Available online at www.ijsrnsc.org

IJSRNSC

Volume-5, Issue-3, June 2017
Research Paper

Int. J. Sc. Res. in Network Security and Communication

www.ijsrnsc.org

ISSN: 2321-3256

Performance Analysis of Self Adaptive Image Encryption Technique

Rashmi P[1*], Bharathi R K[2], Shruthi Prabhakar[3], Reshma Banu[4], Rachana C R[5]

[1*]DoS in Computer Science, Pooja Bhagavat Memorial Mahajana Education Centre, Mysuru, India
[2] Dept. of MCA, Sri Jayachamarajendra college of Engineering, Mysore, India
[3]DoS in Computer Science, Pooja Bhagavat Memorial Mahajana Education Centre, Mysuru, India
[4] Dept. of ISE, GSSS Institute of Engineering and Technology for Women, Mysuru, India
[5] DoS in Computer Science, Pooja Bhagavat Memorial Mahajana Education Centre, Mysuru, India

Corresponding Author: rashmibdp@gmail.com

Received: 22nd May 2017, Revised: 08th Jun 2017, Accepted: 21st Jun 2017, Published: 30 Jun 2017

Abstract- This paper presents an efficient Self Adaptive Image Encryption Technique based on multiple chaotic maps. An efficient and fast encryption algorithm is designed with the help of traditional methods of permutation-diffusion and double simple 2D chaotic systems. Existing methods which are found in secure upon chosen-plain text or known-plain text attack in the process of permutation or diffusion. The key streams are dependent on the plain-image. Consequently, different plain-images will have different key streams in both processes. This design can solve the problem of fixed chaotic sequence produced by the same initial conditions but for different images. The mathematical experiments and performance analysis demonstrate that the proposed algorithm is large enough to resist the brute-force attack and has excellent encryption performance.

Keywords-Image Encryption, chaotic map, Permutation, Diffusion

I. INTRODUCTION

With the ever increasing growth of image transmission through computer networks especially the multimedia, internet and security of digital images has become a major concern. A secure computing environment would not be complete without considering encryption technology. Image encryption, in particular, is a challenging task due to some intrinsic properties like bulk data capacity, high storage redundancy, which are generally difficult to handle by traditional techniques. The image encryption is well known and it has extensive applications in multimedia systems, internet communication, medical imaging, tele medicine and so on. In spatial domain, the basic ideas for image encryption involves bit-wise permutation, pixel transformation etc. Among several existing methods the tree-structure based methods, chaos based methods and cellular automata based methods are most popular. During the past decades, there has been an increased interest in chaos based encryption. Because the characteristics of the chaotic maps have attracted the attention of cryptographers as they have many fundamental properties like periodicity, mixing and sensitivity to initial conditions so that good ciphers can be obtained. The two-dimensional or the high dimensional chaotic maps are usually employed to encrypt an image.

A chaos-based image encryption scheme typically comprises two processes: Permutation and substitution. Permutation involves confusion of pixels and diffusion just replaces a pixel by another value. The chaotic maps were achieved by using Logistic map, Cat map, Tent map, Baker map, etc. In the diffusion process pixel values are altered sequentially based on previous pixel values. The Fridrich architecture becomes the base for many chaos based image encryption schemes. There are varieties of approaches for permutation and diffusion process. Lian et al. [1] used the modified standard map for confusion step and tent map for diffusion. The origin point of standard map is taken as randomly selected point so that image can be well shuffled. In [2], dynamic S-boxes were designed to get block ciphers. Permutation is done with these block ciphers and Tent map is used here to generate the block ciphers whereas cyclic shifting operations are used in diffusion. In [3], a new cryptosystem based on Fridrich architecture is proposed in which bit-level permutation is performed. It replaces pixel wise permutation and is more secure as it alters not only the position but also the value. It employs cat map for bit-level permutation and Logistic map for diffusion. Wang et al. [4] used the chaotic structure for colour images and tried to encrypt the R, G, B components separately and also to reduce the correlation in order to increase the security.

II. LITERATURE REVIEW

In this section selected important contributions from the existing literature is discussed. Zhou YC, Bao L, Chen

CLP,[5] discussed a simple and direct way is to perform encryption on them, so that they can only be decrypted correctly with the correct key. As a result, how to efficiently provide security protection to these secret images has become an urgent issue.

Wang Y, Wong KW, Liao XF, Xiang T, Chen GR,[6] proposed different from text encryption, images have their intrinsic properties such as bulky data capacity, high redundancy, and high correlation between image pixels.

Fu C, Meng WH, Zhan YF, Zhu ZL, Lau FCM, Tse CK, Ma HF, [7]discussed that traditional techniques (for example, AES and IDEA) are not suitable for real-time encryption of images. To meet the challenge of image protection, there are many schemes proposed in recent years. We use those techniques for imageProtection.

Behnia S, Akhavan A, Akhshani A, Samsudin,[8] discussed that,to meet the challenge of image protection, there are many schemes proposed in recent years. We use those techniques for image Protection.

Zhu HG, Zhao C, Zhang XD [9] discussed various challenges in security related issues during data transfers. There are various security models following different enciphering techniques for the betterment of secured data transfer. Though there exist many complex cryptographic encryption algorithms, which provide high level of security, vulnerability of those algorithms increases day after a day.

Pareek NK, Patidar V, Sud KK, [10] discussed the various challenges facing in security related issues during data transfers. To meet the challenge of image protection, there are many schemes proposed in recent years. Among them, the chaos-based encryption algorithms have shown good efficiency. Maybe we should attribute this success to the characteristics of chaotic system itself such as parameter setting, random behaviour, and sensitivity to initial condition.

Sam IS, Devaraj P, Bhuvaneswaran RS,[11]describes security analysis of the BLP system is performed and presented. The BLP method combine pixel shuffling bit shuffling, and diffusion, which is highly, disorder the Plain image.

Ye GD, Wong KW,[12] describes several image encryption schemes based on chaotic maps have been proposed. Nevertheless, most of them hinder the system performance, security, and suffer from the small key space problem. This paper presents an efficient hybrid image encryption scheme based on a chaotic system that overcomes these disadvantages.

Ye RS,[13] adopting the classical permutation-diffusion architecture. This means that the whole encryption process is divided into two stages, i.e., permutation and diffusion to achieve high security for data.

Kocarev L, Jakimoski G, Stojanovski T, Parlitz U,[14] proposed a new image encryption scheme using a secret key is proposed. In the substitution process of the scheme, image is divided into blocks and subsequently into gray components. Each gray component is modified by performing operation which depends on secret key as well as a few most significant bits of its previous and next gray component.

Zhu CX,[15] proposed an encryption scheme with two rounds of diffusion only, the chaotic sequence was generated by a four-dimensional hyper chaotic system with four given initial conditions x0; y0, z0, and w0. Then the method did a pre-processing for the iterated values from the chaotic system to make a better statistical performance.

Li CQ, Liu YS, Xie T, Chen MZQ,[16],analysed the security of zhu proposed work and suggested a cryptanalysis method known-plaintext. They pointed out that the secret keys, which are used, could be found when two pairs of known plain-image and cipher-images are available.

Wang XY, Teng L, Qin X,[17] colour image encryption algorithm was introduced , which used only the Logistic map to generate the chaotic sequence with given initial conditions a; x0 and a1; y0. The iterated chaotic values were used for pixel scrambling and diffusion.

Arroyo D, Diaz J, Rodriguez FB, [18] discussed the successfully crypt analysed this scheme through a chosen-plaintext attack. The drawbacks of the cryptosystem were also analysed in detail in two aspects: (1) Small key space, and (2) Low sensitivity to the plain-image.

Abd El-Latif AA, Li L, Wang N, Han Q, Niu XM,[19] discussed the permutation is an operation of exchange the positions of the image pixels, of which can disturb and reduce the high correlation exist in the plain-image pixels.

The issues identified in the literature review for image encryption methods are,

1. Existing methods are inadequate security
2. Unsuitable key stream generation for image encryption
3. Image encryption with limited randomness.
4. Existing methods have not done Performance analysis of image Encryption (Entropy, MSE,NPCR, PSNR,UACI)

To overcome the existing techniques, proposed the proposed self-adaptive image encryption. The rest of this paper is organized as follows, the proposed self-adaptive image encryption algorithm is described in Section 3. Two updating mathematical models are established for the initial conditions of the system. Section 4 gives the numerical experiments using proposed algorithm. The performance analyses performed in Section 5 demonstrate the security and the efficiency. Finally, conclusions are drawn in Section 6.

III. PROPOSED METHOD

The model for proposed image encryption is shown in **Figure 1**. Input may be any coloured image (R, G, B pattern) and R, G, B pattern will be in the form of [m x m] matrix. This algorithm will make use the technique of permutation and diffusion process, which means that each pixel of the input image is replaced by an additional value. The value will be produced by using chaotic map. The proposed a image encryption algorithm which holds the self-adaptive method. In the permutation stage, the chaotic sequence for the circular shuffling is generated dependent on the plain-image. Furthermore, in the diffusion, the permuted image is divided into blocks. We choose the last block to update the initial conditions of the chaotic system. The output will be an encrypted image.

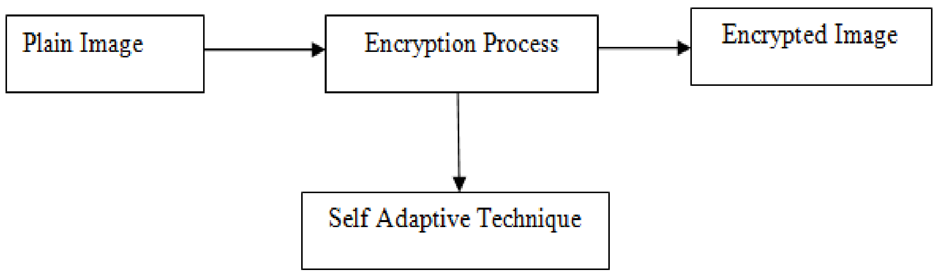


Figure 1: Block diagram of the Proposed Method

IV. MATHEMATICAL EXPERIMENTS

In this section, efficiency of the proposed algorithm is calculated by conducting the mathematical experiments. With initial conditionsx_0= 0.506; y_0= 0.878 and r_1 = 402 for 2D Logistic map, and x_0 =0.816; y_0= 0.447 and r_2 =6354for generalized Arnold map. Control parameters are μ_1=3.67; μ_2=3.97, γ_1=0.204; γ_2=0.142; a=2, and b=1. To deduce the computation, set $\emptyset_i$=0; i=1,2,3,4. Experiments are carried out by Matlab 7.0 using a platform of Windows 7 PC with an Intel(R) Pentium (R), 2.30 GHz CPU. All input RGB images are selected as mxm. The information entropy of the cipher-image can reach 7.99767.

V. PERFORMANCE ANALYSIS

The performance analyses are carried out using histogram analysis, correlation coefficient analysis, information security analysis, Differential Attack Analysis, MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio).

a. Histogram Analysis

Histogram is a test to showcase the distribution of pixels in the image. It also examines the possible contrast between the plain image and cipher image distribution in histogram. The cipher image histogram is widely uniform and flat distribution. The plain image histogram has some peaks and it is unevenly distributed. Even if another image is considered it would also be subjected to a difference in distribution. It is observed that, **Figure 4** shows that histogram of encrypted images is uniformly distributed. The cipher image histogram is uniformly distributed and nothing can be extracted. The information obtained from the encrypted image in histogram is uniformly distributed and this algorithm withstands statistical attacks.

b. Correlation Coefficient Analysis

Histogram is an important statistical feature of digital image. An ideal secure image encryption should produce the encrypted images with uniform histograms. Strong correlation of two adjacent pixels is normally found in every meaningful plain-image. A good encryption algorithm should have the ability to remove and reduce this correlation. We randomly choose pairs of adjacent pixels in vertical, horizontal and diagonal directions, and calculate the correlation coefficient by Eq. (1) [20, 21].The values of the correlation coefficients are listed in Table 1 after applying the proposed encryption method. Therefore, we conclude that the proposed algorithm ....(1) exhibits us a good performance in practice.

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

TABLE 1: CORRELATION COEFFICIENTS BETWEEN ADJACENT PIXELS FOR DIFFERENT IMAGES

Test Image	**Adjacency**	**Correlation Coefficients**	
		Plain Image	Encrypted Image
Test Image 1	Horizontal	0.9659	0.0760
	Vertical	0.9502	0.0904
	Diagonal	0.905	0.0941
Test Image 2	Horizontal	0.9947	0.0020
	Vertical	0.9777	0.1080
	Diagonal	0.9778	0.1109
Test Image 3	Horizontal	0.9722	0.0343
	Vertical	0.9734	0.0585
	Diagonal	0.9735	0.0617
Test Image 4	Horizontal	0.9280	0.0142
	Vertical	0.9589	0.0151
	Diagonal	0.9591	0.0190
Test Image 5	Horizontal	0.9895	0.0085
	Vertical	0.9875	0.0360
	Diagonal	0.9876	0.0401

TABLE 2: COMPARISON WITH CORRELATION COEFFICIENTS WITH OTHER ALGORITHMS

Algorithm	**Correlation Coefficients**		
	Horizontal	**Vertical**	**Diagonal**
Proposed Algorithm	0.0760	0.0904	0.0941
Zhou et al.(25)	-0.00009	-0.00005	0.00072
Gao & Chen 2008 (28)	-0.0142	-0.0074	-0.0183
Tedmori & Al Najdawi (29)	0.0023	0.0042	0.0053

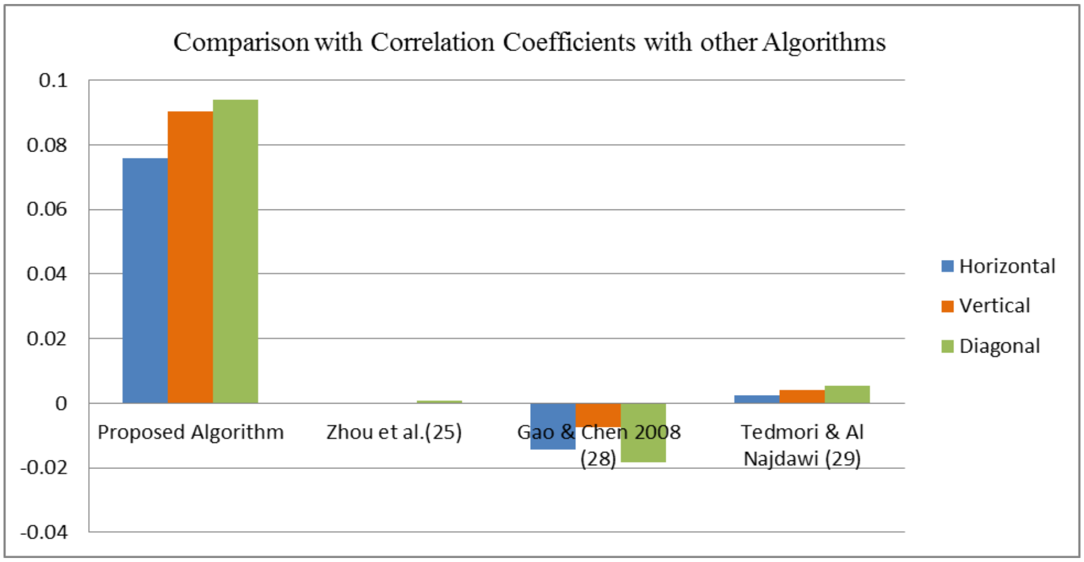


Figure 2: Comparison with Correlation Coefficients with other Algorithms

Table 2 compares the Correlation coefficient of the proposed algorithm with the existing algorithm. It is observed that the original plain image is highly correlated and the encrypted image has less correlation. The propped algorithm has lesser correlation among the pixels in comparison with other algorithms. The graphical representation for the same depicted in Figure 2.

Information entropy analysis

In information theory, entropy is the most significant feature of disorder, or more precisely unpredictability. To calculate the entropy H(X) of a source x, we have:

$$H(X) = \sum_{i=1}^{n} Pr(x_i) \log_2 \frac{1}{Pr(x_i)}$$

where X denotes the test image, xi denotes the ith possible value in X, and Pr(xi) is the probability of X =xi, that is, the probability of pulling a random pixel in X and its value is xi. For a truly random source emitting 2N symbols, the entropy is H(X) =N. therefore, for a ciphered image with 256 gray levels, the entropy should ideally be H(X) =8. If the output of a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security.

Mean Square Error

Mean squared error (MSE) is defined as an average of the square of the difference between actual image and encrypted image. The MSE is given by the equation,

$$\text{MSE} = \frac{1}{\text{MxN}} \sum_{i=1}^{n} \sum_{j=1}^{n} (x(i,j) - y(i,j))^2$$

Where x (i, j) represents the original image and y (i, j) represents the encrypted image and i and j are the pixel position of M x N image.

MSE is zero when x (i, j) =y (i, j).

Number of Pixel Change Rate (NPCR):

If C1 and C2 are original image and encrypted image respectively. C_1 (i, j) and C_2 (i, j) are original image pixel and encrypted image pixel respectively. The NPCR is then defined as [31, 32].

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{\text{MxN}} \text{ X } 100\%$$

Where, D is bipolar array.

$$D(i,j) = \begin{cases} 1, & C1(i,j) \neq C2(i,j) \\ 0, & \text{otherwise} \end{cases}$$

Peak Signal to Noise Ratio (PSNR)

The peak signal to noise ratio is evaluated in decibels and is inversely proportional to MSE. It is given by the equation

$$\text{PSNR} = 10 \log_{10}\left(\frac{255}{\text{MSE}}\right)$$

Unified average changed intensity (UACI)

It is used measure the intensity rate difference between the original image and encrypted image.[31,32]

$$\text{UACI} = \frac{1}{N}\left[\sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{255}\right]$$

If C_1 and C_2 are original image and encrypted image respectively. C_1 (i, j) and C (i , j) are original image pixel and encrypted image Pixel respectively.

TABLE 3: PERFORMANCE ANALYSIS FOR DIFFERENT IMAGES.

Parameter	Test Image 1	Test Image 2	Test Image 3	Test Image 4	Test Image 5
Entropy plain image	6.0251	7.7509	7.2642	6.9930	6.8186
Entropy encrypted image	7.9324	7.9950	7.9859	7.9900	7.9796
NPCR	99.6353	99.5850	99.5773	99.6246	99.5819
UACI	43.8496	33.9282	30.8771	34.7622	34.7497
MSE	200.3046	88.8432	75.8053	156.0209	159.0056
PSNR	25.1139	28.6446	29.3338	26.1990	26.1167

TABLE 4: COMPARISON OF SPEED FOR DIFFERENT SIZES

Image size	System Characteristics	Ref. [20]	Ref. [27]	Proposed Method
256x256	Intel (R) Pentium (R),2.30 GHz CPU	0.07020	0.30420	0.517836
512x512	Intel (R) Pentium (R),2.30 GHz CPU	0.25740	1.15441	0.521022
1024x1024	Intel (R) Pentium (R),2.30 GHz CPU	0.99841	4.63323	0.511666

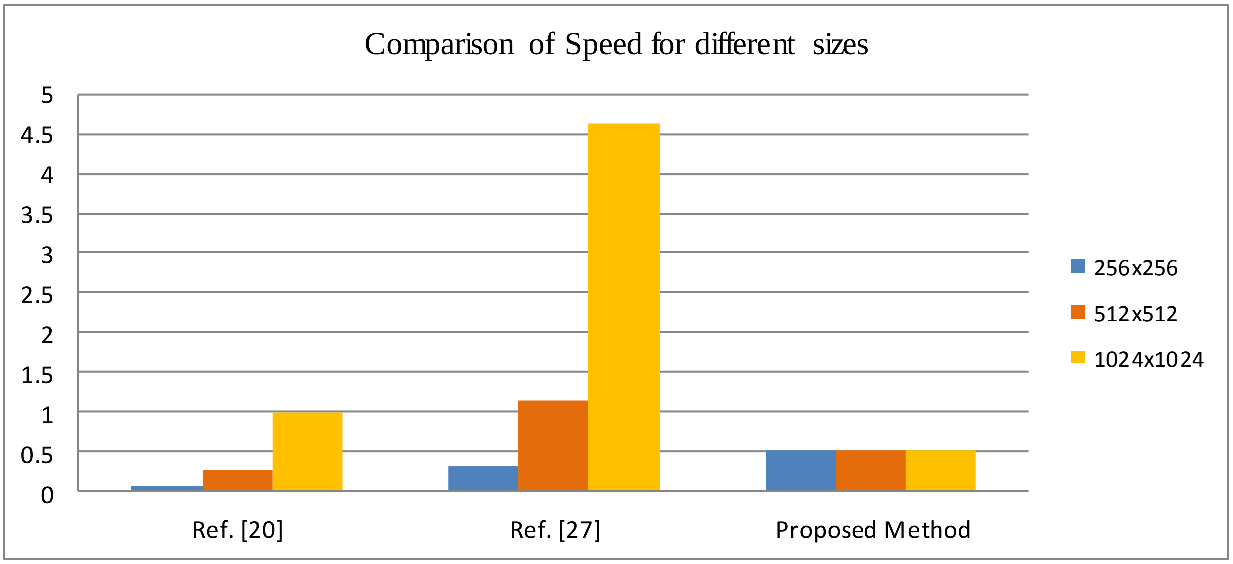


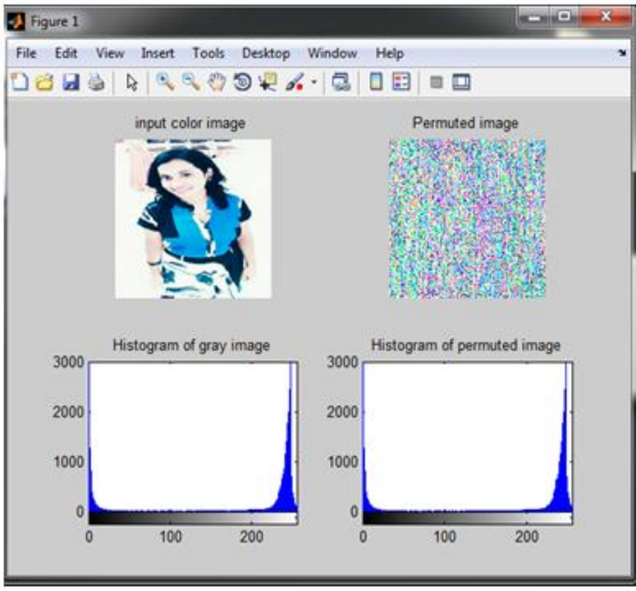
Figure 3: Comparison of Speed for different sizes

TABLE 5: DEPENDENCY ON THE PLAIN-IMAGE.

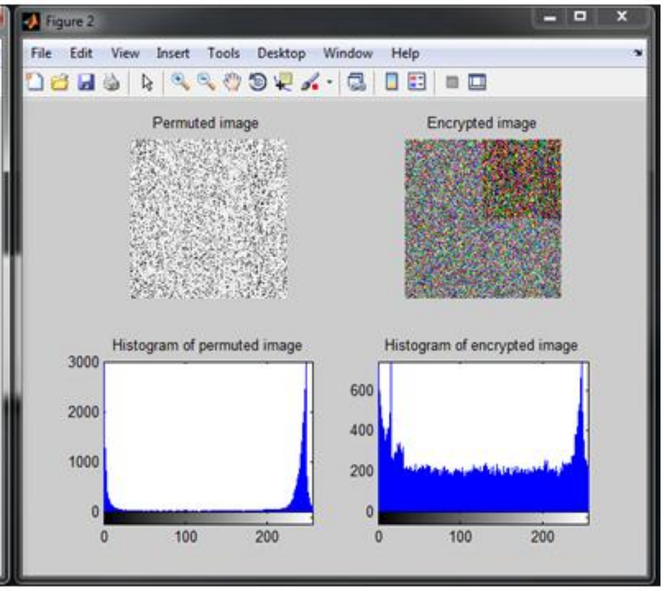
Methods	Ref. [6]	Ref. [27]	Ref. [30]	Ref. [9]	Ref. [31]	Proposed Method
Permutation Stage	No	__	No	No	No	Yes
Diffusion Stage	No	YES	YES	YES	No	Yes

Table 4 list the time cost of different algorithms using various images. The data show that a faster speed is achieved by using proposed method. The graphical representation for the same depicted in **Figure 3.**

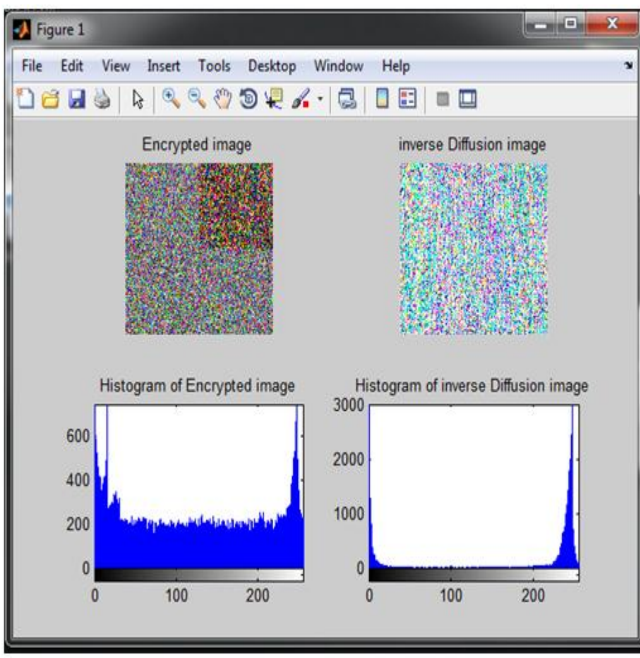
Test Image 1:



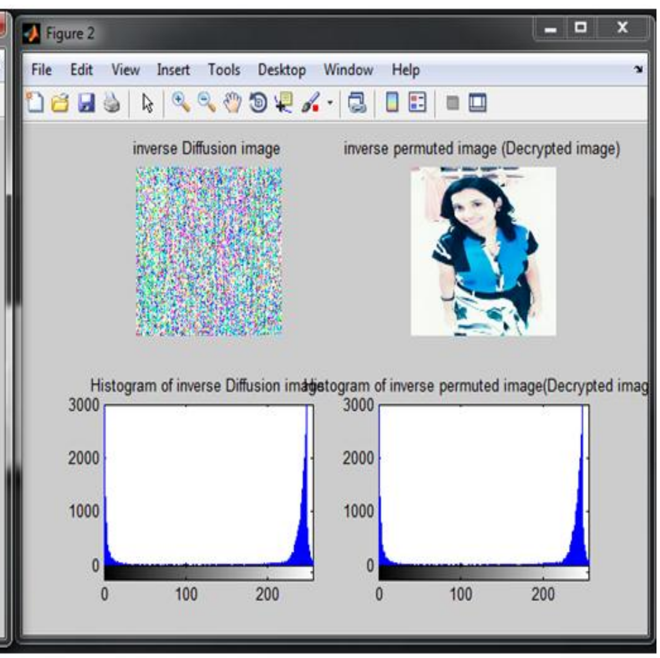
Permuted Image



Encrypted image



Inverse diffusion process



Decrypted image

Test Image 2:

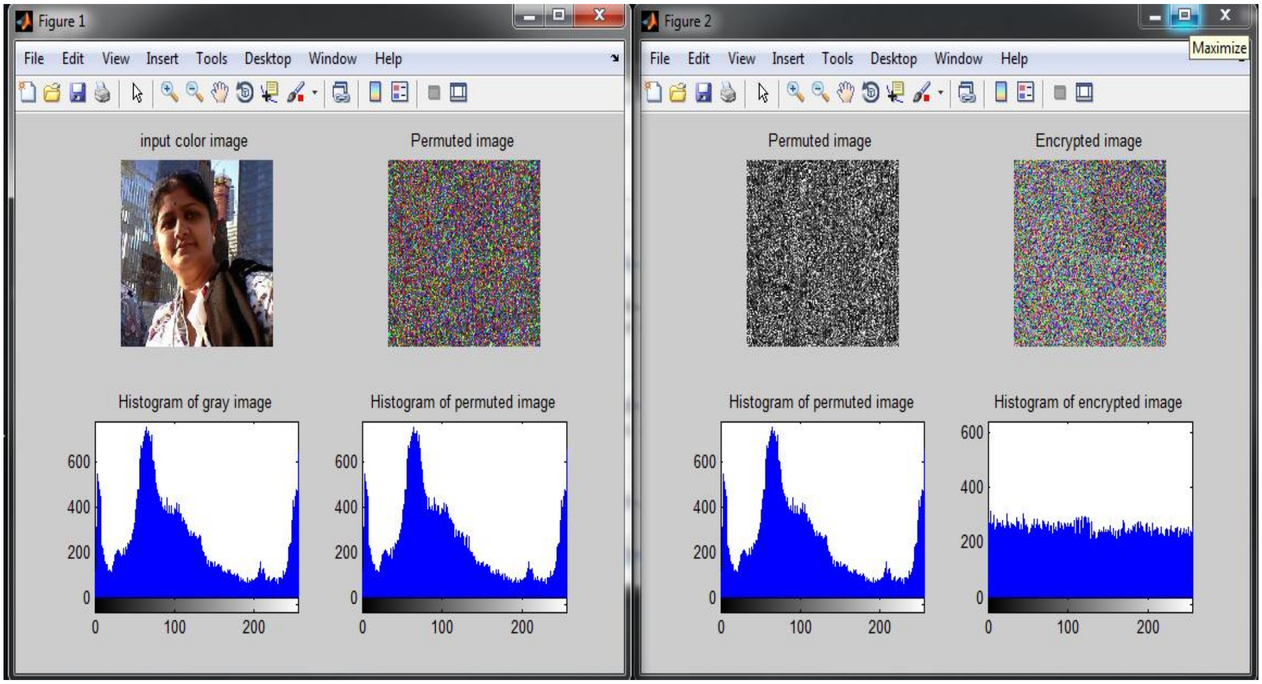


Figure 1
File Edit View Insert Tools Desktop Window Help
input color image
Permuted image
Histogram of gray image
Histogram of permuted image
Figure 2
Maximize
Permuted image
Encrypted image
Histogram of permuted image
Histogram of encrypted image

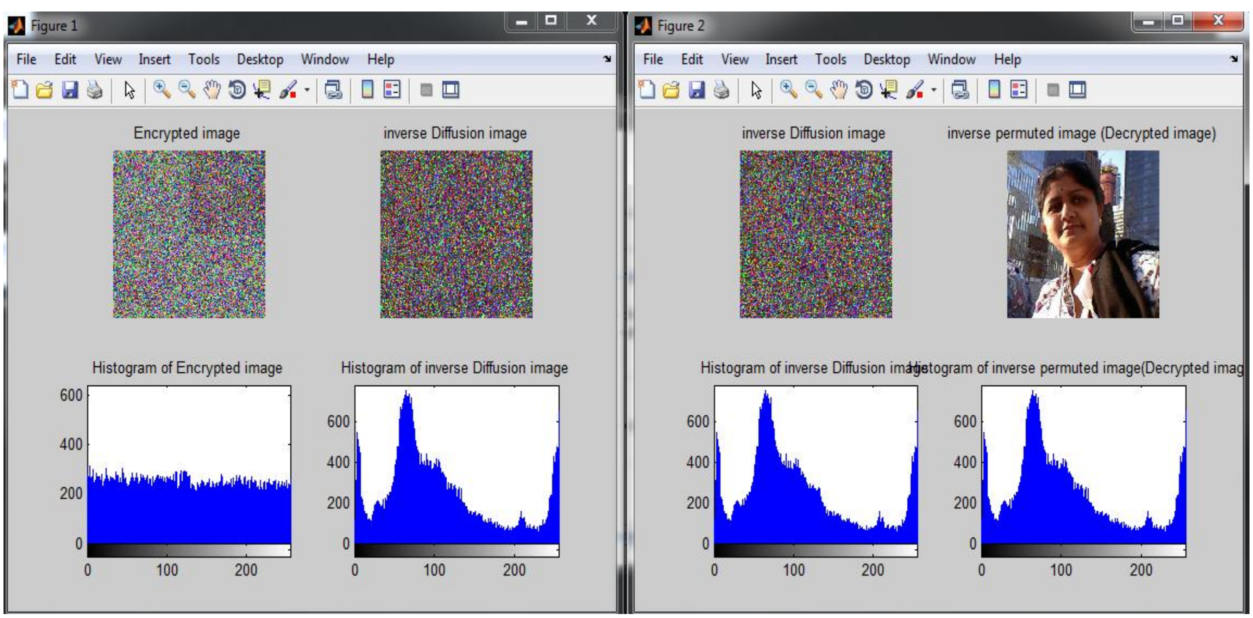


Figure 1
File Edit View Insert Tools Desktop Window Help
Encrypted image
inverse Diffusion image
Histogram of Encrypted image
Histogram of inverse Diffusion image
Figure 2
inverse Diffusion image
inverse permuted image (Decrypted image)
Histogram of inverse Diffusion image
Histogram of inverse permuted image(Decrypted imag

Test Image 3:

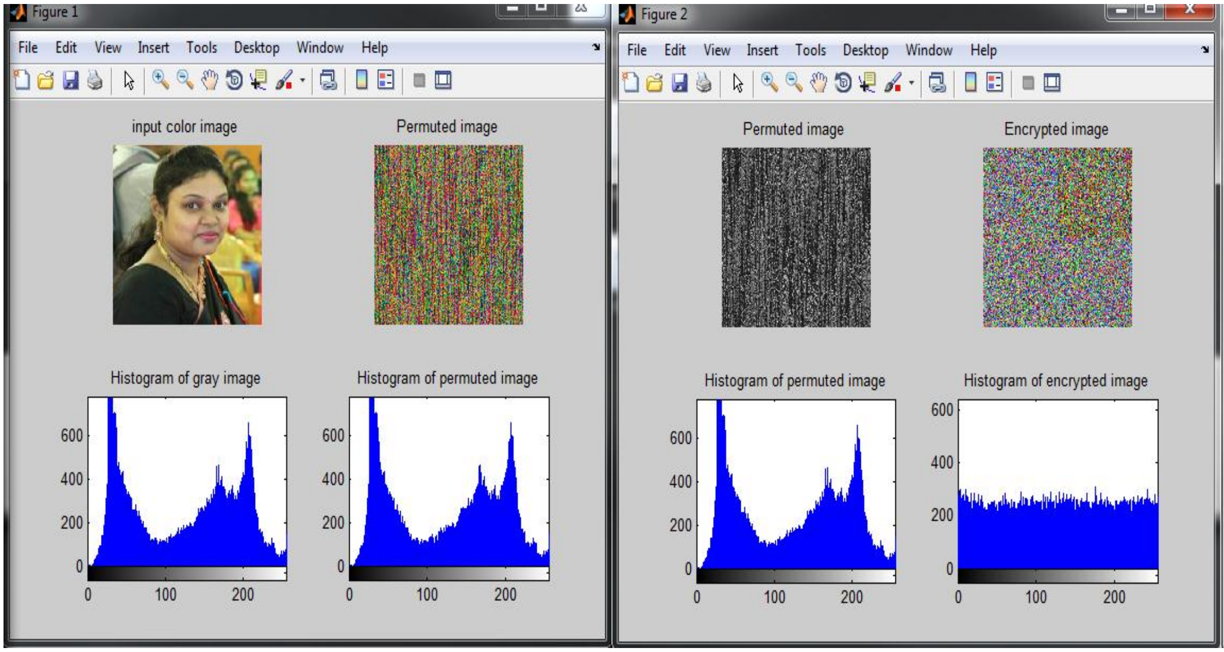


Figure 1
File Edit View Insert Tools Desktop Window Help
input color image
Permuted image
Histogram of gray image
Histogram of permuted image
Figure 2
Permuted image
Encrypted image
Histogram of permuted image
Histogram of encrypted image

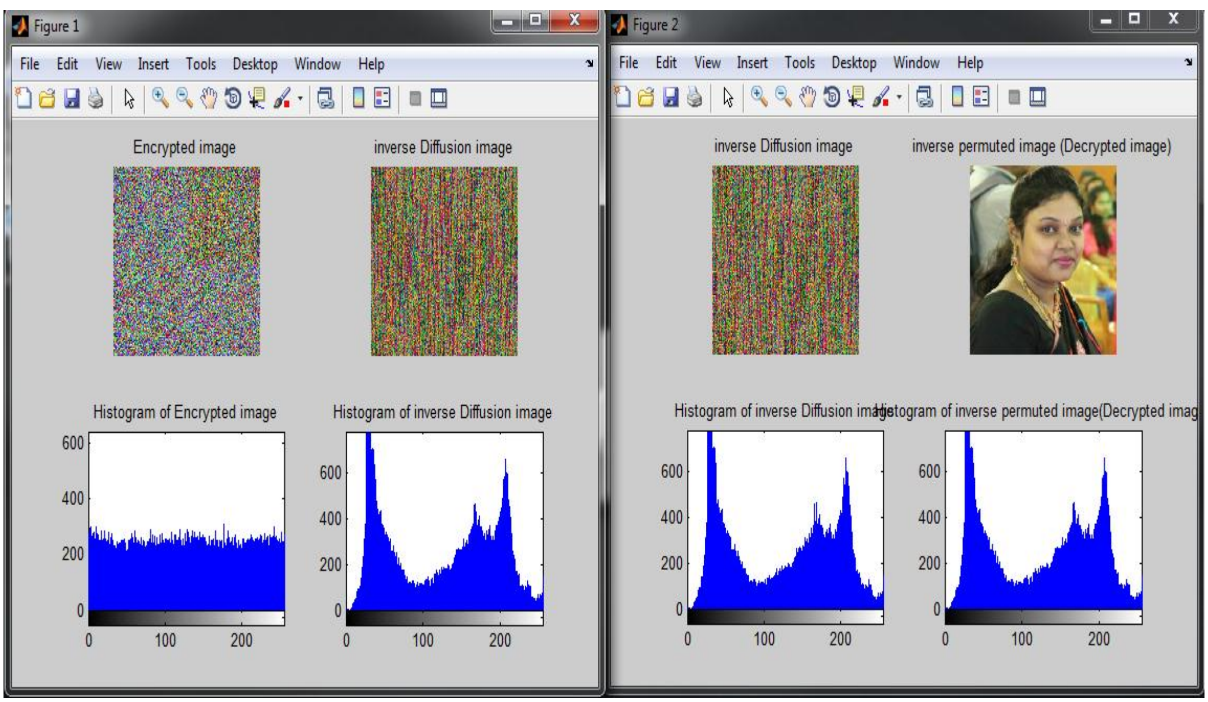
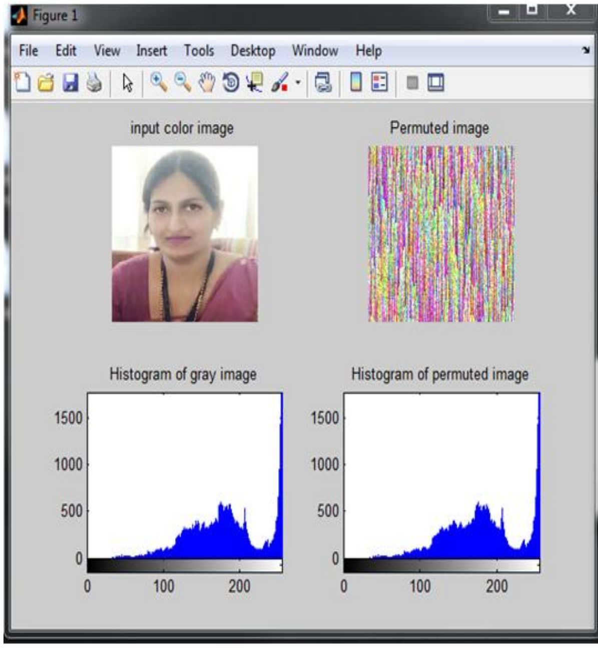
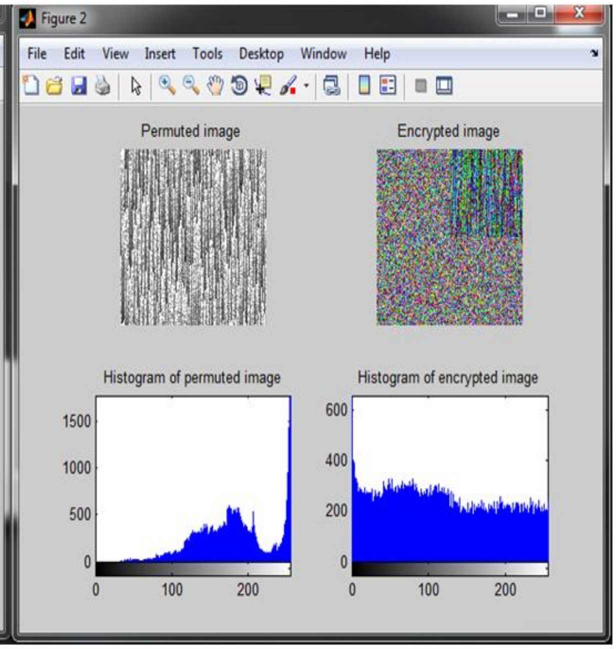


Figure 1
Encrypted image
inverse Diffusion image
Histogram of Encrypted image
Histogram of inverse Diffusion image
Figure 2
inverse Diffusion image
inverse permuted image (Decrypted image)
Histogram of inverse Diffusion image
Histogram of inverse permuted image(Decrypted imag

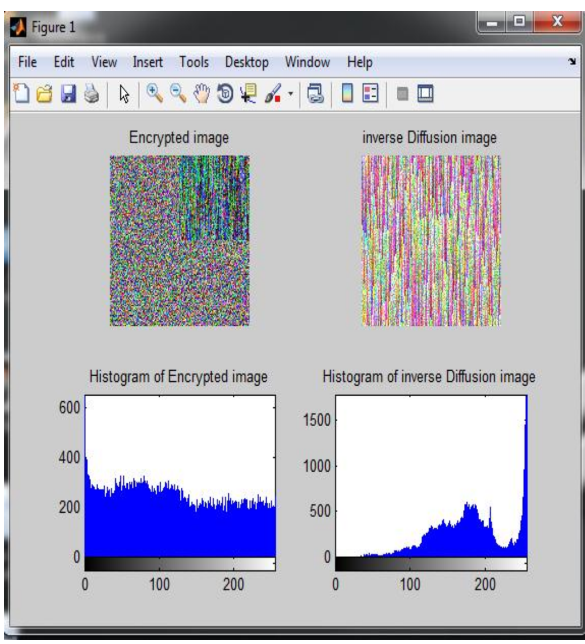
Test Image 4:

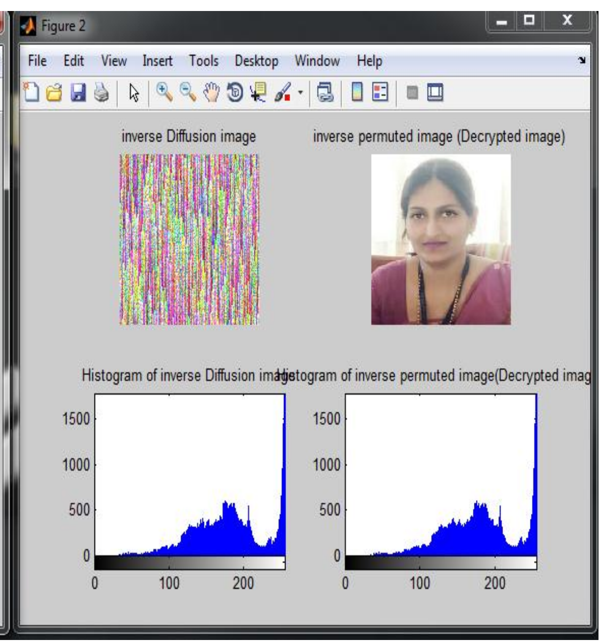


Permuted Image



Encrypted image





Test Image 5:

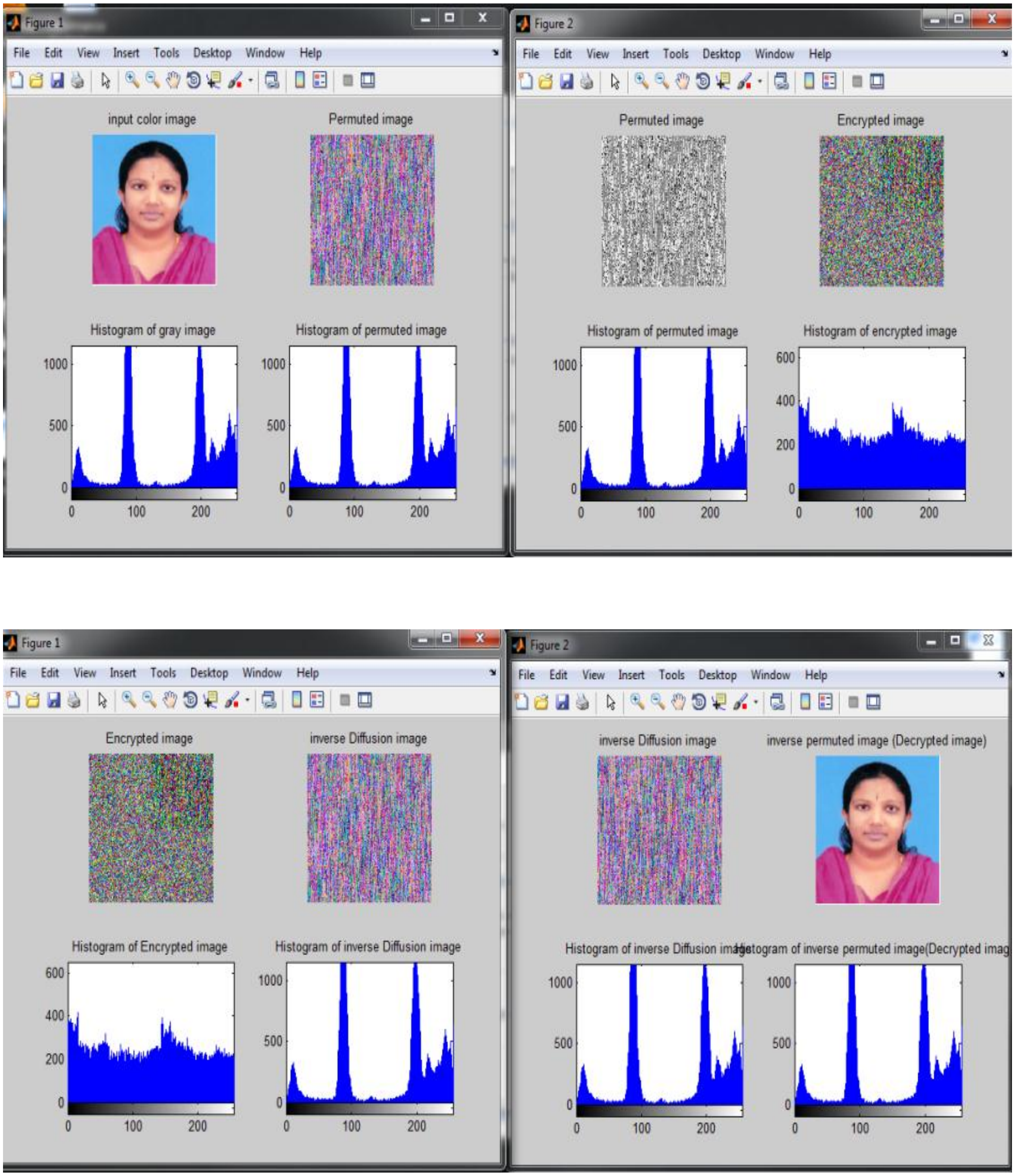


Figure 4: Experimental Results for Different Test Images

VI. CONCLUSION

In this paper, a novel self-adaptive chaotic image encryption algorithm is proposed. The key streams generated in both the processes of permutation and diffusion are dependent on the plain-image. Traditional methods consider diffusion only. Block method is introduced in the encryption process with fast computation. High-dimensional complex partial equations are avoided. Self-adaptive update models are designed automatically for keys according to the original images. Simulation results show that the NPCR, UACI, and information entropy are better than those of a comparable cryptosystem. All these results justify the superior security and computational efficiency of our cryptosystems.

ACKNOWLEDGMENT

The work described in this paper is supported by **Dr. C K Renukarya**, Director, Pooja Bhagavat Memorial Mahajana Education Centre, Mysuru. I am grateful to **Smt. Rachana C R**, Associate Professor & HOD, DoS in Computer Science, Pooja Bhagavat Memorial Mahajana Education Centre, Mysuru for providing me the opportunity to undertake this project.

REFERENCES

[1]. ShiguoLian, Jinsheng Sun and Zhiquan Wang ang, "*A Block Cipher based on a suitable use of the Chaotic Standard Map*", Chaos Solitons and Fractals, Vol. 26, No. 1, pp.117-129, 2005.

[2]. Yong Wang, Kwok-Wo Wong, Xiaofeng Liao, Tao Xiang, "*A Block Cipher with Dynamic S-boxes based on Tent Map*", Communications in Nonlinear Science and Numerical Simulation, Vol. 14, No. 7, pp. 3089-3099, 2009.

[3]. Zhi-liang Zhu, Wei Zhang, Kwok-wo Wong and Hai Yu, "*A Chaos-based Symmetric Image Encryption scheme using a Bit-Level Permutation*", Information Sciences, Vol.181, No.6, pp. 1171-1186, 2011.

[4]. Xingyuan Wang, Lin Teng, Xue Qin, "*A Novel Colour Image Encryption Algorithm based on Chaos*", Signal Processing, Vol. 92, No. 4, pp. 1101-1108, 2012.

[5]. Zhou YC, Bao L, Chen CLP, "*Image encryption using a new parametric switching chaotic system*", Signal Process, Vol.93, Issue.11, pp.3039-3052, 2013.

[6]. Wang Y, Wong KW, Liao XF, Xiang T, Chen GR., "*A chaos-based image encryption algorithm with variable control parameters*", Chaos Solitons Fract, Vol.41, Issue.4, pp.1773-1783, 2009.

[7]. Fu C, Meng WH, Zhan YF, Zhu ZL, Lau FCM, Tse CK, Ma HF, "*An efficient and secure medical image protection scheme based on chaotic maps*", ComputBiol Med, Vol.43, Issue,8, pp.1000–1010, 2013.

[8]. Behnia S, Akhavan A, Akhshani A, Samsudin A, "*Image encryption based on the Jacobian elliptic maps*", J SystSoftw, Vol.86, Issue.9, pp.2429-2438, 2013.

[9]. Zhu HG, Zhao C, Zhang XD., "*A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem*, Signal Process Image Commun, Vol.28, Issue.6, pp.670-80, 2013.

[10]. Pareek NK, Patidar V, Sud KK., "*Diffusion-substitution based gray image encryption scheme*", Digital Signal Process, Vol.23, Issue.3, pp.894-901, 2013.

[11]. Sam IS, Devaraj P, Bhuvaneswaran RS., "*An intertwining chaotic maps based image encryption scheme*", Nonlinear Dyn, Vol.4, Issue. 69, pp.1995-2007, 2012.

[12]. Zhang X, Wang C, Zheng Z., *"An Efficient Chaotic Image Encryption Algorithm Based on Self-adaptive Model and Feedback Mechanism*", KSII Transactions on Internet and Information Systems, Vol.11, Issue.3, pp.1-9, 2017.

[13]. Ye RS., "*A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism*", Opt Commun, Vol.284, Issue.22, pp.5290-5298, 2011.

[14]. Kocarev L, Jakimoski G, Stojanovski T, Parlitz U., "*From chaotic maps to encryption schemes*", In IEEE International Symposium on Circuits and Systems, Monterey, p.514-517, 1998.

[15]. Zhu CX., "*A novel image encryption scheme based on improved hyperchaotic sequences*", Opt Commun, Vol.285, Issue.1, pp.29-37, 2012.

[16]. Li CQ, Liu YS, Xie T, "*Chen MZQ. Breaking a novel image encryption scheme based on improved hyperchaotic sequences*", Nonlinear Dyn, Vol.73, Issue.2, pp.2083-2089, 2013.

[17]. Wang XY, Teng L, Qin X., "*A novel colour image encryption algorithm based on chaos*", Signal Process, Vol.92, Issue.4, pp.1101-1108, 2012.

[18]. Arroyo D, Diaz J, Rodriguez FB. Cryptanalysis of a one round chaos-based substitution permutation network. Signal Process 2013;93:1358–64.

[19]. Abd El-Latif AA, Li L, Wang N, Han Q, Niu XM., "*A new approach to chaotic image encryption based on quantum chaotic system, exploiting colorspaces*", Signal Process, Vol.93, Issue.11, pp.2986–3000, 2013.

[20]. Norouzi B, Mirzakuchaki S, Seyedzadeh SM, Mosavi MR., "*A simple, sensitive and secure image encryption algorithm based on hyper-chaotic systemwith only one round diffusion process*", Multimedia Tools Appl., Vol.71, Issue.3, pp.1469-1672, 2014

[21]. Huang XL., "*A designed image encryption algorithm based on chaotic systems*", J ComputTheorNanosci, Vol.9, Issue.2, pp.2130-2135, 2012.

Authors Profiles

Rashmi P is currently studying MSc in Computer Science at Department of Studies, Post- Graduate Wing of SBRR Mahajana First Grade College, K.R.S Road, Metagalli, Mysuru. She worked as a Technical staff in the Department of Computer Science and Engineering at JSS Academy of Technical Education, Mauritius. She obtained her Bachelor of Computer Applications from BMS College for Women's, Bangalore, affiliated to Bangalore University, Bangalore. She was presented papers in various National/International Conferences.

Dr.R.K.Bharathi is working as Associate Professor Department of MCA, Sri Jayachamarajendra college of Engineering., (SJCE) Mysore. She has 20 years of teaching experience in Computer Science (including 12 years of research experience and 2 years of Industry experience). She obtained MCA and M.Sc, Technology (By Research) from University of Mysore, Mysore and PhD from Mangalore University, Mangalore. She is the Research Supervisor at JSS Research Foundation, Affiliated to University of Mysore, Mysore and

Visveswaraiah Technological University, Belagavi, Karnataka. She has served as a member of Board of Examinations at various boards. She has presented/published several Research papers in International, National Journals/Conferences. Guiding student projects of 25 credits to MCA students. Organized many National level workshops and Conferences. Completed many funded projects. Her areas of interest and research include Document Image Analysis and Pattern Recognition,

Dr. Reshma Banu working as an Professor & HOD in the Department of ISE, GSSS Institute of Engineering and Technology for women, Mysuru. She Represented Dept. of ISE during NBA Visit. She succeeded in Getting NBA Accreditation by New Delhi, India, for the Information Science & Engineering Dpt. for 3 years. (Validity: 01-07-2017 to 30-06-2020). She is having 16 years of Teaching and Research Experience. Currently Nominated as Coordinator for implementation of ICT initiative's to VTU from GSSSIETW, Mysuru. She has won the Young Scientist Award from AUFAU,VIRA-2016 for the Initiatives, Discoveries and Developments in the discipline of Wireless Communication Networks. Session chair & committee member for various International and National conferences. Organized several National Level Competition / Certification Workshop/ Conferences/ FDP/ Technical Session/ Seminar/ Student Convention/ Technical talk. Successful in getting KSCST funded project for the dept sanctioned for the year 2017. She was the Organizing Chair for IEEE International Conference- 2016, at GSSSIETW-Mysuru. She is nominated as Special Session Co-ordinator for Elsivier Conference, International Conference on Advanced Material Technologies (ICAMT)-2016 organized by Indo American Institutions - Technical Campus(IAITC), Visakhapatnam, Andhra Pradesh, India. Editorial board Member for International Journal of Engineering And Robot Technology. She is one of the Reviewer for The Fifth International Conference on Cyber Security, Cyber Welfare and Digital Forensic (CyberSec2017). She is the Nodal Co-Ordinator for BITES (Board of IT education Standards) at GSSSIETW-Mysuru. She is Examiner/valuator/ Paper setter for Visvesvaraya Technological University, Belagavi. She has published nearly 40 Research papers in International, National Journals/conferences. She is a Member of IEEE,CSI, IAENG, IBM Academic Initiative, and LM ISTE.

Smt. Shruthi S Prabhakar is working as Assistant Professor in the Department of Studies in Computer Science, Post- Graduate Wing of SBRR Mahajana First Grade College, K.R.S Road, Metagalli, Mysuru which is affiliated to University of Mysore. She has 4 years of teaching experience in Computer Science. She obtained her B.E in Computer Science and Engineering and M. Tech in Computer Network Engineering from VTU, Belgavi. She has presented/published several Research papers in International, National Journals/Conferences. She has guided many projects for PG Students. Her areas of interest and research include mobile communication, Database management Systems and web Programming.

Smt. Rachana C R is working as Associate Professor & Head in the Department of Studies in Computer Science, Post- Graduate Wing of SBRR Mahajana First Grade College, K.R.S Road, Metagalli, Mysuru which is affiliated to University of Mysore. She has 14 years of teaching experience in Computer Science. She obtained her B.E in Computer Science and Engineering from Adichunchanagiri Institute of Technology, Chikmagalur and M. Tech in Computer Network Engineering from National Institute of Engineering, Mysuru, affiliated to Visvesvaraya Technological University, Belgavi. She has completed her M.Phil.in Computer Science. She is currently pursuing her research in the area of 'Security Issues in Cloud Computing' at VTU, Belagavi. She is serving as a reviewer of 'The European Journal of Engineering Education'. She has served as a member of Board of Examinations at various boards. She has presented/published several Research papers in International, National Journals/Conferences. She is a Member of Institution of Engineers (India), Computer Society of India, International Association of Engineers (IAENG), International Association of Computer Science and Information Technology (IACSIT). She has delivered a number of special lectures in the area of Computer Science and Soft Skills at various institutions. Her areas of interest and research include Cloud Computing Security, Web Programming, Peer-to-Peer computing, Personality Development and Soft skills and Electronic Commerce.

