Digital Image Security System Based on Logistic and Chebyshev Techniques

Dr. G. Nagaraju[1], P. Udaya Bhanu[2], M. Vaishnavi[3], R. Ravi Teja[3], K. Sai Rohit[3], R. Vineel kumar[3]

[1,2]Assistant Professor, [3]B. Tech Students

[1,3]Department of ECE, S.R.K.R. ENGINEERING COLLEGE (A), BHIMAVARAM, Andhra Pradesh, India.

[2]Department of EEE, S.R.K.R. ENGINEERING COLLEGE (A), BHIMAVARAM, Andhra Pradesh, India.

Abstract: **In this paper, we propose a new image encryption algorithm based on chaotic maps. It mainly uses two chaotic maps namely Logistic chaotic map and Chebyshev's chaotic map. A digital image is taken as input and is converted to grayscale image for easy implementation of operations. This encryption technique includes two main operations. Permutation at pixel level and masking. Permutation at bit level. This encryption algorithm includes Confusion and Diffusion processes. Confusion of pixels is done by using the Logistic chaotic map. And then diffusion key is generated based on Chebyshev's chaotic map to diffuse the pixels at bit level. By this proposed encryption scheme, an effective Cipher image is created with high-level security. Decryption is the reverse of encryption process. This Chaotic digital image encryption algorithm is implemented using MATLAB software. This encryption technique is tested for images of various sizes. This encryption technique is robust and also has ability to withstand various common attacks like differential, statistical and noise attacks.**

Keywords: **Digital image, Logistic, Chebyshev, encryption algorithm**

1. INTRODUCTION

With the rapid development of Internet and Communication technologies, digital image communication and its applications plays a vital role in transmission of information. Digital images are now used widely in various fields such as mobile internet, cloud computing, big data, social networking and multimedia [1]. Digital image transmission can undergo various attacks due to open nature of networks. However, security and reliability are the major aspects in every field, image encryption has attracted more attention [2]. The image encryption algorithms are classified into many functions like naive and selective where the keys are symmetric and asymmetric. The naïve function encrypts all the pixels of image where the selective function encrypts only the certain pixels. The selective function is fast but the naïve function is robust [3]. Various algorithms are available for encryption namely AES (Advanced Encryption Standard), DES (Data Encryption Standard), RSA (Rivest Shamir Adelman) which are well compatible for text. Digital images have intrinsic properties that are different from texts, such as bulk data and strong correlation among pixels, which make the traditional encryption techniques unsuitable [4]. Consequently, some interesting and promising theories such as chaotic systems are introduced and implemented in digital image encryption.

G. Nagaraju, et al., presented a paper on a New Watermarking Scheme for Medical Images with Patient's Details [5]. This work presents how to extract the characteristics and features of tumor image by general segmentation methods for malignant risk computation and presents the use of digital watermarking for applica-tions of automated tumor image analysis. Here personal information such as name, age, gender, location, ADHAAR number, contact number etc., and tumor information such as tumor types, area of the tumor, severity, and any other useful information are embedded to the tumor image. Encrypting that image with well-known encryption algorithms is also possible to avoid unnecessary nuisance from information hackers. Chaos has great properties such as ergodicity, high randomness, high sensitivity to initial conditions and control parameters and low computational complexity. And thus, many encryption techniques are proposed based on the chaotic maps [6]. Matthews proposed one-dimensional chaotic map for image encryption [7]. Wang implemented a colour image encryption based on logistic map [8]. Liu developed a colour image encryption by combining spatial bit-level permutation and high-dimensional chaotic systems [9]. And many more encryption techniques are suggested based on a single chaotic map or a chaotic system in combination with DNA encoding, Henon map, Arnold map, Lorentz systems, etc.

Chaotic systems exhibit non-linear performance, thus resulting in unpredictable behaviour. Even chaotic system has lot of advantages, it is deficient in security when it is used alone. A chaotic map can confuse only a single image pixel which does not ensure high security and confidentiality. It will be prone to various threats and can be cracked by attackers easily by using pixel comparison method [10]. Nagaraju, G. et al., suggested an algorithm [11] which proposes a new way to image encryption with reversible data hiding (IERDH) scheme with a unique private key in RGB images. A room is allocated in medical image for embedding the data by combining 2-level discrete wavelet transform and 4x4 discrete cosine transform. For any medical images, the patient details are also important to store along with actual image. So, these details are imported from excel sheet, and encrypted with the help of carrier image which is generated by special key.

This Cipher data image is embedded into allocated transformed image. Combine the individual components to get the transmitted medical image with hidden patient's details. Reverse is possible to restore patient's details from received medical image. Hence, we proposed an algorithm using two chaotic maps, Logistic chaotic and Chebyshev's chaotic map. This digital image encryption algorithm ensures high-level security and can resist various common attacks [12]. G. Nagaraju, et al., recommended an intelligent image watermarking approach [17] for secured chaotic-based medical images with patient details is proposed. The method uses combination of a non-sub sampled type contourlet transformation (NSCT), and a redundant discrete wavelet transformation (RDWT) with singular value decomposition (SVD) to present acceptable development in heartiness and indistinctness. Also, security is guaranteed by applying an encryption procedure dependent on 2D maps confused co-ordinations in therapeutic picture watermark. In our methodology, the host picture was initially partitioned into subpictures and NSCT executed on most extreme entropy sub-pictures have. At that point RDWT is actualized for picture NSCT and particular vectors of RDWT coefficients are determined. Indistinguishable procedure applied to the watermark picture. Solitary esteems of the two watermarks are incorporated into the host framework is singular. Execution assessment shows this procedure when assaulted, by consolidating NSCT, RDWT, SVD and disordered encryption, this methodology makes a solid, undetectable, sheltered and custom fitted to the wellbeing the board application.

Ramaraju PV, et al., proposed an Advanced Image Encryption Algorithm [22] which deals with the secrecy of images, so image encryption is the best technique for information hiding. The novelty of the work lies in generating key images for encryption. Here the key image is created with the help of secret alphanumeric keyword. Each alphanumeric key will be having a unique 8bit value generated by Binary key table. Problem is to be investigated and resolved is how to get the image encryption algorithm which is simple yet safe, with the lightweight and efficient computing. This encryption algorithm which combines Playfair cipher and the Vigenere cipher gives better results. The experimental results showed a correlation between the elements of the image after encryption has decreased significantly. The average of quality of encryption showed that the rate of change of image pixels is high enough so that cipher image difficult tidentify. The resulting image is found to be more distorted in this technique. By applying the reverse process, we get the decrypted image. G. Nagaraju, et al., recommended an Optimized Image Watermarking Scheme Based on IWT and DCT [27], which proposed a combined watermarking scheme of images based on Integer wavelet transform and discrete cosine Transforms. The imperceptibility of image changes according to different values of the scaling factor that is used in embedding. We choose an optimised scaling factor that gives us a good imperceptibility of the watermarked image as well as good capacity and robustness.

G. Nagaraju, et al., presented a paper on Secure hybrid watermarking technique in medical imaging [30], in which the algorithm explored two main fields that, the encryption of medical images using DNA Encoding and Spatiotemporal Chaos Algorithm and the embedding of medical images in cover image using hybrid transformation of NSCT, RDWT and SVD. The goal of this study was to develop a methodology to improve the robustness, imperceptibility and security for medical information without implementing a physical model, thus saving time, money and reducing the risks associated with hacking partners. In this paper, patient health document as one watermark and his medical image as another watermark are used. The theoretical model has demonstrated that it is possible to use this type of technique and apply it to a complex digital image transmission. The correlation observed before and after encryption and embedding procedures. Experimental results show how robustness and imperceptibility and security of medical images are improved.

In the proposed algorithm, a random sequence is created using logistic map function to confuse the image pixels. And then the diffusion key is generated using the Chebyshev map equation to diffuse the image pixels at bit level. Finally, we obtain an effective Cipher image with high security, which is encrypted from a grayscale image. Decryption is the inverse process of encryption. Decryption is the process done on obtained cipher image to extract the original grayscale image at the receiver end. The original grayscale image can be extracted from the cipher image only when the key value is exactly matched. Key value includes the control parameters, initial conditions for chaotic maps. This encryption scheme is tested on images of various sizes. The results of this encryption algorithm have proven that this technique has benefits such as simple implementation, robustness, less complexity, time compatible and high security.

In this paper, we discuss the chaotic systems used in our encryption algorithm in sections 2 and 3. Image encryption algorithm and its simple representation is given in section 4. The Experimental results, algorithm performance and security analysis are conducted in section 5 respectively.

2. LOGISTIC CHAOTIC MAP

The Logistic map is a polynomial map of order two [13]. It generates a one-dimensional non periodic chaotic sequences which are random in nature.

The mathematical representation of this map is as follows [14,15] :

$$Xn+1 = \mu \; Xn \; (1- Xn). \quad n = 1, 2, \ldots.. \quad (1)$$

μ is the bifurcation parameter where $0 < \mu <= 4$, Xn Є (0, 1). When $3.57 <= \mu < 4$, the map exhibits chaotic behaviour [16].

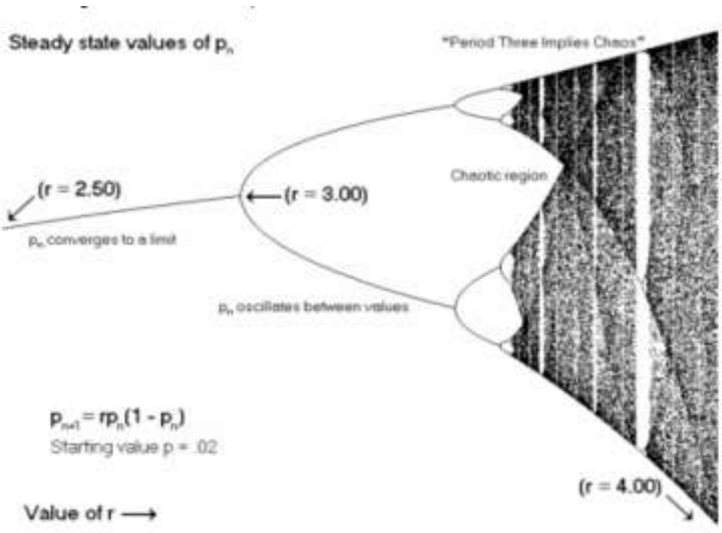


Figure 1: Bifurcation diagram for equation 1.

This algorithm uses logistic map equation to confuse the pixels of original grayscale image. For example,
Step 1: Let the size of grayscale image be M x N.

$$S = \{1, 2, 3, \ldots\ldots\ldots M * N\} \qquad (2)$$

Step 2: Generate a pseudorandom sequence of respective size using the logistic equation.

$$A = \{A1, A2, A3, \ldots\ldots\ldots As\} \qquad (3)$$

Step 3: Sort the sequence A and obtain their positions.

$$Index = \{I1, I2, I3, \ldots\ldots Is\} \qquad (4)$$

This is used to find the first largest number of sequence A and place it in the position of I1. Second largest number is placed in I2 and every value is confused accordingly. The confused pixels are then diffused using second chaotic system called Chebyshev map.

3. CHEBYSHEV'S CHAOTIC MAP

The mathematical expression of Chebyshev's map is given as:

$$Zn+1 = \cos (\omega \text{ x } \arccos (Zi)) \qquad (5)$$

Where $-1 <= Zi <= 1$, $2<= \omega <= 6$. When ω Є [2, 6] Chebyshev's map exhibits chaotic behaviour [18]. In a condition of infinite computational accuracy, this map can produce an infinite length, nonperiodic, chaotic real-valued sequence [19]. Hence, Chebyshev's map is very useful in digital image encryption.

In this algorithm, this Chebyshev's chaotic map is mainly used to diffuse the image pixels. A diffusion key is generated using this map, using which the confused grayscale image is then diffused.

4. IMAGE ENCRYPTION AND DECRYPTION ALGORITHM:

Step1: Take input image of size M x N. Convert it into grayscale image of size M x N.
Step2: Convert the grayscale image into 2 one dimensional arrays to represent rows and columns.
Step3: Iterate equation (2) to generate random sequence of numbers by taking initial values of x (1) =0.7 and μ =3.62
Step4: Sort the sequence in descending order and obtain the index values and confuse the original image with these values.
Step5: Iterate the equation (5) with the initial parameters of ω=3.628 and z (1) =0.632.
Step6: Obtain the vector Z by using the formula Z=abs(round(k*255)). abs(x) return the absolute value of each element in array. Round(x) is used to round each element of x to the nearest integer.
Step7: Convert the value of z to binary and shift the values circularly for diffusion. Convert the binary values into decimal and stores them in a temporary vector.
Step8: Obtain the key value by perform the ex-or operation between elements of z and elements of temporary vector. This step completes the diffusion process.
Step9: In this step we perform the ex-or operation between the key value and original image values. This step produces the cipher image which is the result of encryption.
Step 10: Decryption is the reverse process of encryption.

Step11: Obtain the correlation coefficient and entropy values of the encrypted image and also obtain the histograms of original and encrypted images.

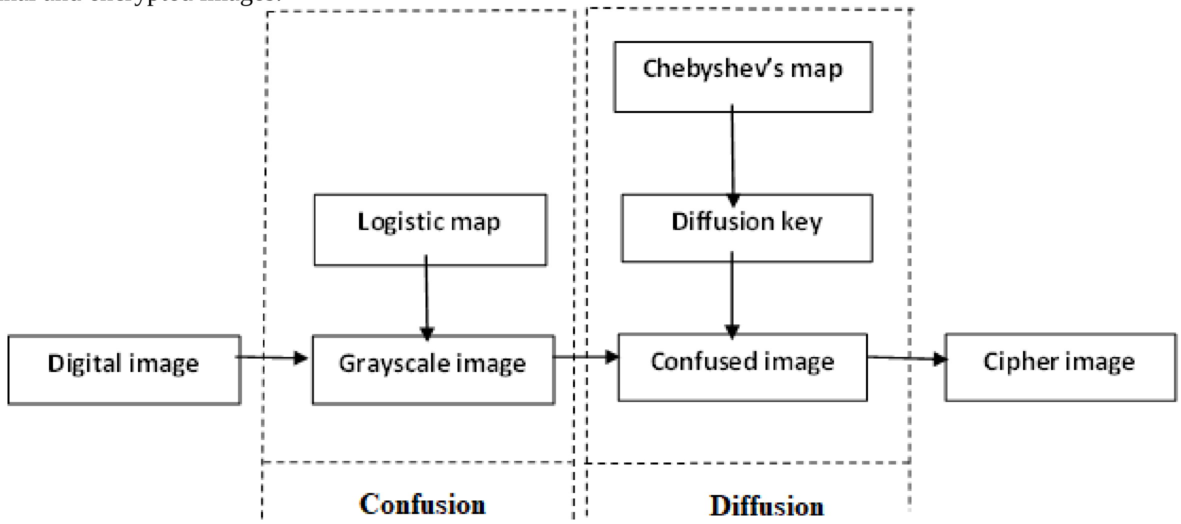
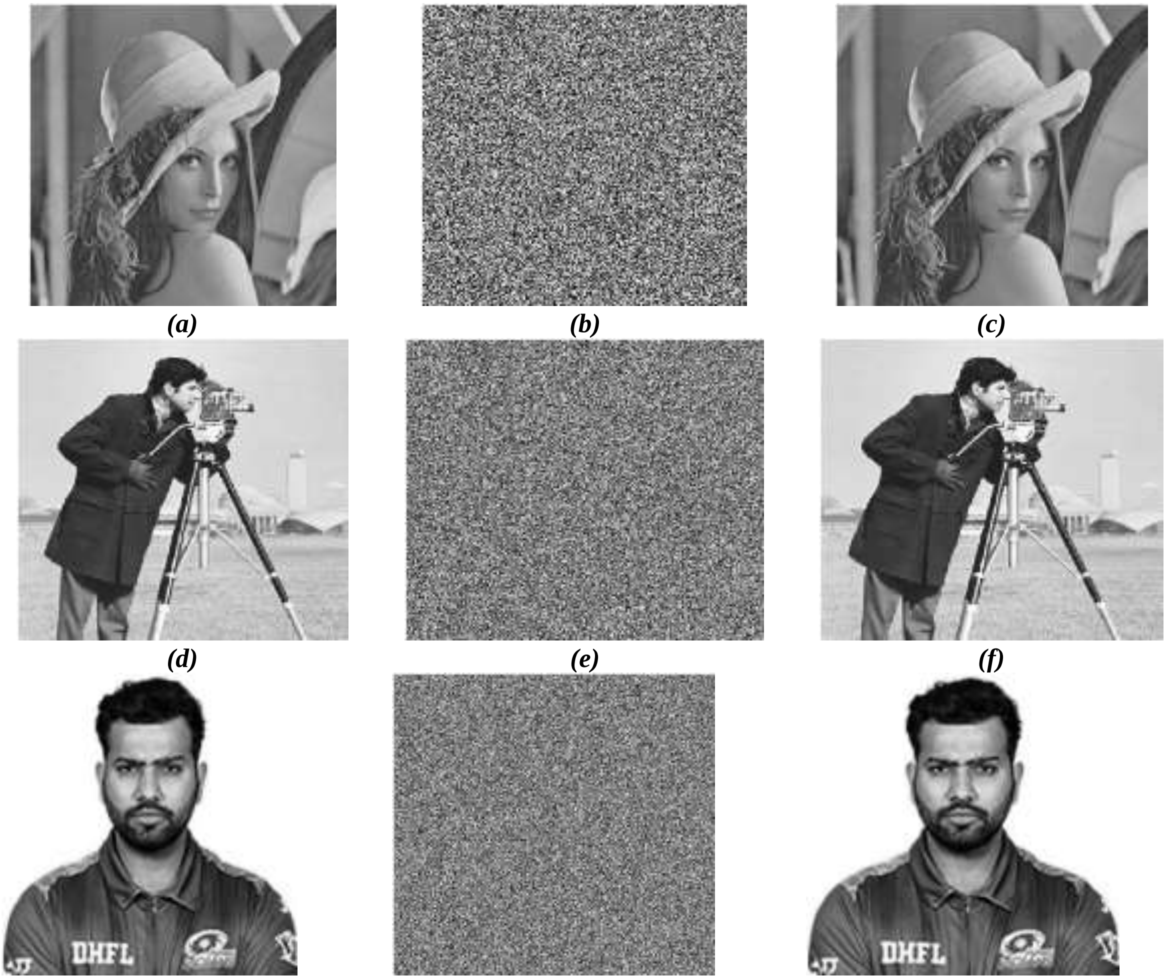


Figure 2: Block diagram for proposed encryption algorithm.

5. EXPERIMENTAL RESULTS:

In our algorithm, we have set the initial values of logistic map; x (1) =0.7, µ=3.62 and for the Chebyshev map the initial values are ω=3.628 and z (1) =0.632. The input grayscale image is of size 256 x 256. The original, encrypted and decrypted images are shown in figure 3. From the results we can conclude that the plain image can be decrypted without distortion.



(a) *(b)* *(c)*

(d) *(e)* *(f)*

(g) *(h)* *(i)*

Figure 3: Experimental Results. (a) Lena plain image, (b) Lena cipher image, (c) Decrypted Lena image,

(d) Cameraman plain image, (e) Cameraman cipher image, (f) Decrypted Cameraman image, (g) Rohit plain image, (h) Rohit cipher image, (i) Decrypted Rohit image.

6. SECURITY ANALYSIS:

6.1 Histogram Analysis:

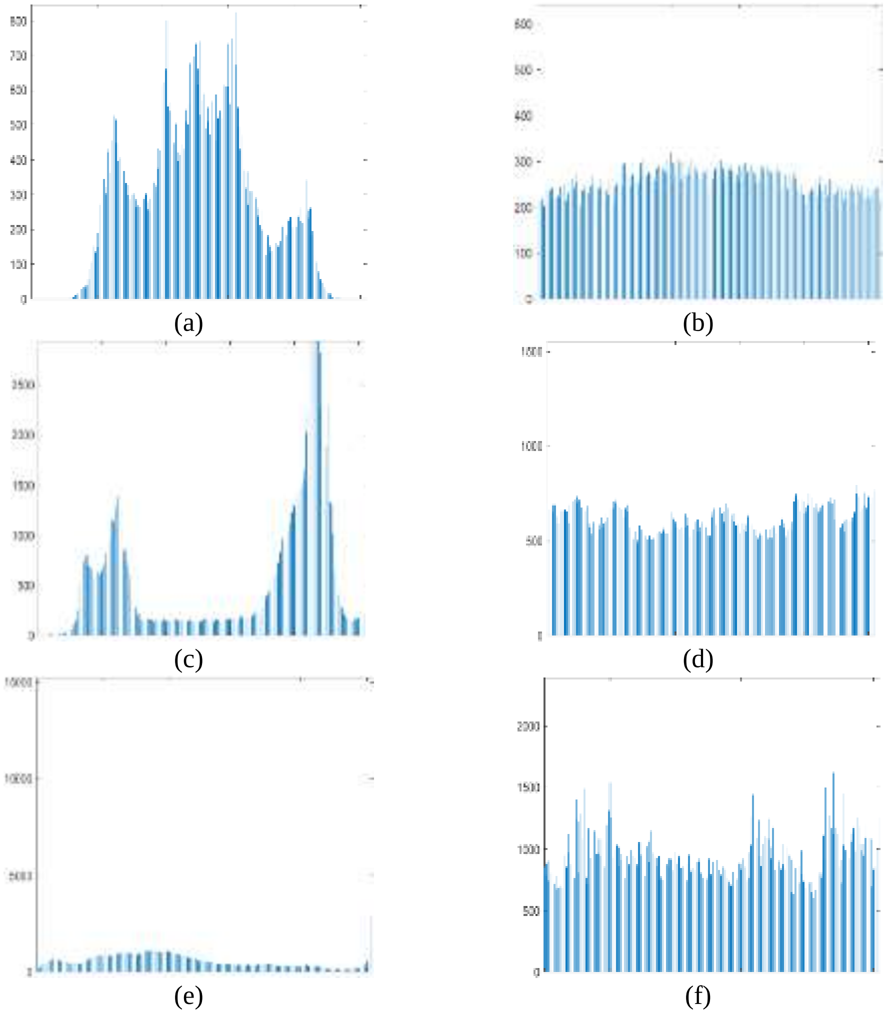


Figure4: Histogram analysis. (a) Histogram of Lena plain image, (b) Histogram of Lena cipher image, (c) Histogram of Cameraman plain image, (d) Histogram of Cameraman cipher image, (e) Histogram of Rohit plain image, (f) Histogram of Rohit cipher image.

6.2 Image entropy analysis: The entropy or average information of an image is a measure of the degree of randomness in the image. According to Shannon's theory entropy of a source is obtained by the following equation

$$H(x)=\sum_{i=0}^{2^n-1} p(xi)\log 1/p(xi) \qquad \rightarrow(6)$$

P(xi) is the probability of symbol xi and N represents the number of bits to represent symbol. According to the equation 1 the entropy for a random image which is having 256gray levels is 8. For the cameraman image the entropy of the encrypted image shown in figure 1(d) is 7.9909 and it is very close to 8 which tells that the cipher image is closer to the original image. We have conducted the entropy test for different images and the results are listed in table 1. All the listed entropy values are closer to 8 which shows that the data leakage in the encryption process is very less and the encryption process can resist entropy attack.

IMAGE	ENTROPY
Lena	7.9920
Cameraman	7.9909
Rohit	7.9728
Ship	7.9625

Table 1: Entropy analysis of different images

6.3 Correlation analysis: In this analysis we randomly select some adjacent pixels of both the plain and cipher images and we will calculate the correlation coefficient of both the images. Correlation analysis will be performed on images in horizontal, vertical and diagonal directions. In this paper we have selected 2000 adjacent pixels in horizontal, vertical and diagonal directions from both the plain and cipher images. Correlation coefficient can be calculated by using the equation.

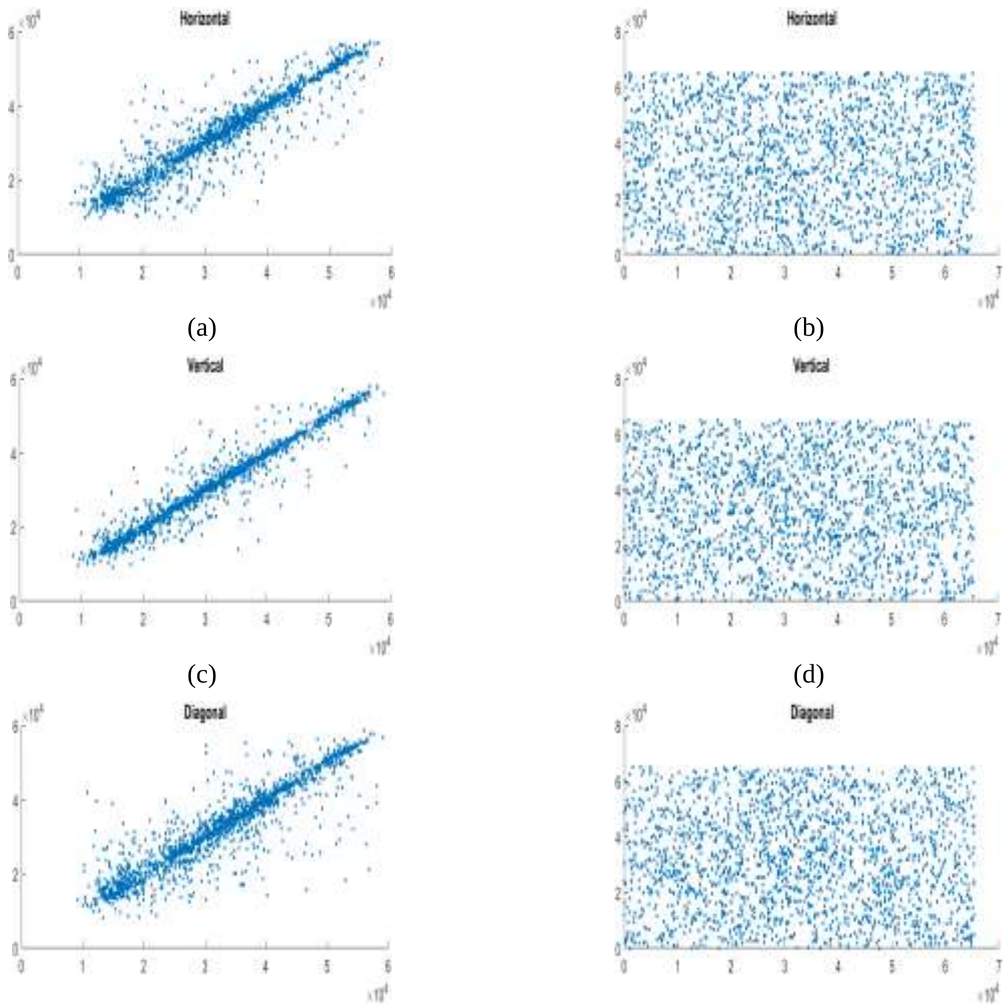
$$correlation = \frac{cov(x,y)}{}\sqrt{D(x)}*\sqrt{D(y)} \rightarrow (7)$$

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})$$

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

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N}x_i$$

Where x and y are the grey values of pixels and N is the number of selected pairs. Correlation analysis for Lena image is performed along the horizontal, vertical and diagonal directions and their distributions are shown in figure5.



(a)

(b)

(c)

(d)

(e)

(f)

Figure5: (a) Correlation analysis of plain image along horizontal direction (b) Correlation analysis of cipher image along horizontal direction (c) Correlation analysis of plain image along vertical direction, (d) Correlation analysis of

cipher image along vertical direction (e) Correlation analysis of plain image along diagonal direction (f) Correlation analysis of cipher image along diagonal direction

6.4 Differential Analysis: The result of the encryption scheme is that the encrypted image should not be recognised by the hacker which means that both the original and encrypted images should not be identical. The difference between the images can be measured by obtaining NPCR and UACI values for the plain and cipher images. NPCR is defined as number of pixels change rate. Larger values of NPCR make sure that the encryption scheme can resist plain text attack. UACI is defined as the unified average changing intensity. UACI is the change rate of the average strength of the original and encrypted images. Large values of UACI make sure that the encryption scheme can resist differential attacks. NPCR and UACI values are calculated by using the equations 8&9.

$\text{NPCR}= (\sum_{ij} D(i,j)/S)*100 \quad \rightarrow(8)$
$\text{UACI}= 1/S[\sum_{ij} (|c(I,j)-c'(I,j)|/255)]*100 \rightarrow(9)$
$S=1/W*H$
Where W and H denotes the Width and height of the image. C and C' are the encrypted images before and after one pixel of the plain image is changed. We have calculated the both the NPCR and UACI values for different images and those values are listed in the table 2. We also calculated the cross- correlation coefficient for different images and those values are also listed in table 2.

7. CONCLUSION

In this paper we proposed an encryption algorithm based on pixel confusion and diffusion. In this algorithm plain image is taken as input and it is converted to grey scale image. This algorithm involves the usage of Logistic map and Chebyshev map. Logistic map is used for confusing the pixels of plain image. Chebyshev map is used to produce a diffusion key. After the diffusion we obtain the cipher image by performing the ex-or operation between the bits of key and image. Decryption process is the reverse process of encryption. The experimental results shows that our encryption scheme produces good encrypted images and it can resist common attacks. Therefore, this mechanism is good enough to be applied in image encryption.

REFERENCES:

[1] Y. Liu, X. Tong, and S. Hu, "A family of new complex number chaotic maps, based image encryption algorithm," Signal Processing: Image Communication, vol. 28, no. 10, pp. 1548–1559, 2013.

[2] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," Signal Processing, vol. 97, pp. 172–182, 2014.

[3] M. Babu, G. Shamala devi, M. Yamini krishna, M. Viswa Prasanna, N. Iswarya, "Image Encryption using Chaotic maps and DNA encoding", 2020.

[4] M. Kar, A. Kumar, D. Nandi, M. K. Mandal, "Image encryption using DNA coding and Hyperchaotic systems", IETE Technical review, 37:1, 12-23, 2018.

[5] G. Nagaraju, P. Pardhasaradhi, V.S Ghali, "A New Watermarking Scheme for Medical Images with Patient's Details", International Journal of Engineering& Technology, 7(3.31), (2018), 25-29.

[6] Chunyan Song, Yulong Qiao, "A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos", 2015.

[7] Matthews, R. On the derivation of a chaotic encryption algorithm. Cryptologia 1989, 13, 29–42.

[8] Wang, X.Y.; Lei, Y.; Liu, R.; Kadir, A. A chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn. 2010, 62, 615–621.

[9] Liu, H.J.; Wang, X.Y. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt. Commun. 2011, 284, 3895–3903.

[10] Heping Wen, Simin Yu, Jinhu Lu, "Breaking an image encryption algorithm based on DNA encoding and spatiotemporal chaos", 2019.

[11] Nagaraju, G. & Pardhasaradhi, P. & Venkata subbarao, Ghali. (2019). ERDH in medical images based on 2-D compound transform domain technique. International Journal of Recent Technology and Engineering. 7. 1571-1577.

[12] Jian Zhang, DongXin Fang, Honge Ren, "Image encryption algorithm based on DNA encoding and chaotic maps", vol. 2014, Article ID 917147.

[13] L. Liu, Q. Zhang, and X. Wei, "A RGB image encryption algorithm based on DNA encoding and chaos map," Computers and Electrical Engineering, vol. 38, no. 5, pp. 1240–1248, 2012.

[14] A. A. Abd El-Latif, L. Li, N. Wang, Q. Han, and X. Niu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces," Signal Processing, vol. 93, no. 11, pp. 2986–3000, 2013.

[15] M. Franc¸ois, T. Grosges, D. Barchiesi, and R. Erra, "A new image encryption scheme based on a chaotic function," Signal Processing: Image Communication, vol. 27, no. 3, pp. 249–259, 2012.

[16] S. Rohith, K N Hari Bhat, A Nandini Sharma, "Image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of linear feedback shift register", IEEE 2014.

[17] G. Nagaraju, P. Pardhasaradhi, V. S. Ghali, Sateeshkumar Deevi, "An Intelligent Watermarking Technique for Secured Medical Images with Patient Health Document". The Journal of Research on the Lepidoptera 51(3), 1-17(2020).

[18] H. Liu and X. Wang, "Color image encryption based on onetime keys and robust chaotic maps," Computers & Mathematics with Applications, vol. 59, no. 10, pp. 3320–3327, 2010.

[19] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," Applied Soft Computing Journal, vol. 12, no. 5, pp. 1457–1466, 2012.

[20] I. Hussain, T. Shah, and M. A. Gondal, "Application of S-box and chaotic map for image encryption," Mathematical and Computer Modelling, vol. 57, no. 9-10, pp. 2576–2579, 2013.

[21] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," Signal Processing, vol. 92, no. 4, pp. 1101–1108, 2012.

[22] Ramaraju PV, Nagaraju G, Chaitanya RK. Image Encryption and Decryption using Advanced Encryption Algorithm. Discovery, 2015, 29(107), 22-28.

[23] M. Shan, J. Chang, Z. Zhong, and B. Hao, "Double image encryption based on discrete multiple-parameter fractional Fourier transform and chaotic maps," Optics Communications, vol. 285, no. 21-22, pp. 4227–4234, 2012.

[24] S. Mazloom and A. M. Eftekhari-Moghadam, "Color image encryption based on coupled nonlinear chaotic map," Chaos, Solitons and Fractals, vol. 42, no. 3, pp. 1745–1754, 2009.

[25] Q. Zhang, Q. Wang, and X. Wei, "A novel image encryption scheme based on DNA coding and multi-chaotic maps," Advanced Science Letters, vol. 3, no. 4, pp. 447–451, 2010.

[26] A. Bakhshandeh and Z. Eslami, "An authenticated image encryption scheme based on chaotic maps and memory cellular automata," Optics and Lasers in Engineering, vol. 51, no. 6, pp. 665–673, 2013.

[27] G. Nagaraju, Dr. P.V. Ramaraju, P. Udaya Bhanu, Y.S.V. Satyavathi, T.Srinadh, K.Ganesh, K.Hari Subrahmanyam, "Optimized Image Watermarking Scheme Based on IWT and DCT". International Journal of Advanced Science and Technology 29(4), 132-147 (2020).

[28] W. Chen, C. Quan, and C. J. Tay, "Optical colour image encryption based on Arnold transform and interference method," Optics Communications, vol. 282, no. 18, pp. 3680–3685, 2009.

[29] Thakur S, Singh AK, Ghrera SP, Elhoseny M (2018). Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. Multimed Tools Appl., 78(3): 3457-3470.

[30] G. Nagaraju, P. Pardhasaradhi, V. S. Ghali, and G.R.K Prasad, "Secure hybrid watermarking technique in medical imaging", Eur. J. Mol. Clin. Med, vol.07, no. 05, pp. 160-176, 2020.

ABOUT AUTHORS:

Dr. G. NAGA RAJU

Presently working as assistant professor in Dept. of ECE, S.R.K.R. Engineering College, Bhimavaram, AP, India. He received B.E. degree from S.R.K.R Engineering College, Bhimavaram in 2002, M.E. degree in Computer electronics specialization from Govt. College of Engg., Pune University in 2004 and Doctorate from Department of ECE, KL University, Vaddeswaram in 2021. His current research interests include Image processing, digital security systems, Signal processing, Biomedical Signal processing, and VLSI Design.

P. UDAYA BHANU

Presently working as assistant professor in Dept. of EEE, S.R.K.R. Engineering College, Bhimavaram, AP, India. She received B. Tech degree from DNR College of Engineering and Technology, Bhimavaram in 2016, and M. Tech degree in Power Systems and Automation specialization from S.R.K.R Engineering College, Bhimavaram in 2018. Her current research interests include Signal processing, Image processing, Power systems and Automation.

M. VAISHNAVI

Currently pursuing B. Tech in Electronics & Communications Engineering from S.R.K.R. Engineering College, Bhimavaram, Andhra Pradesh, India.

R. RAVI TEJA

Currently pursuing B. Tech in Electronics & Communications Engineering from S.R.K.R. Engineering College, Bhimavaram, Andhra Pradesh, India.

K. SAI ROHIT

Currently pursuing B. Tech in Electronics & Communications Engineering from S.R.K.R. Engineering College, Bhimavaram, Andhra Pradesh, India.

R. VINEEL KUMAR

Currently pursuing B. Tech in Electronics & Communications Engineering from S.R.K.R. Engineering College, Bhimavaram, Andhra Pradesh, India.