International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

Ls Chaotic based Image Encryption System Via Permutation Models

A Sharmila banu[1], R Prem kumar[2]

[1]Mount Zion College of Engineering and Technology, Pudukkottai, Tamilnadu, India.
[2]Assistant Professor of ECE, Mount Zion College of Engineering and Technology, Pudukkottai, Tamilnadu, India.

Abstract - *Information security plays a significant role in all fields, especially those related to confidential business or military affairs, multimedia data, innovative technologies in data and PC sciences. Picture assumes an imperative job in the data transfer, with the rapid development of communication network. Picture encryption is difficult from that of writings because of some inborn highlights of pictures, for example, mass information limit and high excess, which are bulky complicated to hold by conventional methods. Unauthorized accesses of personal or private information is became serious issue in this modern world. The security problems have attracted a huge of concerns not only from researcher's side but also the normal public. Where encryption is a classical and efficient way to solve these type of problems, for this paper based on multiple diffusion models (X and +), a completely unique chaotic cryptography scheme. In this paper propose a symmetric figure encryption base on LS chaotic based dissemination models.*

***Key Words*: Diffusion, Secret key, Cipher image**

1. INTRODUCTION

Ref [1] the speedy development of transmission media, people put forward higher necessities on the security and accuracy of the information. Digital image that may be a typical two-dimensional information smitten the intrinsic options of huge size, bulk information capacity, high redundancy, and high bond along with neighboring pixels become one in every of necessary kinds of multimedia system. In ref [2] Image is calculated by grid in two ways to accomplish pressure and encryption and then coming about picture is re-scrambled by the cyclic move operation controlled by hype-chaotic method. These types of progression transform the values of the pixels efficiently. An efficient image compression algorithm combining 2-D CS with hyper-confused framework is available, which upgrades the security framework and achieves high-speed encryption during 2 Dimensional CS. In ref [3] three dimensional cat maps introduce for input stream making, with the iterations of cat map, three state variables are concurrently produced, and they are apply to compressed sensing (CS), permutation and diffusion process. In ref [4] 3-D cat map to mix up arrangement of figure pixels and uses one more chaotic map to confuse the bond between the original and encrypted image, these system significantly enhance the resistance to statistical. This type of system is mostly suitable for real-time multimedia image encryption and transmission application. In ref [5] Encryption and information hiding technique are used to develop the defense moreover confidentiality of the transmit template.

In ref [6] chaos picture encryption with permutation-diffusion through which spatiotemporal confused framework displayed by coupled guide grids used to produce random sequences, in permutation- the equal dimension of simple image, which mix up the arrangement of pixels completely, in diffusion-bidirectional diffusion used to diffuse every pixel to all additional pixels of the image. In ref [7] chaos-based cryptosystem having two stages they are, confusion stage is pixel transformation somewhere pixel position is changed in excess of complete image without disconcerting the rate of pixels. The transformation is conceded away in a arrangement. Next stage of encryption process aims at varying the value of all pixels in entire image.

In ref [8-9] chaos based image cipher system design composes of two stages are permutation and diffusion, these design has drawn worldwide attentions and spreads of sequential variants are after that probable for protected communication. The algorithm decomposes input images into bit-planes, arbitrarily swap bit-blocks along with dissimilar bit-planes, and conducts XOR operation connecting the scrambled images and secret matrix. At last, an encrypted PNG picture is obtain by screening four mixed grayscale images while its red, green, blue in addition to alpha mechanism.

In ref [10] new square picture encryption conspire dependent on mixture chaotic map and lively arbitrary enlargement technique to use cat map. For the diffusion process, an intermediate parameter is considered by the picture square. The delegate parameter is utilized as the underlying parameter of turbulent guide to create arbitrary information tributary. In ref [11] tent map proposed a new picture encryption conspire. Initially, the tent map adjusted to create clamorous key stream that is appropriate for picture encryption. After that, chaos type tributary is generating by a 1-D diagram.

In ref [12] a non-chaos representation scheme via secret key in 128-bit. In this design, representation is separated into quite a few energetic block along with every block passes throughout the 8 round of dispersion method. In every round, block size is kept back different which depends on the secret key used in the algorithm. In ref [13] digital image scrambling a procedure is transforms significant images into

insignificant image in regulate to improve ability to confront attack and successively improve security. Basically image scrambling method the new figure information is secreted, so that data won't be effectively captured. In ref [14] picture mixing is well-organized method for gave a security image, the idea of image scrambling is to modify the image pixel positions throughout matrix transform; these strategy utilizes R-prime mix to scramble image. In ref [15] for this method the picture figure utilizing square based scrambling and picture separating (IC-BSIF). The block-based scrambling is able to separate nearest pixels to dissimilar rows and columns, and thus can capably weaken the strong correlations connecting adjacent pixels.

To prove this function, then I have to work among a new picture method which has the admirable scrambling and also permutation properties for withstand different attacks.

2. THE PROPOSED IMAGE ENCRYPTION SCHEME

2.1 System design

This paper works under scrambling and permutation method. This method efficiently to increase the amount of security and also prevent hacking against the illegal persons, the result of block results in sequential block-by-block encryption. Our planned image encryption proposal is shown in Fig. 1. In this work initially, the plain image are convert into gray scale image then the bit plane decomposition operation is performed, because the bit plane splicing is principally used for splitting images into binary planes. Each bit is employed to represent the intensity of every constituent of an image, next scrambling operation are performed after that a logistic sine map for key generation via arithmetic equations to get partial encrypted images. Finally, the permutation operation is performed to get a final encrypted output.

2.2 Chaotic system

Chaotic systems are incredibly perceptive toward initial parameter values and their connected evaluations perform recognition to their inherent characteristics. This implies that a small amendment in input parameter value causes immense change within the price that's generated by the evolution performs. Logistical map is solitary in every foremost common chaotic maps, notably in image encryption.

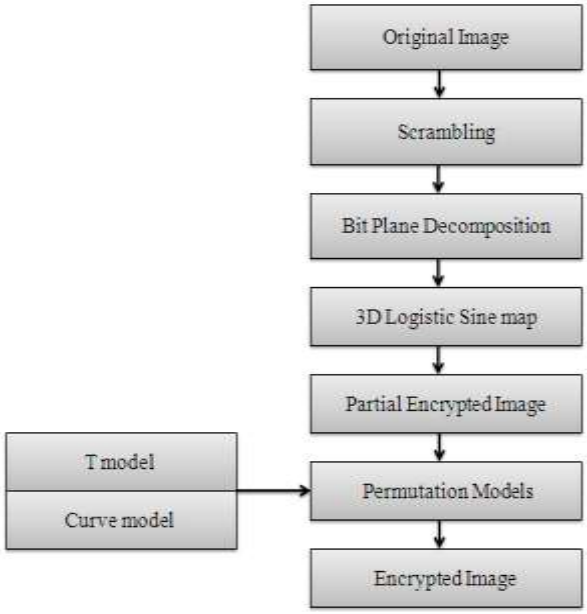


Fig-1: Image Encryption System

2.3 Bit plane decomposition

A non-negative decimal number d can be converted to a binary demonstration with n bits as follows,

$$N=\sum_{i=1}^{n} b_{i2^{i-1}} = b_1 2^0+b_2 2^1+b_3 2^2+\ldots\ldots\ldots\ldots b_n 2^{n-1} \quad (1)$$

For a grayscale image, pixel value ranges from 0 to 255 and thus each pixel can be represented by an 8-bit binary sequence [16]. Consequently, we can decompose a grayscale image into 8 bit-planes, where the i-th bit-plane is formed by the i-th bit of all pixels (i=1,2……8).

2.4 Random scrambling

Scrambling is a simple process to split the image into equal row and column by randomly, this process to enhance the secrecy. Be that as it may, scrambling the packed examined picture just improves encryption execution, while it overlooks improvement of pressure execution. The scrambling can be received to encode when the scrambling procedure can't be anticipated. Encryption process scrambles the substance of information, for example, content, picture, sound, and video to make the information mixed up or endless for the period of transmission.

2.5 Logistic sine map

Logistic calculated guide be obvious amid the majority well known riotous maps, especially, in picture encryption. Strategic guide has a decent disorganized conduct when 3.5699456<r<=4. Since r progressively close to 4, sequence is also better. The general straightforwardness of the strategic guide makes it a broadly utilized purpose of the section into a thought of the idea of the chaos.

2.6 Permutation models

In order to vary the pixel esteems, the calculation utilizes the dissemination property of map, wherever neighboring data is spread out [17]. The equal size of unique picture which rearranges the position of image pixels completely, the key stream created by riotous guide in the dissemination step relies upon both the key in addition to the basic-image [18].

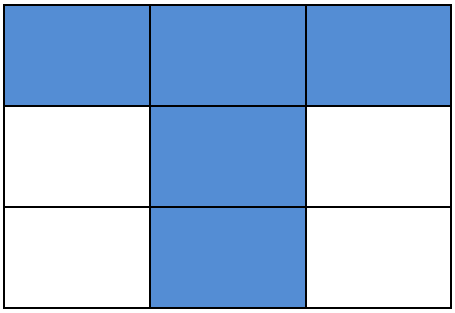


Fig-2: T model design

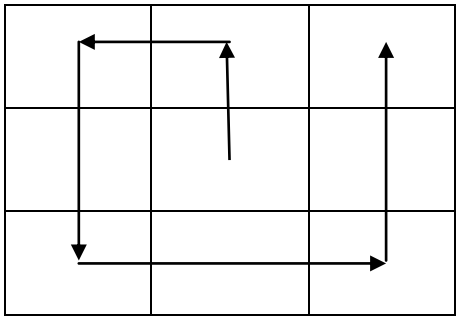


Fig-3: Curve design

PROPOSED ENCRYPTION ALGORITHM:

Step 1: The standard image are converted into gray scale image

Step 2: then the gray scale image are scrambled via scrambling purpose

Step 3: Next the bit plane disintegration process are performed after that the image are transform into ciphered image.

Step 4: The dispersion models of T are performed with in the ciphered image, after that the images are encrypted.

Step 5: finally the encrypted images of T representation propose to incorporate Curve model after that the image are encrypted.

DECRYPTION ALGORITHM

Step 1: perform opposite procedure of the encrypted image of T and Curve representation Design is decrypted

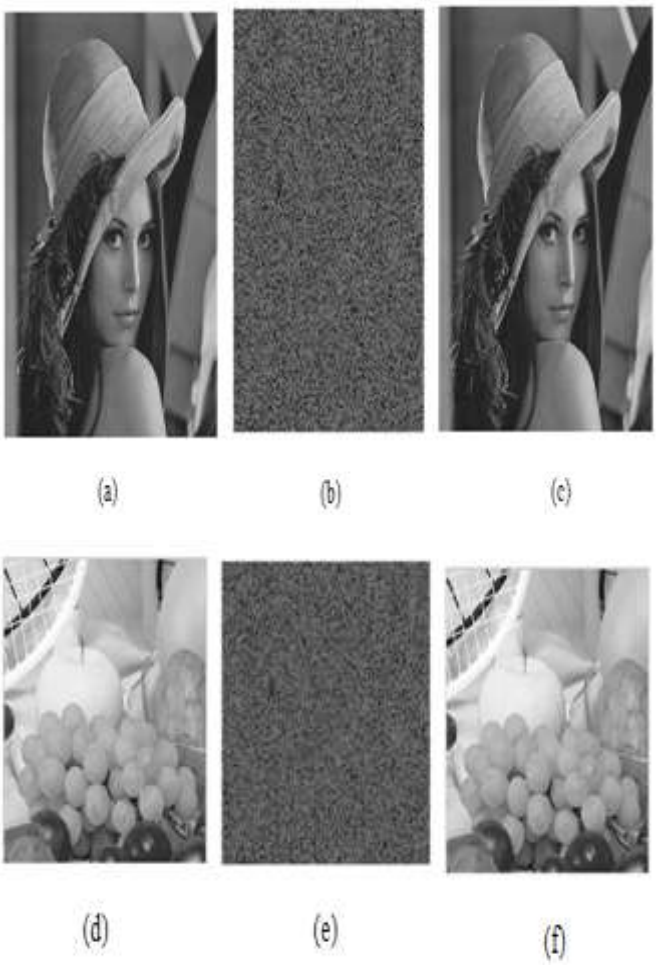
Step 2: The Decrypted image of T and Curve Models diffusion of cipher image is performing a bit plane disintegration process is performed.

Step 3: After that the cipher image are change into scrambled image of arbitrary scrambling.

Step 4: Finally, the scrambled images are changed into gray scale image, later than get into the original image.

3. RESULT AND DISCUSSION

Running speed is an important characteristic parameter for encryption algorithms The planned method have be implement using Matlab10 and speed performance has been measured on a personal computer with a 2.60 GHz Intel (R) Core (TM) i5-3320M CPU, 4 GB RAM, among Windows 7 as the operating system.



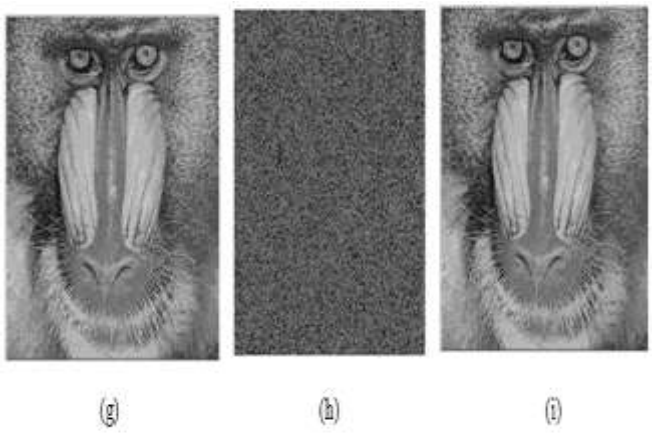


Fig-4: Experimental results: (a)standard picture Lena, (b) Encrypted image of (a), (c) Decrypted image of (b), (d) standard picture Fruits, (e) Encrypted picture of (d), (f) Decrypted picture of (e), (g)simple picture baboon, (h) Encrypted figure of (g), (i) Decrypted figure of (h).

3. 1 Histogram

An economical image encryption should noise similar toward output to attain an unvaried histogram. This histogram could be diagrams to facilitate the amount of pixels for every value that may be originate inside picture. The outputs of our algorithmic program for all the check images and their histograms are illustrated

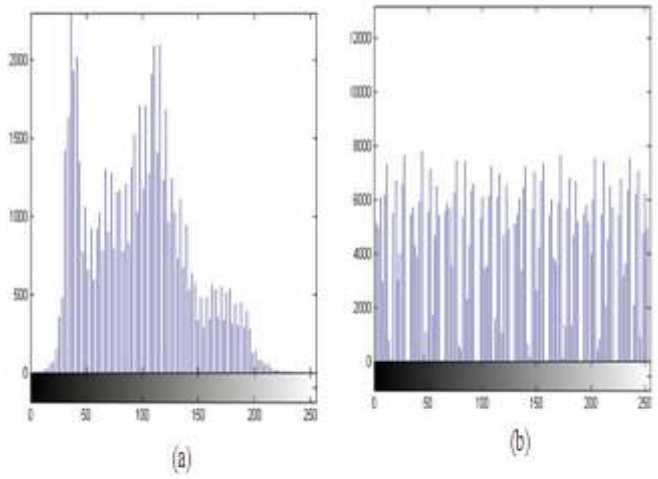


Fig-5: (a) Histogram of the Lena image, (b) Histogram of the encrypted image of (a).

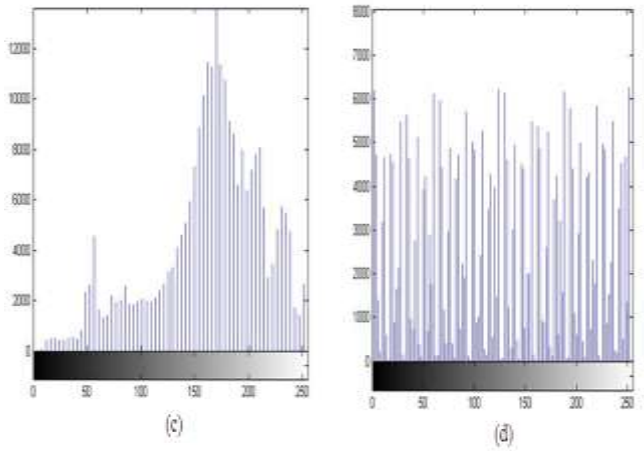


Fig-5: (c) Histogram of the Fruits image, (d) Histogram of the encrypted image of (c).

3.2 Information entropy

The information entropy able to be designed by,

$$G(m) = \sum_{i=0}^{2^n-1} x(m_i) log \frac{1}{x(m_i)} \quad (2)$$

In which g (m) represents the information entropy of an sequence source m, x (mi) denotes the probability of symbol mi.

On behalf of an unsystematic picture with 256 grey levels, the entropy ought to supremely be 8.

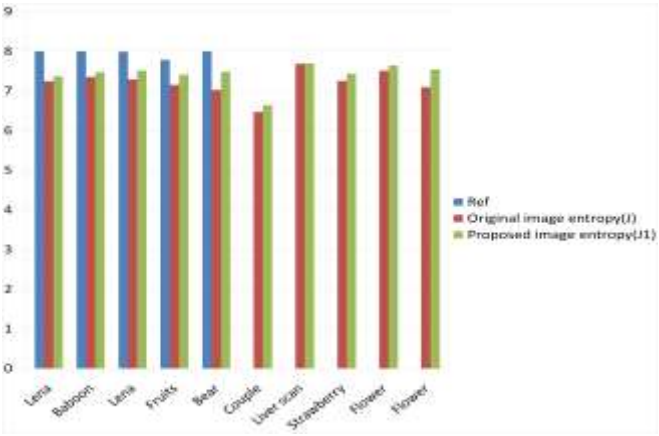


Fig-6: Entropy Analysis

3.3 Correlation analysis

Correlation could be an acquainted linear relationship that is employed to calculate the bond between two adjacent pixels in a picture. Because of high relationship connecting 2 adjacent pixels, plain image is susceptible to applied mathematics analysis attacks. An honest secret writing theme ought to break this relationship the maximum amount as potential. During this example, we have a tendency to indiscriminately choose a thousand pixels from the plain image and their encrypted image, and determine

the correlation coefficients in parallel, perpendicular and crosswise.

$$r_{x,y} = \frac{E((x-E(x))(y-E(y))}{\sqrt{D(x)D(y)}} \quad (3)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (4)$$

$$G(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \quad (5)$$

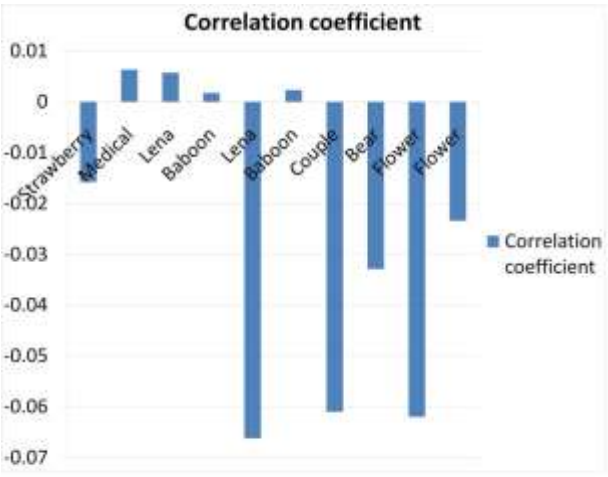


Fig-7: Correlation analysis

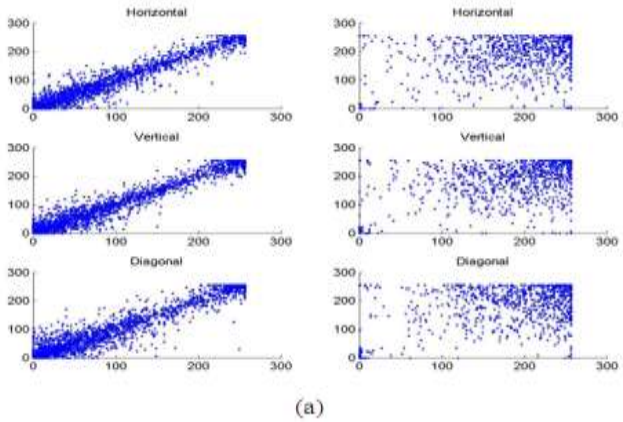


Fig-8: Correlation of adjacent pixel in Baboon

3.4 NCPR and UACI

The differential attack is a kind of chosen-plaintext attacks. The attackers sometimes attain plain image in order to transforming one pixel esteem, following the distinction between two figure pictures and utilizing the manufactured associations to recover the cipher-text not including secret key. There are two criteria for estimating the distinction connecting two figure pictures: number of pixels change rate (NPCR) and unified average changing intensity (UACI).

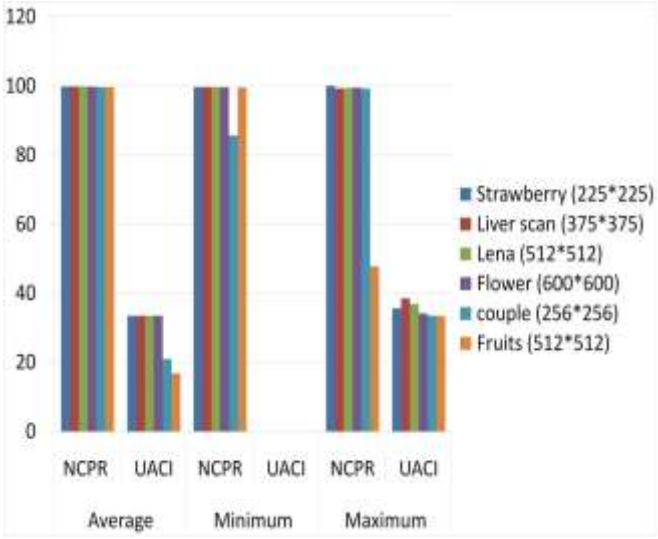


Fig-9: NCPR and UACI

3.5 Speed analysis and performance comparison

Running pace is a noteworthy trademark parameter for encryption calculations, when the security level may maybe the prerequisites. Logistic based image encryption scheme is used in this work. In the proposed algorithm, is explained based on diffusion process. This work leads to a security improvement when compared with other algorithms.

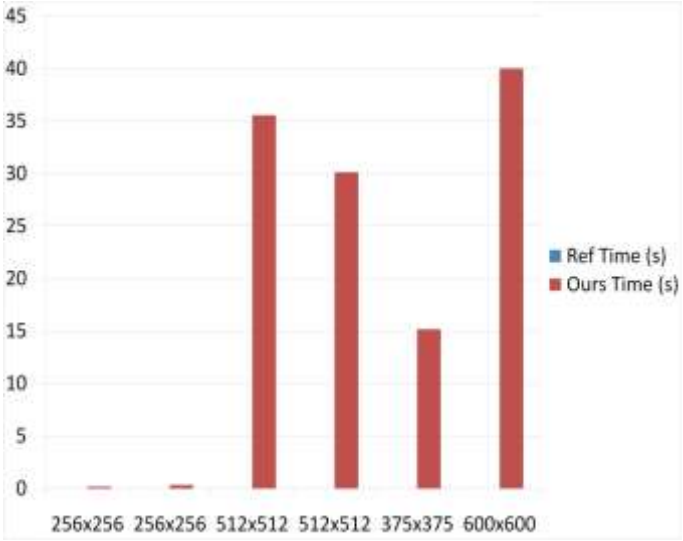


Fig-10: Speed Analysis

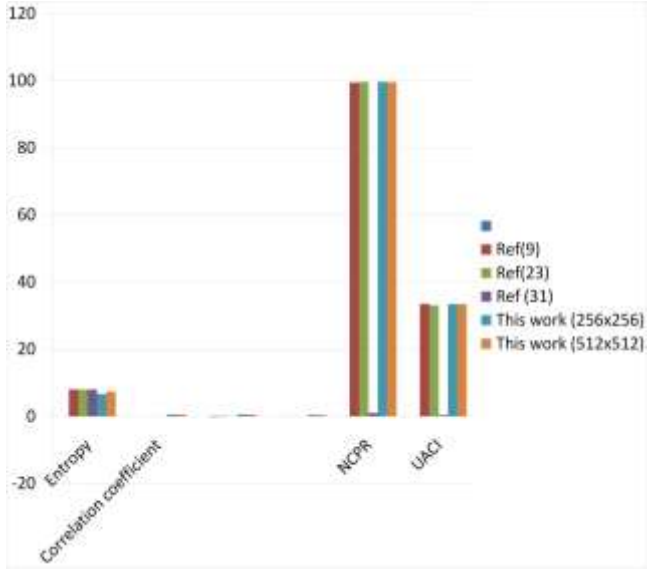


Fig-11: Comparison Analysis

4. CONCLUSION

The method use toward translate new picture into one more image which be not identifiable by illegal user. This paper presents a 3-D logistic picture encryption algorithm base scheduled simple diffusion models. A picture representation algorithm has been planned to give a protected cryptosystem to broadcast multiplicity of images. The dispersion procedure change corresponding pixel position. All these techniques help to design a more complex and secure cryptosystem to transmit the data over the insecure network. Designing the Pi model and X model diffusion on a chaotic system, the corresponding experimental results show that proposed image encryption scheme now increase the level of security and also time saved for this system. In future we are designing a multiple diffusion models to hybrid an image encryption systems and adding the segmentation based chaotic system.

REFERENCES

[1] Mingxu Wang, Xingyuan Wang, Yingqian Zhang, Zhenguo Gao, "A novel chaotic encryption scheme based on image segmentation and multiple diffusion models", journal of Optics and Laser Technology, vol. 108, 2018, pp. 558–573.

[2] Nanrun Zhou, Shumin Pan *et.al.,* "Image Compression-Encryption Scheme Based On Hyper-Chaotic System and 2D Compressive Sensing", Optics & Laser Technology, vol. 82, 2016, pp. 121-133.

[3] Junxin Chen, Yu Zhang, Lin Qi, Chong Fu, Lisheng Xu, "Exploiting Chaos-Based Compressed Sensing And Cryptographic Algorithm For Image Encryption And Compression", Journal of Optics & Laser Technology, vol.99, 2018, pp. 238-248.

[4] Guanrong Chen, Yaobin Mao, Charles K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos,Solitons &Fractals, vol. 21, Issue. 3, 2004, pp. 749-761.

[5] Muhammad Khurram Khan, Jiashu Zhang, Lei Tian, "chaotic secure content-based hidden transmission of biometric templates", Chaos, Solitons &Fractals, vol. 32, Issue. 5, 2007, pp. 1749-1759.

[6] Xuanping Zhang, Zhongmeng Zhao, "Chaos-based image encryption with total shuffling and bidirectional diffusion", Journal of Nonlinear Dynamics, vol. 75, 2013, pp. 319-330.

[7] K. Sakthidasan@Sankaran and B. V. Santhosh Krishna, "A new chaotic algorithm for image encryption and decryption of digital color images", International Journal of Information and Education Technology, vol. 1, Issue. 2, 2011, pp. 137-141.

[8] Zhenjun Tang, JuanSong, XianquanZhang, Ronghai Sun, "Multiple-image encryption with bit-plane decomposition and chaotic maps", journal of Optics and Laser Technology, vol. 80, 2016, pp. 1-11.

[9] Zhongyun Hua, Yicong Zhou, "Design of image cipher using block-based scrambling and image filtering", journal of Information Sciences, vol. 396, 2017, pp. 97-113.

[10] Xingyuan Wang, LintaoLiu, YingqianZhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique", Journal of optics and lasers in engineering, vol. 66, 2015, pp. 10-18.

[11] Chunhu Li, Guangchun Luo, Ke Qin, Chunbao Li, "An image encryption scheme based on chaotic tent map", Journal of nonlinear dynamics. Vol. 87, issue. 1, 2016, pp. 127-133.

[12] Narendra K Pareek, Vinod Patidar and Krishan K Sud, "Substitution-diffusion based Image Cipher", International Journal of network security & Its applications (IJNSA), Vol. 3, issue. 2, 2011, pp. 149-160.

[13] Prarthana Madan Modak, Dr. Vijaykumar pawar, "A comprehensive survey on image scrambling techniques", International journal of science and research (IJSR), vol. 4, issue. 12, 2015, pp. 814-818.

[14] Sourabh Chandra, Sk Safikul Alam, Debabrata Samanta, "Data hiding with pixel scrambling technique by modified shuffling", International journal of information science and intelligent system, vol. 3, issue. 2, 2014, pp. 1-3.

[15] Zhongyun Hua a , Yicong Zhou, " Design of image cipher using block-based scrambling and image filtering", Journal of Information science, vol. 396, 2017, pp. 97-113.

[16] Zhenjun Tang, JuanSong, XianquanZhang, RonghaiSun, "Multiple-image encryption with bit-plane

decomposition and chaotic maps", journal of optics and lasers in engineering, vol. 80, 2016, pp. 1-11.

[17] Guoji Zhang, Qing Liu, "A novel image encryption method based on total shuffling scheme", journal of Optics Communications, vol. 284, 2012, pp. 2775–2780.

[18] Benyamin Norouzi, Sattar Mirakuchaki, seyed, Mohammad Sevedzadeh Sevedzadeh, Mohammad Reza Mosavi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process", journal of Multimedia Tools Applications, vol. 73, issue. 3, 2014, pp. 1469-1497.

[19] Rim Zahmoul, Ridha Ejbali, Mourad Zaied, "Image encryption based on new Beta chaotic maps", journal of Optics and Laser in Engineering, vol. 96, 2017, pp. 39-49.

[20] Yicong Zhou n, LongBao,C.L.PhilipChen, "A new 1D chaotic system for image encryption", journal of signal processing, vol. 97, 2014, pp. 172-182.

[21] Rasul Enayatifar, Abdul Hanan Abdullah, Ismail Fauzi Isnin, "Chaos-Based Image Encryption Using A Hybrid Genetic Algorithm and DNA Sequence", journal of Optics and Laser Engineering, Vol. 56, 2014, pp. 83-93.

BIOGRAPHIES

Sharmila Banu A, M.E–Communication Systems, B.E–Electronics and Communication Engineering, Mount Zion College of Engineering and Technology.

Prem Kumar was born in India in 1984. He received a B. E degree in Electronics and Communication Engineering from Anna University Chennai 2005. He received the M. E degree in VLSI design from Anna University, Chennai in 2007. He is currently submitted the Ph. D thesis at Anna University, Chennai. His areas of interests are media, security, image processing, vlsi design, cryptography. He is the life time member of ISTE, IETE, and CSI.