International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 13, Number 2 (2017), pp. 273-284

http://www.ripublication.com

Comparative Analysis of Various İmage Encryption Techniques

Shikha Jaryal
Department of Computer Engineering and Technology,
Guru Nanak Dev. University, Amritsar, Punjab, India.

Chetan Marwaha
Department of Computer Engineering and Technology,
Guru Nanak Dev. University, Amritsar, Punjab, India.

Abstract

Encryption and decryption which are devoted to biological hard problems, is preferable to those which are based on mathematical ones. Although image encryption based on DNA (deoxyribonucleic acid) cryptography is an immature, and has its own significance in research area. This paper presents a various encryption algorithms that are based on bit level scrambling, cyclic shift & swapping, chaotic maps, DNA coding, compressed sensing. In this paper, the comparison of various encryption techniques is discussed that has been carried out on key space and speed. So, the study shows that the various techniques which were used are secure & reliable and also brings the attention towards the performance of these algorithms.

Keywords: Image encryption, DNA cryptography, Bit level, Compressive sensing, Chaos theory, Cyclic shift & swapping.

1. INTRODUCTION

Nowadays, electronic services and devices comprise of additional functions of storing and transmitting multimedia messages. Digital image information exchange have increased so rapidly, so security has become an essential issue to consider for safe transmission. To make the transmission secure over the internet, encryption of image is very important.

1.1 Image Encryption

Encryption is a procedure of hiding the information, when the information is transferred through a network. Image security is distinct from text security with some inherent characteristics for example- mass information capacity and greater relationship among pixels. That is why conventional encryption algorithm such as for example international data encryption algorithm (IDEA), data encryption standard (DES), and advanced encryption standard (AES) are no longer sufficient for image encryption [1].There are several techniques like Steganography [2], Watermarking, and Visual cryptography techniques are employed from ancient age to till date for the security of images. Several new methods have now been proposed applying various practices and calculations. Few of those are chaotic system [3-13], optical transform [14], DNA cryptography [15-18], compressive sensing [19-20].

- **Chaos Theory** - Chaos theory explains the behavior of specific nonlinear dynamic system that shows dynamics under certain conditions which are deterministic and unpredictable.
- **DNA Cryptography** -DNA cryptography is an evolving technique which perform operations on methods of DNA computing. Biological structure of deoxyribonucleic acid (DNA) contains nucleotides named as Adenine(A), Cytosine(C), Guanine(G) and Thymine(T). DNA cryptography is focussed on utilising DNA sequences to encode binary data in certain sort or another.

Advantages of DNA computing:

- Speed : Combining DNA strands made the computations 100 times quicker compared to the quickest computer.
- Stroage requirement : The storage density of DNA memory is approximate 1 bit per cubic nanometer whereas conventional computer requires 1012bit per cubic nanometer.
- Power requirement : DNA computing does not require outside power source.
- **Compressive sensing** - In [22], it is a signal sampling technique which could directly acquires a condensed representation with almost negligible loss of information through dimensionality reduction when data is compressible. We are able to reconstruct images and sometimes even exactly from a number of samples which is far smaller than the specified resolution of image.

2. GENERIC FRAMEWORK

Image encryption consists of few general steps which are as follows:

2.1 Select Image

Plain image is being read by the system which is to be encrypt.

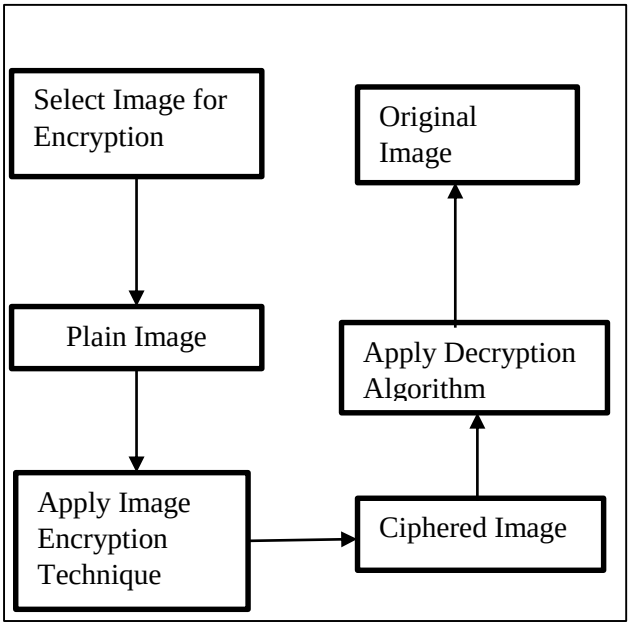

Figure 1: General approach for image encryption

2.1 Apply Image encryption technique

There are various techniques to encrypt an image, which scrambles the plain image and generate the ciphered image as an output.

2.2.1 Bit Level Scrambling

In gray scale image each pixel may be represented as an 8 bit binary value,distributed by

P(x,y)= K(8),K(7),K(6),K(5),K(4),K(3),K(2),K(1).

Usually the upper four bitplanes of 8 bit gray scale image (i.e. 8th, 7th, 6th, and 5th) contains significant amount of information while the lower four bit planes (4th, 3rd, 2nd, and 1st) contains less information as shown in figure2. The percentage of pixel information is distributed by

$$K(I) = \frac{2^i}{\sum_{i=0}^{7} 2^i} \quad (1)$$

- Bit Level Permutation – It scrambles the gray scale image by changing its positions and corresponding values at the same time.
- Bitplane decomposition– As the name suggest it decomposes the image into subparts. In [9], binary bitplane decomposition decomposes the gray scale image into 8 bit binaryplanes where in fact the nth bitplane be composed of all nth bits of binary representation of every pixel. A non-negative decimal number N may be illustrated by way of a binary sequence ($b_{n-1}\ldots b_1, b_0$) as shown in equation 2:

$$N=\sum_{i=0}^{n-1} b_i\, 2^i = b_0 2^0 + b_1 2^1 + \ldots\ldots\ldots + b_{n-1} 2^{n-1} \quad (2)$$

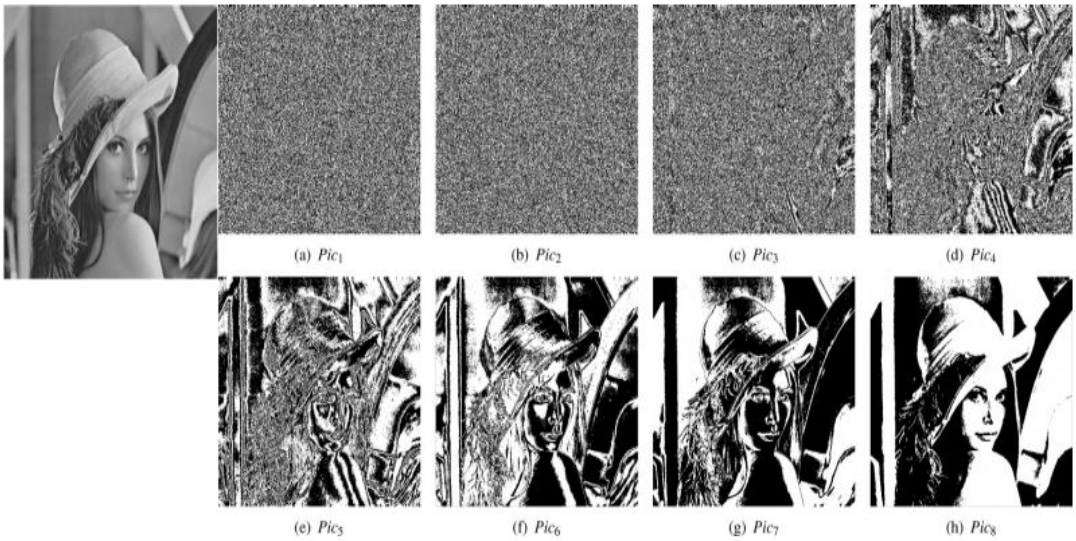

Figure 2: Plain image, (a) to (d) - lower four bitplanes, and (e) to (h) - upper four bitplanes [10]

2.2.2 Cyclic shift and Swapping

Cyclic shist is capable of chnaging the value of pixel. Example:- 10000000 is just a binary representation of a pixel, then 3 bit cyclic shift is, 00000100. Furthermore, cyclic shift is reversible and not symmetric for decryption process. So cyclic shift is just a scheme for changing the values and scrambling the values of an image in [23].

In [24], , each pixel was swapped with another positioned following it, whose location was set with a chaotic system and value of the last confused pixel. A small modification within the plain image was thus influence the following pixel swapping process and disseminate to the remaining of the encrypted image. So in this manner swapping and cycling shift is useful in image encryption and decryption.

2.2.3 Chaotic Maps

In[5], An iterated function "f" of a situation space "S" determined chaotic system and are extremely responsive to initial condition. The iterated function generates the values which are entirely arbitrary in nature but restricted between bounds. The iterated function changes the present stateof the system into the next one, i. e.

$$FS_{n+1=}(S_n) \qquad (3)$$

Where Sn ϵ S indicates a state of the system at the discrete time. In chaos based cryptography, it is normally a finite binary space.

$$\mathrm{S} = \mathrm{P} = \mathrm{C} = \{0, 1\}\,\mathrm{n}, \mathrm{n} = 1, 2 \ldots$$

Where P=Plain text, C=Cipher text.

There are various types of chaotic system which were used for encryption by various authors such as arnold cat map, logistic maps, piecewise linear chaotic maps, low and high dimensional chaotic maps, lorenz chaotic system etc. Usually high dimensional chaotic maps prefered over low dimensional chaotic maps due to the high security features. Each type of chaotic map came with its own different feature.

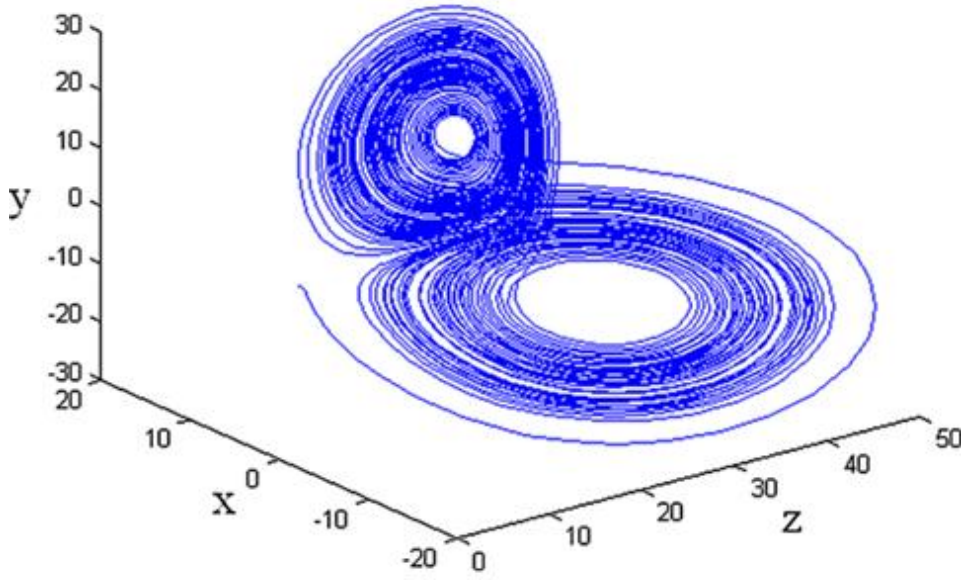

Figure 3 : Chaotic behavior (lorenzsystem) [3]

2.2.4 DNA coding

In [21], there are four nucleotides, namely A, T, C, and G, whereby pairing is allowed only between A and T & C and G. Moreover, the binary value pair for each pixel in grayscale image constitutes a complementary relationship pair. By using the digit pairs 00, 01, 10, and 11, DNA bases four nucleotides (A, C, G, and T) can be encoded. Some operations like addition, subtraction, xor can be performed.

Table 1. Rules for DNA coding

	I	**II**	**III**	**IV**	**V**	**VI**	**VII**	**VIII**
T	11	11	10	10	01	01	00	00
A	00	00	01	01	10	10	11	11
G	10	01	11	00	11	00	10	01
C	01	10	00	11	00	11	01	10

Table 2. Addition (Rule V)

Rule 5	**A**	**G**	**C**	**T**
A	C	T	A	G
G	T	A	G	C
C	A	G	C	T
T	G	C	T	A

Table 3. Subtraction (Rule III)

Rule 3	**A**	**G**	**C**	**T**
A	C	T	A	G
G	T	C	G	A
C	A	G	C	T
T	G	C	T	A

Table 4. XOR (Rule VII)

Rule 7	**A**	**G**	**C**	**T**
A	T	C	G	A
G	C	T	A	G
C	G	A	T	C
T	A	G	C	T

2.2 Decryption

At last apply decryption on ciphered image to obtain the plain image at the receiver end.

2.3 Parameters and various attacks

There are various parameters used to measure the image encryption level by calculating or analysing some parameters. The general aspects which must be consider are key space, histogram analysis, correlation coefficient analysis, number of pixels change rate, UACI, PSNR, and MSE. All of these parameters helps in detecting the level of algorithm to resist a particular attack as shown in Table 5.

Table 5. Parameters and description

S.no	Types of attacks	Parameter name	Description
1	Brute force attack	Key space	Guessing the correct key by analyzing the key value is referred to as brute force attack which can be resisted by having algorithm of sufficiently large key space.
2	Statistical attack	(i) Histogram analysis, (ii) Correlation coefficient analysis	(i) If the values of pixels in histogram is not uniform then, information can be leaked. So uniform distribution is good for resisting statistical attack. (ii) Encrypted image must have low correlation with adjacent (horizontal, vertical, diagonally) pixels.
3	Differential attack	(i) NPCR (ii) UACI	(i) Number of pixels change rate – $\frac{\sum_{s,t} D(s,t)}{M \times N} \times 100\%$ Where, M&N are width and height of image respectively, $D(s,t) = \begin{cases} 1, c_1(u,v) \neq c_2(u,v) \\ 0, otherwise \end{cases}$ Where C_1 and C_2 are ciphered image before and after modification of pixel. (ii) Unified average changing intensity – $\frac{\sum_{u,v} \lvert C_1(u,v) - C_2(u,v) \rvert}{M \times N \times 255} \times 100\%$
4	Noise attack	(i) PSNR (ii) MSE	(i) PSNR(Peak signal to noise ratio) – It computes the quality of the recovered image $10 \times log_{10} \frac{255 \times 255}{MSE} (db)$ (ii) Mean square error – It determines the MSE between the recovered and plain image. $\frac{1}{m,n} \sum_{p=1}^{m} \sum_{q=1}^{n} \parallel A_1(p,q) - A_2(p,q) \parallel^2$ Where m and n are width and height of image, A_1 (p, q) is original image & A_2 (p, q) is recovered image.
5	Occlusion attack	PSNR(peak signal to noise ratio)	During transmission channels may lose some data which result into decrypting the image harder. It is used to test the capacity of recovering the plain images from ciphered images. PSNR is used to evaluate the occlusion performance.

3. LITERATURE SURVEY

(Lu Xu et al. 2016) [25], presented a algorithm for image encryption using piecewise linear chaotic maps which was deployed at bitlevel. After applying binary bitplane decomposition, diffusion and confusion strategy has been applied and hence successfully acheived good security with just single round.

(Xiangyuan Wang et al. 2015) [12], proposed color image encryption with various types of permutation among bits and correlated chaos which improves permutation efficiency and full use of chaotic maps and hence increased the security.

(Xiangyuan Wang et al. 2015) [13], proposed image encryption technique using the combinations of chaotic maps and random growth. It eliminate cyclical phenomenon and generate the random streams which result into improve the security level.

(Muhammad Rafiq Abuturab et al. 2015) [14], suggested an individual channel color image encryption with hartley and graytor transform. The unsymmetric keys, random phase mask provides high robustness and changed angle of graytor transform offers as principal key which is highly sensitive.

(Xing Yuan Wang et al. 2015) [17], in their work proposed a technique which dependupon combination of DNA cryptosystem and chaotic system. Scrambling was done by using various operations like XOR operation on pixels, DNA encoding rules were responsible for creating more confusions and permutation. So in this way it provide more security.

(Wang et al. 2015) [23], presented an algorithm which depends upon cyclic shifts and chaotic system. The arbitrary integers taking the exact same size of the original image were made to do scrambling for cyclic shift operations,then keys are produced by chaotic system. İn this way it is superior nad resist exhaustive attack.

(Yicong Jhou et al.2014) [9], introduced a image encryption employing a bitplane of a plain image as the secret key bitplane to encode images. İt demonstrated an excellent performance of the encryption.

(R Huang et al. 2014) [20], have proposed a method in which a block cipher framework consisted of scrambling, jumbling up S-box and chaotic lattice for encrypting the quantized measurement data. İt was not only acheived confusion,diffusion and sensitivity but also outperforms the existing parallel image encryption methods with respect to the compressibility and the encryption speed.

(Zhang Ying-Qian et al. 2014) [26], presented an encryption technique using mixed linear-nonlinear coupled map lattices. İt permits the lower bitplanes and the higher bitplanes of pixels permute interchangeably without any additional storage space. İt results into superior security and high efficiency.

4. COMPARATIVE ANALYSIS

Table 6: Comparison of techniques based upon 3 parameters

Ref No.	Year	Author name	Technique	Key Space	Compressive Sensing	Speed
[25]	2016	Lu Xu	Bitplane decomposition and Chaotic maps.	0.25×10^{64}	No	Low
[12]	2015	Xingyuan Wang	Permutation and inter related chaos.	10^{108}	No	Low
[13]	2015	Xingyuan Wang	Dynamic random growth technique	$>10^{96}$	No	Moderate
[14]	2015	Muhammad Rafiq Abuturab	Hartley and Graytor transform	$>2^{100}$	No	Low
[17]	2015	Xing-Yuan wang	DNA sequence operation	8.39×10^{54}	No	Good
[23]	2014	Xing-Yuan Wang	Cyclic shift and chaotic system	$8^{256\times256}$	No	Low
[26]	2014	Zhang Ying-Qian	Mixed linear- non linear coupled map lattice	$>10^{120}$	No	Moderate
[20]	2014	R Huang	Compressive sensing	3.4×10^{38}	Yes	Good
[9]	2014	Yicong Zhou	Binary bitplane	4.916×10^{322}	No	Moderate
[24]	2014	Jun-Xin Chen	Swapping based confusion approach	0.18×10^{60}	No	Good
[6]	2012	Guodong Ye	Arnold map	$>2^{100}$	No	Moderate
[8]	2012	Lin Teng	Spatiptemporal chaotic system and self adaptive	10^{56}	No	Moderate
[2]	2012	Nidhi sethi	Logistic mapping	10^{112}	Yes	Moderate
[11]	2011	Hongjun Liu	Spatial bit level permutation and high dimensional chaotic system	1.03×10^{114}	No	Low
[10]	2011	Zhi-Liang zhu	Bit level permutation	10^{42}	No	Low

In Table 6, image encryption techniques are being compared upon 3 parameters which are as follows:

- Key space – It can be determined by calculating the total number of keys which are utilized in the encryption procedure. Greater the value, more will be the security level. İt is calculated as {n round × N_0 (iteration times) × Computational precision}. Normally size of the key should be greater than 2^{100}.
- Compressive sensing – It is a sampling technique which reduces the sampling rate at the exposure of a complex reconstruction on the recipient. So it enables us to work on compressed images.
- Speed – The speed of an algorithm is determined by two main factors known as computational cost and complexity of algorithm used. Computational cost checks the number of rounds during encryption and also consider how many permutation and diffusion operations occurred within a round. It is observed that many of the techniques are more inclined towards providing high security and ignoring the speed.

5. CONCLUSION

Image encryption is distinctive from text encryption for some characteristics like greater interrelation among pixels and mass data volume . In this paper many of new algorithms have been studied like chaotic maps, DNA coding, compressive sensing, bit plane decomposition, cyclic shift and swapping. As it has been observed that the key space of above discussed techniques are large enough to resist any attack and reliable for providing security. Also DNA cryptography outperformed when compared on the basis of computational speed because of its outstanding characteristics. While considering the security and performance, compression of the image could also be consider as well. By hybridising the Compressive sensing and DNA cryptography performance of the encryption can be improved.

REFERENCES

[1] Li S, Chen G, Cheung A, Bhargava B, Lo K-T. On the design of perceptual MPEG- Video encryption algorithms. IEEE Trans Circuits Syst Video Technol 2007; 17 (2):214–23.

[2] Sethi, Nidhi, and Deepika Sharma. "A novel method of image encryption using logistic mapping." *Int. J. Comput. Sci. Eng* 1.2 (2012): 115-119.

[3] Wang XY, Yang L, Liu R, Kadir A. A chaotic image encryption algorithm based on perceptron model.Nonlinear Dyn2010; 62(3):615–21.

[4] Liu HJ, Wang XY. Color image encryption based on one-time keys and robust chaotic maps.ComputMathAppl2010; 59(10):3320–7.

[5] Wang XY, Teng L, Qin X. A novel color image encryption algorithm based on chaos. Signal Process2012; 92(4):1101–8.

[6] Ye GD, Wong KW. An efficient chaotic image encryption algorithm based on a generalized Arnold map. Nonlinear Dyn2012; 69(4):2079–87.
[7] Tong XJ. Design of an image encryption scheme based on a multiple chaotic map. Commun Nonlinear Sci Numer Simul2013; 18(7):1725–33.
[8] Teng, Lin, and Xingyuan Wang. "A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive." *Optics Communications* 285.20 (2012): 4048-4054.
[9] Zhou YC, Cao WJ, Chen CLP. Image encryption using binary bitplane. Signal Process 2014; 100:197–207.
[10] Zhu ZL, Zhang W, Wong KW, Yu H. A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf Sci2011; 181(6):1171–86.
[11] Liu HJ, Wang XY. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun2011; 284(16):3895–903.
[12] Wang XY, Zhang HL. A color image encryption with heterogeneous bit-permutation and correlated chaos. Opt Commun2015; 342:51–60.
[13] Wang XY, Liu LT, Zhang YQ. A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 2015; 66:10–8.
[14] Abuturab MR. an asymmetric single-channel color image encryption based on Hartley transform and gyrator transform. OptLasers Eng 2015; 69:49–57.
[15] Xiao GZ, Lu MX, Qin L, Lai XJ. New field of cryptography: DNA cryptography. Chin SciBull2006; 51(12):1413–20.
[16] Enayatifar R, Abdullah AH, Isnin IF. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Opt Lasers Eng 2014; 56:83–93.
[17] Wang XY, Zhang YQ, Bao XM. A novel chaotic image encryption scheme using DNA sequence operations.OptLasersEng2015; 73:53–61.
[18] Enayatifar R, Sadaei HJ, Abdullah AH, Lee M, Isnin IF. A novel chaotic based image encryption using a hybrid model of deoxy ribo nucleic acid and cellular automata. OptLasersEng2015; 71:33–41.
[19] Zhou NR, Zhang AD, Zheng F, GongL H. Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compres- sivesensing.OptLaserTechnol2014;62:152–60.
[20] Huang R, Rhee KH, U chida S. A parallel image encryption method based on compressive sensing.MultimedToolsAppl2014; 72(1):71–93.
[21] Zhang, Jian, Dezhi Hou, and Honge Ren. "Image Encryption Algorithm Based on Dynamic DNA Coding and Chen's Hyper chaotic System." Mathematical Problems in Engineering 2016 (2016).
[22] Liu, Xiaoyong , et al. "Optical image encryption technique based on compressed sensing and Arnold transformation." Optik-International Journal for Light and Electron Optics 124.24 (2013): 6590-6593.
[23] Wang, Xing-Yuan, Sheng-Xian Gu, and Ying-Qian Zhang. "Novel image encryption algorithm based on cycle shift and chaotic system." Optics and Lasers in Engineering 68 (2015): 126-134.

[24] Chen, Jun-xin, et al. "A fast image encryption scheme with a novel pixel swapping-based confusion approach." *Nonlinear Dynamics* 77.4 (2014): 1191-1207.

[25] Xu, Lu, et al. "A novel bit-level image encryption algorithm based on chaotic maps." *Optics and Lasers in Engineering* 78 (2016): 17-25.

[26] Zhang YQ, Wang XY. Asymmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice.InfSci2014; 273(20):329–51.