Asian Journal of Computer Science and Technology
ISSN: 2249-0701 Vol.8 No.S1, 2019, pp. 70-73

Image Encryption Using Arnold Map

P. Sridevi[1] and J. Suguna[2]
[1]Research Scholar, [2]Associate Professor,
[1&2]Department of Computer Science, Vellalar College for Women, Tamil Nadu, India
E-Mail: sridevi@vcw.ac.in, sugunajravi@yahoo.co.in

***Abstract* - Nowadays transmission of data over the network is increasing and the data can be in the format of text, image, audio and video. Images are widely used in maximum applications of daily life. Image encryption is one of the most recent area of research to meet the demand during image transmission. Transformation of image from one form to erroneous form is called as image encryption. So, it can be secured from unauthorized users. The security of encrypted image is completely dependent on two important aspects i.e. the strength of the cryptographic algorithm and the confidentiality of the key. This paper proposes an algorithm of image encryption based on 3D Arnold cat map combined with logistic chaotic map. To evaluate the security of the encrypted image of this scheme, key space analysis and differential attack are performed. Several test images are used to demonstrate the validity of the proposed encryption algorithm. The experiment result shows that the proposed algorithm provides an efficient and secure approach to real-time image encryption and transmission.**

Keywords: **Chaos, Image encryption, Arnold map, Iterations and Logistic map.**

I. INTRODUCTION

In recent years, information security is an important one in various fields like internet, telecommunication, networks, multimedia systems, mobile phones, satellite, medical imaging and military communication. It is necessary to encrypt the data before transmission over the public network to preserve its security and to prevent unauthorized access. Image is one of the important forms of multimedia data. Image is very large in size, so the image requires large volume of storage and takes more time for transmission. The cryptographic algorithm proposed best methods to increase security of the image through encryption [1].A mathematical function utilized for the process of encryption and decryption of data or image is called a cryptographic algorithm. Existing security techniques are based on the conventional encryption techniques. Conventional cryptography uses single key for both encryption and decryption named as secret key or symmetric key encryption, Conventional encryption is very fast and relatively expensive. Public key cryptography is an asymmetric encryption that used a pair of keys, public key for encryption and private key for decryption of data[3]. The use of chaos techniques for image security is studied in recent years due to the properties of ergodicity, sensitivity to initial conditions and system parameters that are intrinsic in chaotic systems. The various chaotic maps such as Arnold cat map, Logistic map and Henon map are used in isolation or combination with other techniques to achieve efficient image encryption [4].The properties of chaos is good for image encryption and it increases the robustness of cryptosystem against statistical attacks[7].The chaos encryption algorithm leads to develop image security schemes to satisfy the demand of secure image transmission over the communication channel. Encryption algorithms based on chaotic maps like standard map, Logistic map, Cat map, Baker map, Henon map, Chen map and Arnold map are used to get better security performance of image encryption[8].

The rest of this paper is organized as follows. Section II describes brief discussion about related works. Section III explains the proposed methodology. Section IV provides the experimental results and their discussions. Section V concludes the research work.

II.RELATED WORKS

Joshua *et al.*, [1] discussed the strengths of the pseudo randomly enhanced logistic map (PELM) to achieve high security for medical images. The scheme achieved secure encryption by Arnold transformation followed by pixel value modification with chaotic key sequence. The experimental results showed that the scheme promises stronger resistance against common attacks and confirmed that PELM produces better pseudorandom properties than the direct logistic map. Sridevi et al.[5] presented Encryption -then-Compression(ETC) system using chaotic encryption and Asymmetric Numeral Method (ANM) to enhance the image security with high compression performance. Colpitts, Duffing and Henon chaotic system are used to encrypt the image. Asymmetric Numeral Method (ANM) is used for compression to improve the compression performance.The ETC system is analyzed based on the performance measures such as Compression performance, Computation time, Number of Pixel Change Rate [NPCR] and Unified Average Changing Intensity [UACI]. The simulation results proved that the Colpitts henon system is efficient for image security. Junqin Zhaoet al.[8] proposed a permutation-substitution image encryption scheme based on generalized Arnold map. Only one round of permutation and one round of substitution are performed to get the desirable results. The generalized chaotic Arnold maps are applied to generate the pseudo-random sequences for the permutation and substitution. The permutation and substitution are both performed row-by-row/column-by-

column to increase the speed of encryption. The security and performance of the this scheme isanalyzed by statistical analysis, key sensitivity analysis, key space analysis, differential analysis and encryption rate analysis. All the experimental results suggested that the encryption scheme is efficient and highly secure. Patidar *et al.*, [9] proposed a permutation-substitution based image encryption scheme consisting of three processes: preliminary permutation, substitution and main permutation. The image encryption scheme demonstrated strong robustness and great security. To yield excellent key sensitivity and plaintext sensitivity, both preliminary permutation and main permutation are designed to be dependent on the plain-image and controlled through the pseudo-random number sequences (PRNS) generated from the chaotic standard map. The substitution process is initialized with the initial vectors generated via the cipher keys and chaotic standard map. The results showed good resistance against differential analysis. Thampi and Jose [10] suggested a scheme to encrypt color image depends on 3D chaotic maps. Initial conditions for 3D maps are produced with a method involving three keys. The randomly generated keys employed for encryption purpose. 3D maps offer higher security and randomness in comparison with 1D and 2D maps.

III. PROPOSED METHODOLOGY

A chaotic system behavior cannot be predicted and it is composed of two steps: chaotic confusion and pixel diffusion. In the chaotic confusion stage, a combination of the chaotic maps is used to realize the confusion of all pixels. The parameters of the chaoticmaps are used for the confusion key. In the pixel diffusion stage, a plain image permutes or the value ofeach pixel changes one by one with using of the chaotic confusion stage. The parameters of the diffusion function are used for the diffusion key[2]. Most of the schemes faced with some problems such as the lackof robustness and security. This research work proposes a chaotic image encryption scheme using Arnold's Cat Map (ACM). Arnold map is also called cat map. It is two-dimensional invertible chaotic map introduced by Arnold and Avez.The Arnold cat map has been used extensively in image cryptography due to its chaotic nature. When an image is transformed, its original pixel organization is randomize and original pixel positions are restored after a number of iterations.The 2D generalized Arnold map shows excellent chaotic features, such asergodicity, pseudo-randomness, and sensitivity to initial conditions and control parameters.Confusion and diffusion property of the ACM makes it more suitable for image security, but the key of Arnold cat is smaller, and visual effects is also less than ideal. The drawbacks in 2D Arnold map are eliminated by using 3D Arnold map. Initial conditions for 3D maps are produced with a method involving three keys. The randomly generated keys employed for encryption purpose. 3D maps offer higher security and randomness. The classical 2D Arnold map is described byequation.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod N \quad (1)$$

which has two control parameter, P and Q. After performing the 2D Arnold scramblingit becomes x' and y'Where p and q are positive integers, (x ', y') is the new position of the original pixel position (x, y).In this proposed work, 3D cat map is used over a module of M as a finite system as in eq (2), where the vector [x', y', z'] is the scrambled position of the vector [x,y,z], where x, y is the coordinate position of the pixel value z. Pixels are placed in the position according to thefollowing process. 3D Arnold cat map is shown as Eq.2

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = CM * \begin{bmatrix} x \\ y \\ z \end{bmatrix} mod\ M \quad (2)$$

Logistic map is an example among nonlinear equation which can be applied on the experiment mathematic. Although it is simple, it can embody all the nature of nonlinearity phenomenon. The function is defined by the equation

$$X_{n+1=\int(\mu,X_n)=\mu X_n(1-X_n)} \quad (3)$$

Where μ ∈ [3.57 ,4], X n ∈(0 ,1). If μ =4 then the system is in chaotic state, and the system produces sequence with randomness, erotic and the sensibility to original value. All these characteristics can provide a very good shield for the image encrypt operation.

IV. EXPERIMENTAL ANALYSIS

The experimental evaluation of proposed image encryption is simulated by using MATLAB.

The test set is composed of 100 images with various characteristics, 10 of which are used to display the result. Different dimension of image such as 512*512, 256*256 and 128*128 are used.The proposed algorithm is analyzed based on the performance measures such as, number of pixel change rate [NPCR], unified average changing intensity [UACI] and computation time. The security key space of the 3D Cat Map consists of the type of edge detectors, threshold values, parameters and iteration times of the 3D Cat Map. Each of them has a sufficiently large number of possible variations. Therefore, the key space of the encryption algorithm is unlimited. The NPCR & UACI are quantitative and qualitative measures for the strength against possible differential attacks of image ciphers. For a secure transmission, NPCR score must be larger and UACI score must not be larger.

TABLE I COMPARISON OF NPCR

Number of Pixel Change Rate [NPCR]						
Images	**Arnold Map**			**Predictive Error Method**		
	512*512	**256*256**	**128*128**	**512*512**	**256*256**	**128*128**
Lena	98.2	83.4	77.6	91.6	83.5	72.4
Boat	98.8	85.2	78.6	94.6	85.1	73.4
Man	92.3	83.4	75.2	97.6	82.4	74.5
Satellite	96.3	88.6	73.6	91.6	85.4	75.2
Medical	98.6	88.4	76.6	94.6	81.2	71.6
Airplane	96.4	89.4	79.8	91.4	84.6	74.8
House	92.4	82.6	72.2	96.4	83.6	72.6
Baboon	98.5	88.4	76.5	97.8	87.9	74.6
Pepper	97.2	85.5	74.4	92.5	82.7	75.2
Bridge	96.2	82.6	72.4	94.3	89.4	73.5
Avg	96.49	85.75	75.69	94.24	84.58	73.78

A. Number of Pixel Change Rate [NPCR]

NPCR refers to the rate at which the pixels of the encrypted image are altered with the change of one plain image pixel.Table 1 shows the average of NPCR values and indicates that the sensitivity of the encrypted ciphers of 512 x 512 image is 96.49%,leading to the conclusion that the 3D Arnold map provides better encryption and it is very sensitive with respect to small pixel changes.

$$\mathrm{NPCR} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)$$

$$D(i,j) = \begin{cases} 0, & \text{if Im } o(i,j) = \text{Im } c(i,j) \\ 1, & \text{if Im } o(i,j) \neq \text{Im } c(i,j) \end{cases}$$

TABLE II COMPARISON OF UACI

Unified Average Changing Intensity [UACI]						
Images	**Arnold Map**			**Predictive Error method**		
	512*512	**256*256**	**128*128**	**512*512**	**256*256**	**128*128**
Lena	34.4	25.8	18.5	33.2	23.3	13.1
Boat	33.5	24.6	15.8	30.2	22.1	16.4
Man	31.2	25.8	14.4	32.2	20.4	17.7
Satellite	34.6	26.6	19.3	35	21.7	17.7
Medical	35.2	25.8	19.4	36.2	19.3	16.5
Airplane	30.2	22.5	18.6	35.4	21.9	16.7
House	33.4	27.5	20.2	30.4	19.9	19.4
Baboon	33.8	22.2	18.2	31.2	23.3	13.4
Pepper	32.8	28.2	18.8	30.4	23.1	15.5
Bridge	31.5	26.6	17.6	34.9	28.9	22.5
Avg	33.06	25.56	18.08	32.91	22.39	16.89

B. Unified Average Changing Intensity [UACI]

UACI measures the rate intensity of the variations between the plain and encrypted images. From table II, the higher value of UACI indicates the rate of one pixel change which shows that the Arnold map provides better encryption.

$$\mathrm{UACI} = \frac{100}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|\text{Im } o(i,j) - \text{Im } c(i,j)|}{255}$$

C. Computation Time

The computation time of encryption schemes are given in table III. It is found that the average computation time is stable for the two encryption schemes. From the analysis it is clear that the proposed Arnold map encryption shows better result.

TABLE III COMPARISON OF COMPUTATION TIME

COMPUTATION TIME [Seconds]						
Images	**Arnold Map**			**Predictive Error method**		
	512*512	**256*256**	**128*128**	**512*512**	**256*256**	**128*128**
Lena	2.675	1.812	0.879	2.267	1.203	0.398
Boat	2.736	1.202	0.486	2.567	1.601	0.745
Man	2.143	1.156	0.850	2.479	1.967	0.500
Satellite	2.062	1.022	0.354	2.343	1.467	0.513
Medical	2.683	1.043	0.442	2.912	1.789	0.856
Airplane	2.453	1.685	0.353	2.984	1.595	0.854
House	2.345	1.854	0.654	2.785	1.754	0.796
Baboon	2.456	1.725	0.352	2.865	1.385	0.565
Pepper	2.848	1.854	0.683	2.954	1.754	0.754
Bridge	2.442	1.643	0.582	2.174	1.854	0.865
Avg	2.4843	1.4996	0.5635	2.633	1.6369	0.6846

V. CONCLUSION

A new chaotic image encryption method using 3D Arnold map is proposed in this research work. It is observed that the proposed 3D Arnold map gives greater scrambling choices than the existing methods. This results in more chaos and better encryption by providing a larger key space. The satisfactory NPCR and UACI values show that the encryption provides better security. The Arnold method combines good confusion and diffusion properties and analysis shows that the Arnold cryptosystem has higher security due to an extremely large key space. Simulation analysis shows that the encryption algorithm has strong keys, better encryption and fast computation.

REFERENCES

[1] Joshua C. Dagadu, Jianping Li, Emelia O. Aboagye, Xuedzi Ge, "Chaotic Medical Image Encryption Based on Arnold Transformation and Pseudorandomly Enhanced Logistic Map", *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*., Vol. 4, No. 9, September 2017.

[2] Wei Zhou, Wen-Qi Liu, Dong-Liang Wang, Gui-Xiang Zhu, Ying-Jie Hu and Yong-Feng Zhan, "An Efficient Medical Image Protection Scheme with Parallel Chaotic Key Stream Generation", *Information Technology Journal*., Vol. 13, pp. 1602-1611, 2014.

[3] R. Purba, A. Halim and I. Syahputra, Enkripsi Citra Digital Menggunakan , "Arnold's Cat Map, Nonlinear Chaotic Algorithm", *JSM STMIK Mikroskil*., Vol. 15, No.2, pp. 61-71, 2014.

[4] EkoHariyanto, Robbi Rahim, "Arnold's Cat Map Algorithm in Digital Image encryption", *International Journal of Science and Research (IJSR)*, Vol. 5, No. 10, October 2016.

[5] Sridevi.P and Suguna.J, "An efficient Encryption Then Compression System using Asymmetric Numeral Method", *IJET*, Vol. 9, No 5, pp. 3680-3688, Oct-Nov 2017.

[6] M. Mishra, P. Singh, and C. Garg "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", *International Journal of Information and Computation technology*, Vol. 4, No. 7. pp. 741-746, 2014.

[7] A.Anto Steffi, and D. Sharma "Modified Algorithm of Encryption and Decryption of Image using Chaotic Mapping", *International Journal of Science and Research (IJSR)*, Vol. 2, No 2. pp. 77-80, 2013.

[8] Junqin Zhao, Weichuang Guo, RuisongYe,"A Chaos-based Image Encryption Scheme Using Permutation-Substitution Architecture", *International Journal of Computer Trends and Technology (IJCTT)*., Vol. 15 No. 4. pp. 174-185, Sep 2014.

[9] Vinod Patidar, N.K. Pareek, G. Purohit, K.K. Sud. "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption", *Optics Communications*., Vol. 284, No.19. pp. 4331-4339, 2011.

[10] Thampi,C.& Jose, D. "More Secure Color Image Encryption Scheme Based on 3D Chaotic Maps", *International Journal for Advance Research in Engineering and Technology*, Vol.1, No.9. pp. 1-5, 2015.