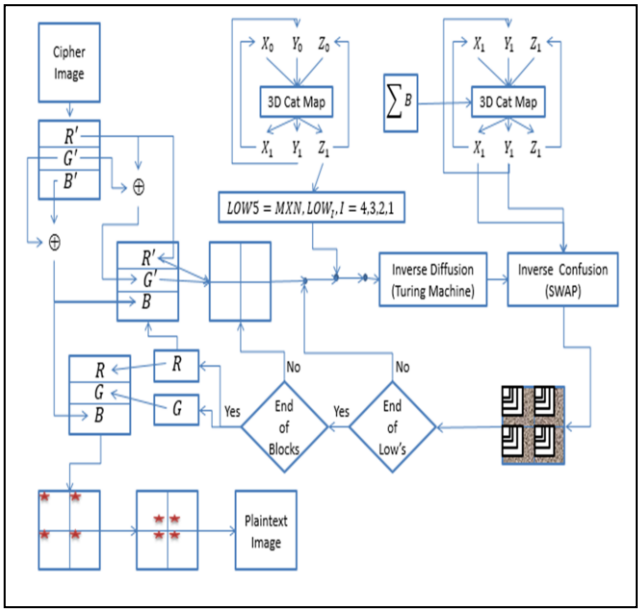

Fig. 4. Flow Diagram of Process of the Introduced Decryption Scheme

V. Experimental Results

We use MATLABR2013a to simulate our proposed scheme on 2.30 GHz CPU, with 4.00 GB memory running on Windows 8.1. We select five standard color images as the plain images which are Lena.bmp, Splash.bmp, Jet.bmp, and Girl.bmp of size 512×512 and Lena.bmp of size 500×400 .

For a chaotic 3D cat map, the initial values $x_0 = 0.3, y_0 = 0.4, and\ z_0 = 0.5$ and six control parameters $a_x = b_x = 1, a_y = b_y = 2, and\ a_z = b_z = 3,$ are served as keys, after iterating the map n_c times, where n_c is a present integer and served as secret key, too.

"Fig. 5" and "Fig. 6" show the results both of original and cipher images, Splash and Jet standard color test images, respectively. In the proposed encryption scheme, one round of the scheme indicates that the cipher reaches a high secure level.

VI. Security Analyses

Security and performance are the crucial requirements for any encryption system. Different from the encryption of textual information, the encryption of visual information requires security against cryptographic attacks such as differential analysis, related-key attack, and statistical attack. Generally, an encryption scheme should be thoroughly analyzed before it can be used in practical applications. Indeed, several metrics can be used to measure the cipher's resistance to some typical attacks, for example, sensitivity analysis, statistical analysis, numeric analysis, etc.

Generally, if the encryption scheme is secure against most of the attacks, we can say that the encryption scheme is of high level of security. Otherwise, the encryption scheme is regarded as of low security. The detailed analyses are investigated in this section as follows.

A. Key space analysis

For an effective cryptosystem, the key space should be sufficiently large enough to prevent brute-force attack. "It is known that [11] the ideal key space should be larger than 2^{100} while considering the current computer computation speed. The total key space of our presented algorithm composed of three parts which are summarized as follow: ① the initial values (x_0, y_0, z_0) ; ② six parameters $(a_x, a_y, a_z, b_x, b_y, b_z)$; ③ preprocess parameter n_c of a chaotic 3D cat map, and then it is around $\approx 2^{392}$ which is much larger than in the algorithms of G. Gu, J. Ling [10] and X. Wang et al. [8]; so it is obvious that the presented technique has a large enough key space to resist common brute- force attacks. The key space comparison with our encryption scheme is shown in Table I.

TABLE I. Key Space Comparison with the Existing Algorithms

Algorithm	*Key Space*
G. Gu, J. Ling [10]	10^{90}
X. Wang et al. [8]	$> 10^{96}$
Proposed algorithm	25×10^{150}

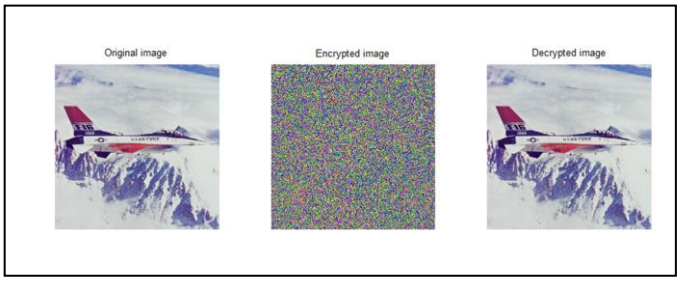

Fig. 5. Encryption and decryption results: Left side with original image, center with encrypted image, and right side with deciphered image of Splash image

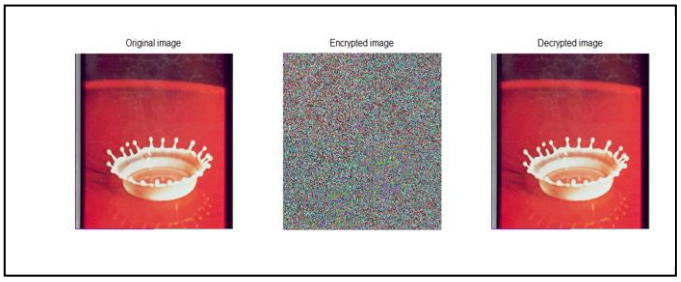

Fig. 6. Encryption and decryption results: Left side with original image, center with encrypted image, and right side with deciphered image of Jet image

B. Statistical analysis

Since most of the existing cipher systems [12] have been cryptanalyzed successfully; we need to prove the robustness and effectiveness of the proposed image encryption scheme against statistical attacks. So in this section, we provide and analyze three statistical tests which are histograms analysis DH and the correlations computation of the adjacent pixels in encrypted images rxy, and information entropy of the ciphered image in order to evaluate the ability of the encryption algorithm to substitute the original image with uncorrelated encrypted image and two other metrics, NPCR and UACI, in order to which evaluate the diffusion characteristics of the encryption algorithm.

1) Histograms of corresponding images

To prevent the information leakage and aggressive attacks [13, 14], it must be ensured that the original and encrypted images do not have any statistical similarity. Histogram analysis is a visual test which reveals the distribution information of pixel values and statistical characteristics of images, by graphing the number of pixels at each color or grey scale intensity level.

An ideal histogram of the encrypted image should have a uniform and completely different histogram against the plain-image. The experimental results of histograms analysis on both original image and its corresponding cipher image using the introduced scheme are shown in "Fig. 7"; where 1st Frame is the original image and its histogram, 2nd Frame is the encrypted image and its corresponding histogram. The histogram of RGB layers are shown in "Fig. 8" where upper figure is the red layer of original image and its histogram, center is the green layer of original image and its histogram, and lower is the blue layer of original image and its histogram.

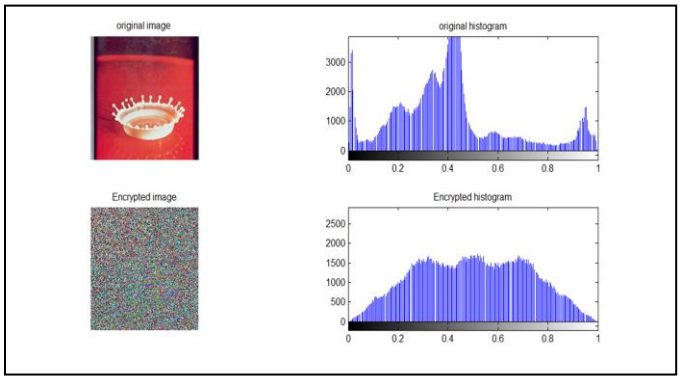

Fig. 7. Histogram analysis of image Splash

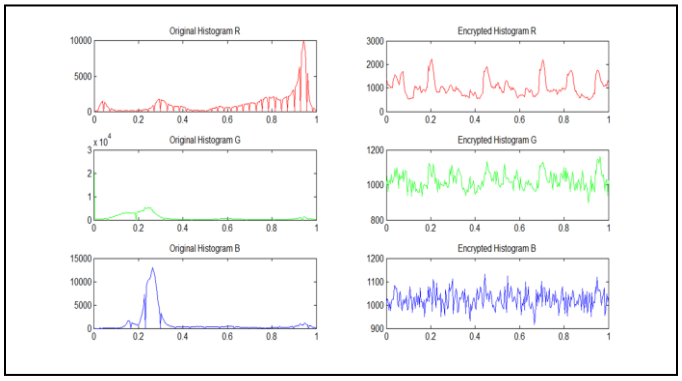

Fig. 8. Histogram Analysis of RGB Layers of Image Splash

2) Correlations Coefficient

In a digital image pixels are not independent and their relevance is great. This may indicate that a large area of the image has similar values. For example, in a common television digital image, the correlation coefficient of adjacent pixels may reach 0.9; that is, the relevance (which means information redundancy) is very big. The smaller the relevance, the better is the encryption effect and the higher is the security. We show the fact that the relevance [2] between plain images and cipher images is very small in two ways. It is important to calculate the correlation coefficients of two adjacent pixels of the encrypted image, so we analyze 2500 pairs of two-adjacent pixels of both original and encrypted images either in vertical, or horizontal, or diagonal directions. To do that, we use the following relations:

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{7}$$

where

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right),$$

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

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2$$

where E(x) is the mean of x , D(x) denotes the variance at pixel value x, and cov(x, y) is the covariance between two

color x and y; where x and y are the gray-scale values of two pixels in the same place in the plain and cipher images, N is the total number of pixels selected from the image for the calculation. For the plain-image, the correlations between adjacent pixels in those directions are close to 1. This means that the adjacent pixels are highly correlated to each other. On the other hand, the correlation coefficients of the encrypted image are close to 0 and hence the adjacent pixels in the encrypted image are entirely uncorrelated to each other as shown in "Fig. 9". All the correlation coefficients are calculated and listed in Table II.

3) Entropy analysis

Entropy is the most significant feature of disorder, or more precisely unpredictability. Relaying on Shannon's theory, "it measures [16] the randomness and quantifies the expected value of the information contained in a message". For example, a long sequence of repeating characters has entropy of 0, since every character is predictable and a truly random sequence has maximum entropy, since there is no way to predict the next character in the sequence. The information entropy H (x) of a plain image of a random variable x can be calculated using the following formula:

$$H(x) = \sum_{i=1}^{N} p(x_i)\log_2 \frac{1}{p(x_i)} \quad (8)$$

where $p(x_i)$ represents the probability distribution of appearance of symbol x. The ideal information entropy value of the cipher image should be close to 8 after encryption, which leads to less possible for the cryptosystem to divulge the information. Table III shows the entropy values of the proposed scheme, as we can find that they are all close to the ideal value 8. As one can see, the information entropy in the proposed algorithm is close to G. Gu, J. Ling [10], and better than X. Wang et al. [8] algorithms as shown in Table IV.

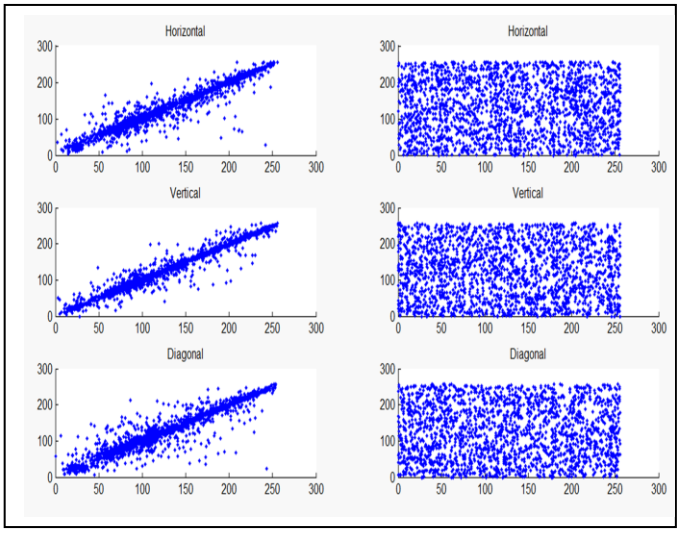

Fig. 9. Correlation chart. Upper frame with horizontal distribution, center with vertical distribution, and lower with diagonal distribution. Left side with Lena tested image, right side the proposed technique

TABLE II. CORRELATION COEFFICIENTS OF ADJACENT PIXELS IN SPLASH IMAGE

Directions	*Plain image*	*Decrypted image*
Horizontal	0.925665	0.014981
Vertical	0.998203	-0.008089
Diagonal	0.925010	0.007515

TABLE III. INFORMATION ENTROPIES VALUES

Tested Images	*Proposed Scheme*
Lena.bmp 512×512	7.9994
Splash.bmp 512×512	7.9991
Jet.bmp 512×512	7.9993
Girl.bmp 512×512	7.9993
Lena.bmp 500×400	7.9989

TABLE IV. THE RESULTS OF COMPARISON OF INFORMATION ENTROPY

Tested image	*The result of information entropies*		
	Proposed Scheme	*G. Gu, J. Ling [10]*	*X. Wang et al. [8]*
Lena.bmp ($\mathbf{256 \times 256}$)	7.99743	7.9999	7.99705

4) Differential attack

A desirable property for cipher image [17] is being sensitive to any tiny changes (e.g., modifying only one pixel) in plain-image to monitor the change in the result. Consequently, we can be able to figure a meaningful relationship between both original and encrypted images. An Assailant often tries to elicit this crucial relationship by making minor changes, usually only one pixel, in the plain-image while encrypting the plain-image with the same encryption keys, and then observes the changes of corresponding cipher image. Also, this action facilitates finding the encryption keys and breaking them.

To test the influence of one-pixel change on the plain image encrypted by the proposed scheme, two common measures may be used [18], number of pixels change rate (NPCR) and unified average changing intensity (UACI), which are calculated. The NPCR is used to measure the percentage of the number of pixels changed in cipher-text after making a slight change in plaintext. Therefore, the theoretical greatest upper-bound of the NPCR is 100%. Therefore, the NPCR is calculated by using the following formula "(9)" and "(10)":

$$NPCR_{R,G,B} = \frac{\sum_{m \times n} D_{R,G,B}(m,n)}{M \times N} \times 100\% \quad (9)$$

where

$$D_{R,G,B}(m,n) = \begin{cases} 1, if\ C^1(m,n) = C^2(m,n) \\ 0, if\ C^1(m,n) \neq C^2(m,n) \end{cases} \quad (10)$$

The UACI is used to measure the averaged intensity change for pixels in cipher-text images after making a slight change in a plaintext image. It is demonstrable that the UACI of an ideal cipher for 8-bit gray images is about 0.3346. Therefore, the UACI is calculated by using the following formula "(11)":

$$UACI_{R,G,B} = \frac{1}{M \times N} \sum_{m,n} \frac{\left| c^1(m,n) - c^2(m,n) \right|}{255} \times 100\% \quad (11)$$

where c^1 and c^2 are cipher images before and after one pixel change in a plain-image, respectively. The pixel values at grid (m,n) in c^1 and c^2 are denoted as $c^2(m,n)$ and $c^2(m,n)$; a bipolar array D is defined as "(10)". Table V shows the results of NPCR and UACI for one pixel change in the following standard images. It is clear that, the proposed cipher has good performances in both the NPCR and UACI analyses. Simulation results fit the expectations of the ideal cipher very well.

As one can see, the NPCR and UACI values in the proposed algorithm are close to G. Gu, J. Ling [10] and better than X. Wang et al. [8] algorithms as shown in Table VI.

TABLE V. THE NPCR AND UACI OF CIPHERED IMAGES WITH ONE BIT DIFFERENT BETWEEN THE PLAIN IMAGES

Test Images	*NPCR*	*UACI*
Lena.bmp 512×512	0.99651	0.34168
Splash.bmp 512×512	0.99699	0.35269
Jet.bmp 512×512	0.99666	0.32529
Girl.bmp 512×512	0.99648	0.32463
Lena.bmp 500×400	0.99629	0.34325

TABLE VI. THE NPCR AND UACI PERFORMANCE

Items	*Proposed Scheme*	*G. Gu, J. Ling [10]*	*X. Wang et al. [8]*
NPCR	0.99651	0.99748	0.99586
UACI	0.34168	0.33915	0.33253

VII. TIME COMPLEXITY

Time complexity has become more and more important issue when the scale of an application grows. So, [19] it is the relation of computing time and the amount of input. Time complexity of an algorithm signifies the total time required by the program to run to completion. In "computational complexity theory", intuitively the "computational" part means problems that can be modeled and solved by a computer. "The main idea of algorithm's analysis [20] is to have a measure of efficiency of algorithms that doesn't depend on machine specific constants, and doesn't require algorithms to be implemented and time taken by programs to be compared".

Formally, the time complexity $O(f(n))$ of the proposed algorithm can be calculated using the following formula:

$$f(m,n) = \left[2 \times \left(4 \times \left(16m_1^2 + 16m_2^2 + 16m_3^2 + 16m_4^2 + 16m \times n \right) \right) \right] + c,$$

where $m_1, m_2, m_3, m_4 < m$

Consequently, the time complexity for the proposed scheme is $O\left(f(m,n)\right) = M \times N$.

VIII. CONCLUSIONS

This paper develops an improving permutation—substitution image encryption architecture, based on a chaotic 3D cat map and Turing machine in the form of dynamic random growth technique. A new block encryption scheme was proposed for secure digital images that included two primary processes, Turing machine for substation and a chaotic 3D cat map for pixels permutation. Many statistical tests were operated to prove the suitability of the algorithm. Experimental tests and statistical analyses have shown effectiveness and robustness of the presented scheme against various attacks; prove that our introduced technique is pretty fast image encryption. According to theses pretty characteristics, the proposed encryption scheme may be convenient for different applications, and demonstrate that it reaches a high-security level while transmitting of digital images over the open network. The results of the comparison show that the proposed scheme has more benefits compared to these algorithms of G. Gu, J. Ling [8] and X. Wang et al. [10] ciphers.

REFERENCES

[1] S. S. Askar, A. A. Karawia, and Ahmad Alshamrani, "Image Encryption Algorithm Based on Chaotic Economic Model," Journal of Mathematical Problems in Engineering, vol. 2015, Article ID: 341729, pp. 1-10, December 2014.

[2] Xiaoyan Zhang, Chao Wang, Sheng Zhong, and Qian Yao, "Image Encryption Scheme Based on Balanced Two-Dimensional Cellular Automata," Mathematical Problems in Engineering, vol. 2013, Article ID: 562768, pp.1-10, November 2013.

[3] Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle," Journal of Electrical and Computer Engineering, vol. 2012, no. 7, pp. 1-13, January 2012.

[4] Adelaïde Nicole Kengnou Telem, Colince Meli Segning, Godpromesse Kenne, and Hilaire Bertrand Fotsin, "A Simple and Robust Gray Image Encryption Scheme Using Chaotic Logistic Map and Artificial Neural Network," Journal of Advances in Multimedia, vol. 2014,no.19, pp. 1-13, December 2014.

[5] 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, pp. 2943–2959, July 2012.

[6] Kamlesh Gupta, and Sanjay Silakari, "New Approach for Fast Color Image Encryption Using Chaotic Map," Journal of Information Security, vol. 2, no. 4, pp. 139-150, October 2011.

[7] 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, pp. 2943–2959, July 2012.

[8] Xingyuan Wang, Lintao Liu, and Yingqian Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," Optics and Lasers in Engineering vol. 66, pp. 10-18, March 2015.

[9] G.R. Chen, Y.B. Mao, and K.C. Charles, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos, Solitons & Fractals, vol, 21, no. 3, pp. 749–761, July 2004.

[10] Guosheng Gu, and Jie Ling, "A fast image encryption method by using chaotic 3D cat maps," Optik - International Journal for Light and Electron Optics, vol. 12, no. 17, pp. 4700–4705, September 2014.

[11] H. Zhu, Cheng Zhaob, Xiangde Zhanga, and Lianping Yanga, "An image encryption scheme using generalized Arnold map and affine cipher," Optik - International Journal for Light and Electron Optics, vol. 125, no. 22, pp. 6672–6677, November 2014.

[12] Narendra K Pareek, "Design and Analysis of a Novel Digital Image Encryption Scheme," International Journal of Network Security & Its Applications (IJNSA), vol.4, no.2, pp. 95-108 , March 2012 .

[13] Saeed Bahrami, and Majid Naderi, "Image Encryption Using a Lightweight Stream Encryption Algorithm," Advances in Multimedia, vol. 2012, Article ID: 767364, pp.1-8, June 2012.

[14] Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari,and Hamida Almangush, "A Novel Image Encryption using an Integration Technique of Blocks Rotation based on the Magic cube and the AES Algorithm," International Journal of Computer Science Issues (IJCSI), vol. 9, no. 4, pp. 41, July 2012.

[15] Yue Wua, Joseph P. Noonan, and Sos Agaian, "Shannon Entropy based Randomness Measurement and Test or Image Encryption," Information Sciences, ElSEVIER, pp. 1–23, March 2011.

[16] Alireza Jolfaei, and Abdolrasoul Mirghadri, "Survey: Image Encryption Using Salsa20," International Journal of Computer Science Issues (IJCSI), vol. 7, no. 5, pp. 213-220, September 2010.

[17] Gelan Yang, Huixia Jin, and Na Bai, "Image Encryption Using the Chaotic Josephus Matrix," Mathematical Problems in Engineering, vol. 2014, Article ID: 632060, pp. 1-13, March 2014.

[18] http://callmenick.com/post/time-complexity-analysis-why-its-important, accessed on (23-10-2015).

[19] http://www.geeksforgeeks.org/analysis-of-algorithms-set-3asymptotic-notations/, accessed on (23-10-2015).