A Performance Comparison of Encryption Algorithms for Digital Images

M. Bala Kumar[a], P. Karthikka[b], N. Dhivya[c], T. Gopalakrishnan[d]
[a,b,c] PG Scholar, Department of Electrical and Electronics Engineering, Dr. Mahalingam College of Engineering and Technology, Pollachi.
[d]Department of Electrical and Electronics Engineering, Dr. Mahalingam College of Engineering and Technology, Pollachi.

***Abstract*— In recent years, image encryption plays an important role in the field of information security and multimedia applications. This paper presents the comparative study of three different encryption algorithms in terms of security and performance. From cryptographic viewpoint, the analysis parameters focussed here are information entropy, correlation coefficients, encryption quality, NPCR (Number of Pixels Changing Rate), UACI (Unified Average Changing Intensity) and processing time. The comparison result shows that each algorithm has its own advantages that suits for different applications.**

Keywords*— Non-chaos, Chaos, Hyper-chaos, Correlation coefficient, Differential measures, Encryption entropy.

I. INTRODUCTION

With the development of network and multimedia technology, digital images are widely used. The image data has some special characteristics like high capacity, redundancy and high correlation among pixels. In some cases, image applications require to satisfy their own needs like real time transmission and processing. One of the main goals that must be achieved during the transmission of information over the network is security. Cryptography is the technique that can be used for secure transmission. This technique will make the information to be transmitted into an unreadable form by encryption so that only authorized persons can correctly recover the information. The security of image can be achieved by various types of encryption schemes. Different chaos based and non-chaos based algorithms have been proposed. The general structure of encryption involves two processes namely, permutation and diffusion. The permutation scheme just shuffles the pixel values based on the algorithm whereas substitution changes the pixel values. Mohammad Ali [1] proposed a block transformation based encryption algorithm. Here the image is divided into a random number of blocks, the blocks are shuffled and the permuted image is given to the Blowfish encryption algorithm. The dividing of image into as much as small blocks reveals higher entropy and less correlation between the pixels. In [2], different types of permutation techniques like bit permutation, pixel permutation and block permutation were analyzed and the combinational permutation technique was proposed. To generate the pseudo random index, LFSR (linear feedback shift registers) were used. In the combinational method, bit or pixel or block permutation techniques were used to break the correlation among the pixels in the image.

Wang *et al* [3] proposed a chaos based encryption algorithm in which both permutation and diffusion are considered as two separate stages. Pixel values are first obtained by image scanning to accelerate the encryption process. Image is first divided into blocks and tent map is used to generate the pseudorandom sequences. In [4], coupling of chaotic function and XOR operation is done to produce large key space to resist brute force attacks. The chaotic function is based on linearity. And this function is used to generate pseudorandom numbers so that row-wise and column-wise shuffling can be done. The algorithm in [5], uses two phases to shuffle the image. In the first phase scrambling of plain-image is done and in second stage mixing operation of scrambled image using discrete states variables of chaotic maps is done. Discrete Cosine Transform (DCT) is used for compression. The proposed algorithm is strong in providing security and is also very fast. Since the key space is large, the attacker cannot decrypt an encrypted image without the correct key.

Vikram Jagannathan *et al* [6], combined compression and encryption simultaneously employing Number theory paradigm. To achieve this they applied Congruence theory and Chinese Remainder Theorem. Both the lossless and lossy compression methods using Number theory are discussed. Compression ratio achieved on Lena image is 1.85 which is better than Huffman and LZW (Lempel-Ziv-Welch). The proposed method has equivalent performance to JPEG2000

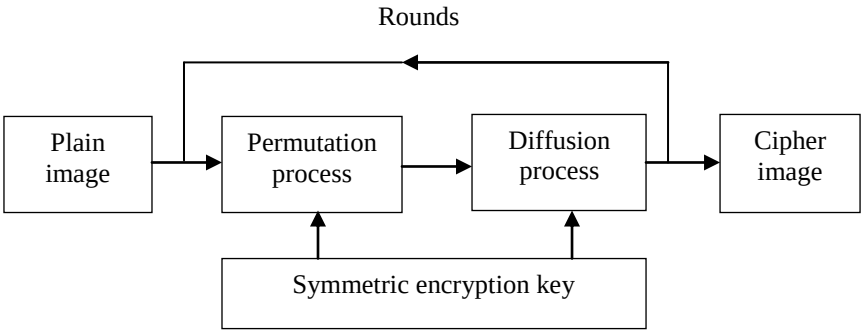

Figure 1. Encryption architecture

which achieve 1.86 compression ratios. But the performance is not better than JPEG-LS, CALIC and SPIHT. However the level of encryption offer is high.

The rest of this paper is organized as follows. Section II provides a description of the selected image encryption algorithms. The efficient measuring methods, security analysis and experimental results are presented in section III. Finally, the concluding notes are introduced in section IV.

II. ENCRYPTION TECHNIQUES

Image encryption algorithms can become an integral part of the image delivery process if they aim towards efficiency and at the same time preserve the highest security level. These algorithms can be classified into three types: non-chaotic, chaotic and hyper-chaotic. The following subsections describe briefly three algorithms of the above mentioned types. The general architecture of the encryption technique is shown in Figure 1.

A. Non-chaotic approach

Non-chaos based method uses different types of scanning to permute the image pixels. The scanning techniques used are zig-zag, rectangular, horizontal, vertical, etc. The Non-chaotic cryptosystem proposed by N. K. Pareek *et al* (2013) has three phases. They are mixing phase, permutation phase and diffusion phase. Key space of this technique is 128 bit that avoids brute-force attack. Mixing process slightly modify the pixel intensity value. Here the image is divided into non-overlapping blocks. Using zig-zag scanning the image block pixels is shuffled. For the zig-zag scanning process the selection of starting pixel location based on the secret key given to the encryption algorithm. In the diffusion process the current pixel is masked with its surrounding pixel. The selection of surrounding pixel also is based on the secret key. The dividing of image into non overlapping blocks varies in each round of the encryption algorithm. The block dimension variation gives the correlation break among the image pixels.

B. Chaotic approach

Chaos theory is a mathematical theory, and it is still in development. It enables the description of a series of phenomena from the field of dynamics. It is focussed on those strictly deterministic dynamic systems that present the peculiarity of being sensitive to initial conditions and when they have a property of recurrence, cannot be predicted over the long term. Since we are in need of huge data message, it needs a quick and secure algorithm for image encryption, so chaotic encryption is widely researched in these years. Discrete chaotic systems such as Logistic map, Tent map, Henon map are designed for image encryption and many researchers proposed an encryption model based on digital chaotic system.

X-J Tong [2013] proposed a novel chaotic map based on topological conjugacy and the chaotic characteristics are proved by Devaney definition. In order to produce a large key space, a new cat map named separated Cat map is also designed in this process for permutation. In the permutation phase, compared with other maps, the key space of cat map is smaller. So to improve the security, the image is divided into four blocks. Each block is processed by cat map and the input parameters are obtained from the Henon map. Because of more control parameters the key space is much larger. With the help of newly designed chaotic map, a real chaotic random sequence is generated for the diffusion process. The experimental results prove that the proposed algorithm is simple and is of higher security.

C. Hyper-chaotic approach

Recently, because hyper-chaos has more than one positive Lyapunov exponent, and have more complex dynamical characteristics than chaos, so secure communication schemes based on hyper-chaotic systems have been investigated, but at present, there is little work about the study of encryption algorithm based on hyper-chaos. In general, as the prediction time of a chaotic system is longer than that of a hyper-chaotic system, so it may be more valuable to study the application of hyper-chaos in encryption algorithms. In recent years,

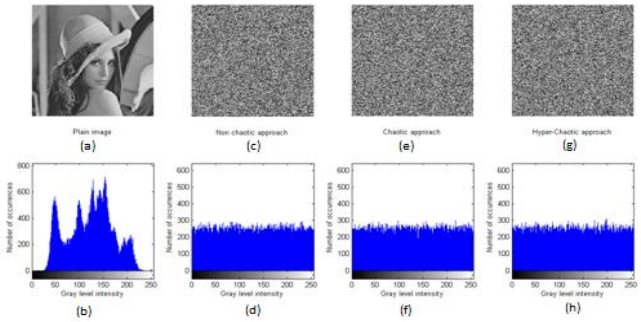

Figure 2. Histogram analysis of the different Encryption approaches. (a) plain image, (b) histogram of the plain image, (c) cipher image of non-chaotic approach, (d) histogram of (c), (e) cipher image of chaotic approach, (f) histogram of (e), (g) cipher image of hyper-chaotic approach, (h) histogram of (g).

when multimedia security is concerned, the need to apply both encryption and compression to digital image communication keeps rising. A number of image encryption schemes combined with compression have been proposed. Some methods divide the image encryption and image compression into two separate stages. Thus, the adversary is mainly on breaking the encryption without considering the compression process. Some methods overcome the defect mentioned by combining the image encryption and compression in a single process. However, these methods need insert additional operation into the procedure, and the procedure is complicated.

Hegui Zhu *et al* (2013) proposed a new image encryption algorithm integrated with compression using 2D hyper-chaos discrete non-linear dynamic system and Chinese remainder theorem is proposed. First, the 2D hyper-chaos discrete nonlinear dynamic system is used to generate two hyper-chaos sequences, and then use them to shuffle the position of pixels in the plain image. Next, the image is encrypted and compressed the shuffled image with a given compression ratio k by the famous Chinese remainder theorem. In the permutation process, a hyper-chaotic orbit $\{(x_k, y_k), k = 0,1, \ldots\}$ is obtained with initial value (x_0, y_0), several iterations are made to get two new sequences $\{x_1', x_2' \ldots.\}$ and $\{y_1', y_2' \ldots.\}$. These sequences are arranged in ascending order and two index order sequences are obtained correspondingly. These index order sequences are applied to permute the image pixel positions. Hence, the image is confused and a shuffled image is obtained. Then the shuffled image is grouped into blocks containing four pixel values which are diffused into one by The Chinese Remainder Theorem and thus encryption and compression are done simultaneously.

3. Comparison criteria and Experimental results

The performance of the encryption algorithms discussed in Section II is compared in terms of the following metrics: Histogram analysis, Correlation coefficient, Differential measures, Encryption entropy and Execution speed.

3.1 Histogram analysis

Histogram analysis is employed to illustrate the superior substitution and diffusion properties of the encryption algorithm. We have analysed the histograms of several encrypted images obtained from the above mentioned approaches and their corresponding plain images. One example of such histogram analysis is shown in Figure 2. Relative uniform distributions in encrypted image histograms point out good quality of method. Therefore, the encryption image does not provide any clue to employ any statistical attack on the discussed approaches, which makes statistical attacks difficult.

3.2 Correlation coefficient

Statistical analysis such as correlation coefficient is used to measure the relationship between neighbouring pixels in an image. For a plain image, the correlation between two adjacent pixels are always high either in horizontal, vertical or diagonal directions, this can be calculated by equation,

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

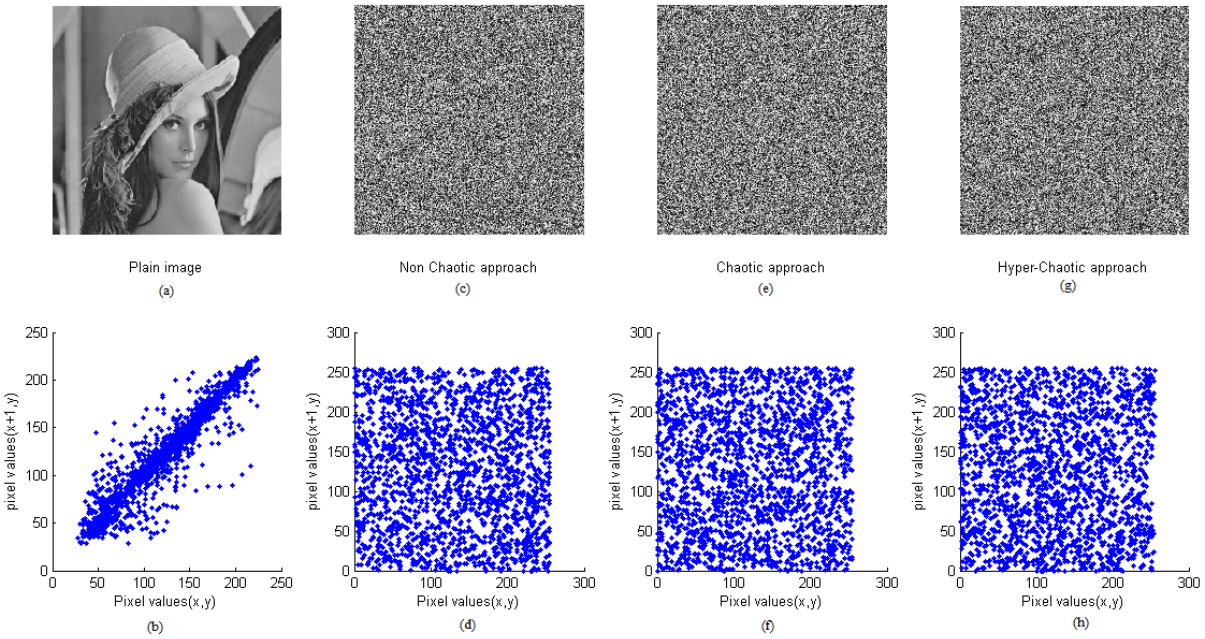

Figure 3. Correlation plots of two horizontaly adjacent pixels, (a) plain image, (b) correlation plot of plain image, (c) Cipher image of Non-Chaotic approach, (d) correlation plot of (c), (e) Cipher image of Chaotic approach, (f) correlation plot of (e), (g) Cipher image of Hyper-Chaotic approach, (h) correlation plot of (g).

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

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x_i))(y_i - E(y_i)) \quad (3)$$

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (4)$$

where x and y are gray values of two adjacent pixels in the image and $E(x)$ and $D(x)$ are the Expectation and Variance intensity respectively. Correlation coefficient of original image is usually high (nearly one). Weaker the correlation coefficient of the encrypted image better the algorithm. Table 1 shows the outcome of the three approaches discussed above using standard Lena gray image. From the table it can be seen that, the hyper-chaotic approach induces more randomness than the other two approaches. Figure 3 shows the correlation plots of two horizontally adjacent pixels in all the three discussed approaches. Similar results are obtained for adjacent vertical and diagonal pixels.

TABLE 1
CORRELATION COEFFICIENT FACTOR

Algorithm	Horizontal	Vertical	Diagonal
Non-chaotic approach	-0.0174	0.0109	0.0063
Chaotic approach	0.0354	0.0258	0.0185
Hyper Chaotic approach	-0.0113	-0.0150	-0.0035

D. Differential measures

To resist differential attack, any change in plain image will cause a significant change in the cipher image. For this two common measures are used. i.e., NPCR and UACI. The NPCR measures the difference in the pixel numbers and UACI is about the average intensity of differences between two images. Always NPCR values should be in the range of 99% and UACI be 33% and this indicates the sensitivity of algorithm.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (5)$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j}\frac{D(i,j)}{255}\right] \times 100\% \quad (6)$$

Differential attack would become inefficient if one minor change in the plain image can cause a significant change in the cipher image. Higher NPCR values are desired for ideal encryption schemes. The UACI values must be in range of 33%.

TABLE 2
NPCR

Algorithm	Lena (gray)
Non-chaotic approach	0.9962
Chaotic approach	0.9947
Hyper Chaotic approach	0.9967

TABLE 3
UACI

Algorithm	Lena (gray)
Non-chaotic approach	0.3351
Chaotic approach	0.3347
Hyper Chaotic approach	0.3362

Table 2 and 3 shows the comparison of these values. From these tables, it is observed that, all the compared techniques have achieved the standard criterion and hence they resist various differential attacks.

E. Encryption entropy

The idea of information entropy was created by Shannon. It has applications in many areas, such as, lossless data compression, statistical inference, cryptography. In recent times it is used in other disciplines, such as, biology, physics, and machine learning. Information entropy is a measure of the uncertainty associated with a random event and it is used to tell how much information there is in an event. The more uncertain or random the event is, the more information entropy it will contain. Therefore, it is very useful for analysing the randomness of an encryption scheme and is estimated by using Equation (7). Here X is the information source with length L.

$$H(x) = -\sum_{i=0}^{i=l-1} p(x_i)\log_2(p(x_i)) \qquad (7)$$

where $p(x_i)$ represents the probability of occurrence of x_i.

For true random information source X emits 2^8 symbols with equal probability $p(x_i) = \frac{1}{2^8}$, i.e. $X = (x_0, x_1, \dots, x_{2^8})$. After computing the information entropy using Equation (7), we get $H(X) = 8$. Actually, given that a practical information source seldom generates random messages, we know that its information entropy value is smaller than 8 in general. However, when the messages are encrypted, their information entropy should ideally be 8. Particularly, if an image encryption algorithm creates symbols with information entropy less than 8, there is a possibility of predictability, which is a threat to the cryptosystem security.

TABLE 4
ENTROPY

Algorithm	Lena(gray)	Cipher
Non-chaotic approach	7.4288	7.9971
Chaotic approach	7.4288	7.9974
Hyper Chaotic approach	7.4288	7.9970

Table 4 shows the entropy values of the discussed algorithms. For a gray scale image having 256 levels, the theoretical value of entropy is 8 bits. But practically achieving this ideal value is not possible. The encryption algorithms that reach the nearest value 8 are appreciable. From Table 4 it is inferred that chaotic approach gives better results compared to other approaches.

F. Encryption speed

Another important tool to evaluate the efficiency of algorithms is measuring the amount of time required to encrypt an image. In this investigation, actual time in CPU cycles will be used as a measure of execution time. In many real-time applications, it is important that the encryption and decryption algorithms are fast enough to meet the requirements. Designer should attempt to optimize a cryptosystem to make the execution time as lower as possible. We have calculated the execution time of the algorithms used for comparison for a standard Lena image of size 512x512 and is shown in Table 5. It is seen that the hyper-chaotic approach consumes less processing time.

TABLE 5
ENCRYPTION SPEED

Algorithm	Seconds
Non-chaotic approach	1.5024
Chaotic approach	1.8126
Hyper Chaotic approach	0.4023

III. CONCLUSION

In this brief, we have performed a performance comparison of the three different image encryption algorithms. From the experimental results, the performance measures like Correlation coefficient, Differential measures, Encryption entropy and Execution speed have been estimated using standard test images. Each of the techniques has its own advantages. Identification of suitable algorithm for a particular application depends on the prerequisites of that application.

REFERENCES

[1] Ali B.Y. Mohammad, J. Aman, Image encryption using block based transformation algorithm, IAENG Int. J. Comput. Sci. 35 (2008) 15–23.
[2] A. Mitra, Y.V. Subba Rao, S.R.M. Prasanna, A new image encryption approach using combinational permutation techniques, International journal of Comput. Eng. 1(2006) 127–131.
[3] Wang Y, Wong KW, Liao XF, et al. A new chaos-based fast image encryption algorithm. Appl Soft Comput 2011 11(1):514–22.
[4] M.francis, T.Grosges, R.Erra, D.Barchiesi A new image encryption scheme based on a chaotic function.Signal Processing: Image Communication 27 249–259/(2012).
[5] V.Radha, D.Maheswari, ―Secured Compound Image Compression Using Encryption Techniques‖, *978-1-4244-5967-4/ IEEE* 2010
[6] V. Jagannathan, Aparna Mahadevan, R. Haraharan and E. Srinivasan, Number theory based Image compression Encryption and Applications to Image Multiplexing, IEEE-ICSCN 2007, MIT Campus, Anna university, Chennai, India,pp.59-64,2007.
[7] N. K. Pareek, Vinod Patidar, Krishan K. Sud, Diffusion-Substitution base gray image encryption scheme, Digital Signal Processing 23 (2013) 894-901.
[8] Xiao-Jun Tong Design of an image encryption scheme based on a multiple chaotic map Commun Nonlinear Sci Numer Simulat 18 1725–1733/(2013).
[9] Hegui Zhu, Cheng Zhao, Xiangde Zhan, A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem , Signal Processing: Image Communication 28 (2013)6700–68.
[10] Guodong Ye, Image scrambling encryption algorithm of pixel bit based onchaos map, Pattern Recognit. Lett. 31 (2010) 347–354.
[11] Jui-Cheng Yen, Jiun-In Guo, A new chaotic key based design for image encryption and decryption, in: Proceedings of IEEE International Symposium on Circuits and Systems, vol. 4, 2000, pp. 49–52.
[12] G. Alvarez, Shujun Li, Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption, Commun. Nonlinear Sci. Numer. Simul. 14 (2009) 3743–3749.
[13] Chengqing Li, Shujun Li, Guanrong Chen, Wolfgang A. Halang, Cryptanalysis of an image encryption scheme based on a compound chaotic sequence, Image Vis. Comput. 27 (2009) 1035–1039.
[14] Zhang G., Liu Q, (2011), 'A novel image encryption method based on total shuffling scheme', Optical communication, Vol 284(12), pp. 2775-2780.

[15] Yushu Zhang, Di Xiao, An image encryption scheme based on rotation matrix bit-level permutation and block diffusion, Commun Nonlinear Sci Numer Simulat xxx (2013).
[16] Solak Ercan et al. Cryptanalysis of fridrich's chaotic image encryption. Int J Bifurcation Chaos 2010;20(5):1405.
[17] Liao XF, Lai SY, Zhou Q. A novel image encryption algorithm based on self-adaptive wave transmission. Signal Process 2010;90 (9):2714–22.
[18] J.L. Liu, Efficient selective encryption for JPEG 2000 images using private initial table, Pattern Recognition 39 (2006) 1509–1517.
[19] G. Alvarez, S.J. Li, Some basic cryptographic requirements for chaos-based cryptosystem, International Journal of Bifurcation and Chaos 16 (8) (2006)2129–2151.
[20] Y. Wang, K.W. Wong, X. Liao, G. Chen, A new chaos-based fast image encryption algorithm, Applied Soft Computing 11 (2011) 514–522.