Chaotic Map Scheme for Image Encryption

Hem Lata[1], Poonam choudhary[2]
[1]*Mtech Scholar,* [2]*Assistant Professor*
[12]*Sirda Institute of Engineering Technology, Sundernagar, Mandi H.P*

Abstract- The image contains sensitive information which can be stolen by the attacker and can be misused. The image encryption is the approach which provides security to the image data. The chaotic map is the encryption scheme which can divide the whole image into certain points and encrypt each path individually. This leads to increase security of the image data. The chaotic map encryption scheme does not use image features for encryption. In this research work, feature extraction algorithm is used with chaotic maps for encryption. The proposed algorithm is implemented in MATLAB and results are analyzed in terms of various parameters. It is analyzed that the proposed algorithm performs well in terms of all parameters.

Keywords- Chaotic maps, Image encryption, Feature extraction.

I. INTRODUCTION

Image Processing is a method to enhance raw images received from cameras/sensors set on satellites, space probes and air ships or pictures taken in normal day-today life for different applications. Different methods have been developed in Image Processing amid the last four to five decades. A digital remotely sensed image is commonly composed of picture elements (pixels) located at the intersection of every row i and column j in every K groups of imagery. Associated with every pixel is a number known as Digital Number (DN) or Brightness Value (BV) that depicts the average radiance of a relatively small area inside a scene [1]. A smaller number indicates low average radiance from the area and the high number is an indicator of high radiant properties of the area. The size of this area impacts the reproduction of details inside the scene.Cryptography is normally referred as "the study of secret". The world has globally connected with internetworking, where in sharing of data has turned out to be more important .Internet is used in different approaches to increase in the growth of the business. The networks have turned out to be more tasks critical and more vulnerable to malicious intents [2]. The rapid growth of computer networks permitted large files, for example, digital images, to be effectively transmitted over the web .Data encryption is broadly used to ensure security be that as it may, the vast majority of the accessible encryption calculation are used for text data. Cryptography is typically referred as "the study of secret". The world has globally connected with internetworking, where in sharing of data has turned out to be more important. Web is used in different approaches to increase in the growth of the business. The networks have turned out to be more tasks critical and more vulnerable to malicious intents. The rapid growth of computer networks permitted large files, for example, digital images, to be effectively transmitted over the web [3].Data encryption is broadly used to ensure security nonetheless, the majority of the accessible encryption calculation are used for text data. Image encryption schemes have been progressively studied to take care of the demand for real –time secure picture transmission over the internet and through remote networks. Encryption is the process of transforming the information for its security with the immense growth of computer networks and the latest advances in digital innovations, an enormous measure of digital data is being traded over the different kind of networks The security of digital picture has turned out to be increasingly important because of rapid evolution of the internet in the digital world today [4]. The security of digital images has pulled in more consideration as of late, and a wide range of picture encryption methods have been proposed to enhance the security of these images. Picture encryption techniques try to convert a picture to another that is difficult to understand. Then again, picture decryption retrieves the original picture from the encrypted one. There are different picture encryption systems to encrypt and decrypts the data and there is no single encryption algorithm satisfies the different picture types [5]. Taking after are the different goals of encryption/decryption which are ordinarily used for images.Feature extraction is done after the preprocessing phase in character recognition system. The primary errand of pattern recognition is to take an input pattern and accurately assign it as one of the conceivable output classes. This process can be divided into two general stages: Feature selection and Classification. Feature selection is critical to the entire process since the classifier won't have the capacity to perceive from poorly selected features [6]. Criteria to pick features given by Lippman are: "Features ought to contain information required to distinguish between classes, be insensitive to irrelevant variability in the input, and furthermore be limited in number, to permit, efficient computation of discriminant functions and to limit the amount of training data required" Feature extraction is an important step in the construction of any pattern classification and aims at the extraction of the relevant information that characterizes each class. In this process relevant features are extracted from objects/alphabets to form feature vectors [7]. These feature vectors are then used by classifiers to perceive the input unit with target output unit. It

ends up plainly simpler for the classifier to classify between different classes by taking a gander at these features as it allows genuinely easy to distinguish. Diagonal based feature extraction technique: Every character image of size 90x 60 pixels is divided into 54 measures up to zones, each of size 10x10 pixels as appeared in figure 8. The features are extracted from each zone pixels by moving along the diagonals of its individual 10 x 10 pixels. Each zone has 19 diagonal lines. Fourier descriptor is generally used for shape examination. The Fourier transformed coefficients form the Fourier descriptors of the shape [8]. These descriptors represent the shape in a frequency domain. Principal Component Analysis (PCA) is a scientific procedure that uses an orthogonal transformation to convert a set of observations of perhaps correlated variables into a set of estimations of uncorrelated variables called principal components.

II. LITERATURE REVIEW

Mohamed A. Mokhtar, et.al, (2017) encryption image was accomplished by utilizing an alternate chaotic mapping. The original image is split into blocks and afterward unique chaotic maps are employed for five stages of proposed encryption algorithm [9]. In the first place, the cubic map is employed to permute the pixels which contained inside the blocks. Second, Henon map has been utilized to diffuse the permuted pixels. Third, a quadratic map has been worked to permute the blocks. Fourth, a logistic map has been utilized to permute every one of the pixels whole an image. The experimental results and analysis display low PSNR value and the suggested encryption image system have exceptionally minor correlation coefficients. A good entropy value is acquired. High values of NPCR, UACI, and height sensitivity to secret keys are additionally acquired. The suggested algorithm is efficient and supplies the best security.

Zaheer Abbas Balouch, et.al, (2017)proposed an image encryption scheme is proposed which incorporates pixels shuffling in rows and columns utilizing two key vectors and after that Zeta Function to further scramble the image [10]. The proposed cipher is a hybrid model based on Rubiks Cube Principle and Zeta Function, resulting in a quick, accurate and energy efficient image encryption scheme which is one of the key requirements of low computing devices particularly mobile phones. It scrambles the original image by applying two random vectors on rows and columns and afterward Zeta Function is connected to further scramble the image. Despite the fact that this algorithm does not perform complex and extensive mathematical calculations but rather still it indicates enough robustness against all attacks regarding image encryption. All mathematical and visual tests infer that this algorithm is effective in sense of speed as well as security too.

Jialin Hou, et.al, (2016) proposed another switching fractional request chaotic system containing fractional request Chen system and the other two fractional request chaotic systems. Chaotic attractors and dynamical investigations including Lyapunov exponent, bifurcation diagram, fractal dimension, dissipation, strength and symmetry are indicated initially. From that point forward, some circuit simulations through Multisim are displayed [11]. The encryption scheme could increase randomness and improve speed of encryption. The security examinations demonstrate that the encryption scheme has a bigger key space and higher sensitivity to key parameters. Moreover, it likewise has stronger randomness and faster speed in encryption process. In spite of the fact that the proposed system has been connected to image encryption yet it is not recently constrained to it. It has idealized prospects in key agreement protocol and neural system.

Xiaolin Wu, et.al, (2016)proposed a novel image encryption algorithm by utilizing the combination of the rectangular transform and the CTM rule [12]. It encrypts the three channels of the plain image in the meantime and these channel encryptions associate with each other. Likewise, by producing the key-streams identified with both the mystery keys and the plain image, its key-sensitivity has been additionally improved. The security of the proposed scheme has been verified by security analysis and experimental evaluations, and our results demonstrate that numerous drawbacks of pure CTM-based schemes have been overcome. Experimental simulation and performance comparison with different systems demonstrate this new scheme has significantly improved the security while as yet possessing every one of the merits of the pure CTM-based schemes, which clearly drives some down to earth value in implementation.

Yinglei Song, et.al, (2016)proposed a novel image encryption algorithm based on two sets of one-dimensional logistic mappings [13]. The pixels in the original image are scrambled based on the logistic mappings in one set. The dim value of every pixel in the scrambled image is then changed by utilizing two XOR operators and the logistic mappings in the other set. Analysis and Testing results demonstrate that this image encryption algorithm can give satisfactory encryption results and the encrypted images can resist exhaustive, statistical and differential attacks.

Arul Thileeban S, (2016) proposed utilizing XOR Cipher to encrypt the binary data in images pixel by pixel as opposed to securing it with an application so it can't be exploited or cracked effortlessly [14]. The proposed model explains multiple approaches to encrypt the Image utilizing XOR Cipher and the analysis demonstrates that by utilizing the proposed model, the images are legitimately encrypted. The proposed model was tried on different images including Mona Lisa, Apollo 11 and NebulaM83 and legitimate results were yielded. The future work would incorporate building up a random function with high entropy factors so that the complexity of the password improves multiple circumstances for defense against savage driving and subsequently an

integration of a chaotic model with XOR cipher can be formed to make it more effective.

III. RESEARCH METHODOLOGY

This work is based on image encryption and basepaper technique is applied on enciphering application in which image is transmitted unsecured channels. To encrypt the image for the transmission over un secured channels image is divided into blocks. The image when divided into blocks and these divided blocks are rearranged to encrypt the image. The blocks are shuffled into fixed pattern and this pattern is decided by the key which used for encryption. The key is derived based on relationship between pixels of the image. The proposed technique performs well and it is been analyzed that proposed technique provide good results against various attacks. In future, we will work on key generation phase to drive key based on textural features of the image so that pixel loss will be minimum at the time of decryption. The proposed algorithm can be applied in the following steps:-

1. Pre-processing Phase: - In the pre-processing phase, the two image are taken as input. The first image is the original image and second image is the image which needs to encrypt. The first image is used to generate key and second image will be encrypted with the key of first image

2. Feature extracted:- In the second phase, the textual features of the first image is extracted using the GLCM algorithm. The GLCM algorithm will extract the features like energy, entropy etc. image.

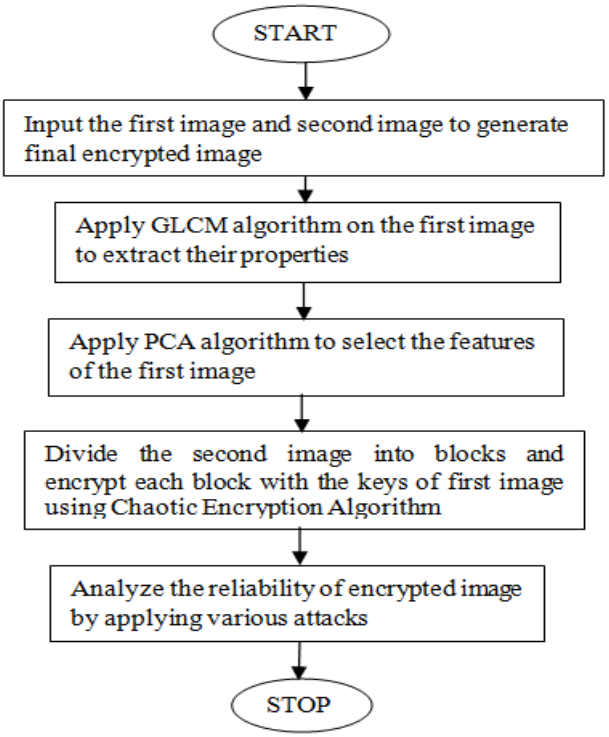

Fig.1: Proposed Methodology

IV. EXPERIMENTAL RESULTS

The proposed research is implemented in MATLAB and the results are evaluated by comparing proposed and existing approaches in terms of various performance parameters.

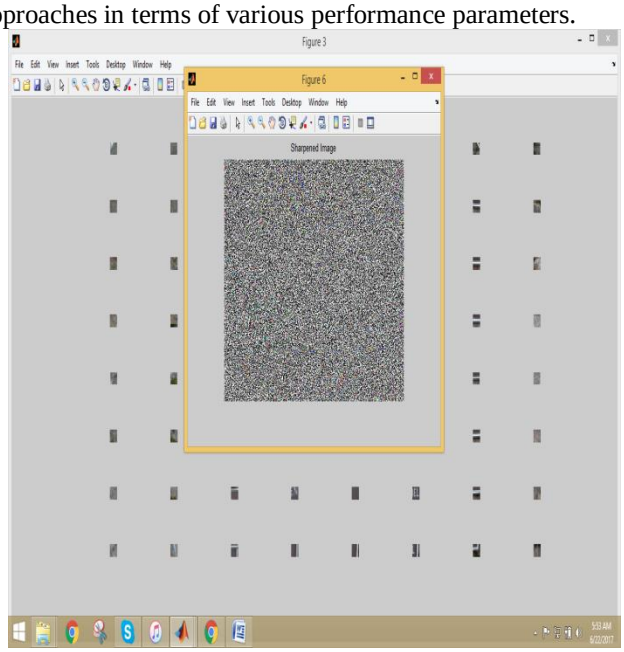

Fig.2: Apply sharpen Attack

As shown in the figure 2, the encrypted image is generated using Chaotic Encryption Algorithm. To analyze the reliability of the generated encrypted image sharpen attack is applied which change the basis properties of the encrypted image

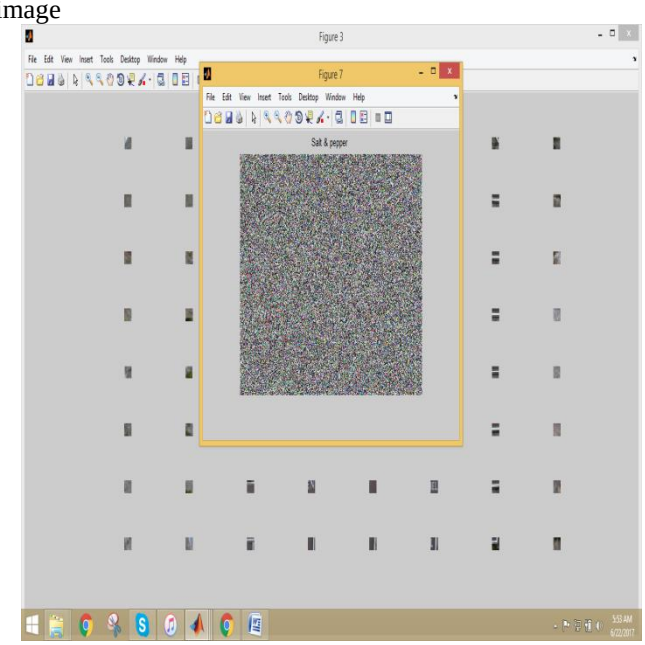

Fig.3: Apply salt & pepper Attack

As shown in the figure 3, the encrypted image is generated using Chaotic Encryption Algorithm. To analyze the reliability of the generated encrypted image salt & pepper attack is applied which change the basis properties of the encrypted image.

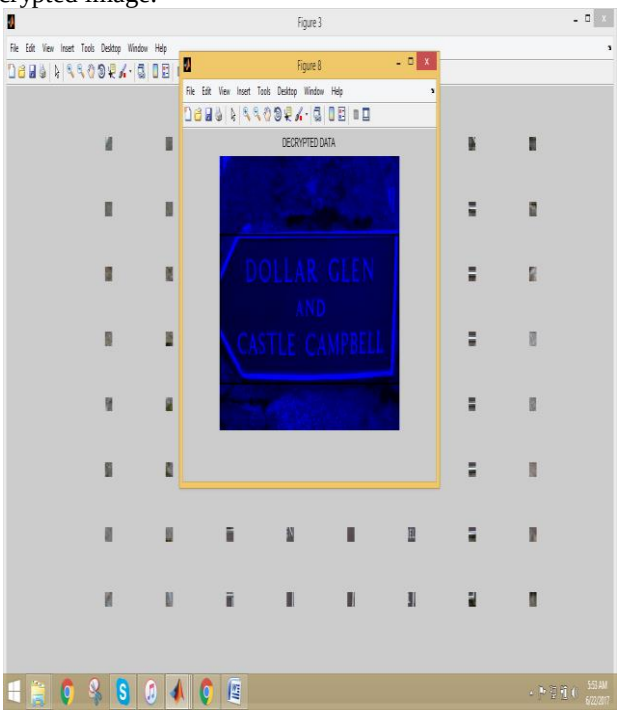

Fig.4: Decryption of image

As shown in the figure 4, the inverse of encryption algorithm is applied which will generate the decrypted image by analyzing their properties.

V. CONCLUSION

In this work, it is been concluded that image encryption is the efficient technique which provide security to the image data. In this work, novel algorithm is been proposed which is based on textual feature of the images. The two images are taken as input in which first image is used to generate key and second image is encrypted with the key of first image using block wise encryption. The textual features of the first image are analyzed using glcm algorithm and PCA algorithm is applied to select textual features of the image. The block wise encryption is applied which generate encrypted image. The reliability of the encrypted image is analyzed by applying various attacks on the image like contrast, sharpen and salt & pepper attack. The results of proposed algorithm is much efficient than existing algorithm in terms of various parameters.

VI. REFERENCES

[1]. S. Rohith, K. N. H. Bhat and A. N. Sharma, "Image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of Linear Feedback Shift Register", 2014, International Conference on Advances in Electronics, Computers and Communications (ICAECC)

[2]. S. V. Sathyanarayana, M. A. Kumar and K. N. Hari Bhat, "Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points", 2011, International Journal of Network Security, vol.12, no.2, pp.166–179

[3]. S. Sowmya and S. V. Sathyanarayana, "Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points over GF(p)", 2014, International Conference on Contemporary Computing and Informatics (IC3I)

[4]. S. Das, S. N. Mandal and N. Ghoshal, "Multiple-Image Encryption Using Genetic Algorithm", 2015, Advances in Intelligent Systems and Computing, vol. 343, pp. 145-153

[5]. L. Abraham and N. Daniel,"Secure Image Encryption Algorithms: A Review", 2013, International Journal of Scientific & Technology Research Vol. 2, no. 4, pp. 186-189

[6]. Y. Wu, J. P. Noonan and S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption", 2011, Cyber Journals: Multidisciplinary Journals in Science and Technology, April Ed. pp. 31-38

[7]. Taneja, N., Raman, B., Gupta, I., "Selective image encryption in fractional wavelet domain", 2011, Int. J. Electron. Commun., 65, pp. 338–344

[8]. Seyedzadeh, S.M., Mirzakuchaki, S., "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map", 2012, Signal Process., 92, pp. 1202–1215

[9]. Mohamed A. Mokhtar, Nayra M.Sadek, Amira G. Mohamed, "Design of Image Encryption Algorithm Based on Different Chaotic Mapping", 2017, IEEE

[10]. Zaheer Abbas Balouch, Muhammad Imran Aslam, Irfan Ahmed, "Energy Efficient Image Encryption Algorithm", 2017, IEEE

[11]. Jialin Hou, Rui Xi, Ping Liu, Tianliang Liu, "The Switching Fractional Order Chaotic System and Its Application to Image Encryption", 2016, IEEE

[12]. Xiaolin Wu, Bin Zhu, Yutong Hu, Yamei Ran, "A novel colour image encryption scheme using rectangular transform-enhanced chaotic tent maps", 2016, IEEE

[13]. Yinglei Song, Jia Song, Junfeng Qu, "A Secure Image Encryption Algorithm Based on Multiple One-dimensional Chaotic Systems", 2016 2nd IEEE International Conference on Computer and Communications

[14]. Arul Thileeban S, "Encryption of images using XOR Cipher", 2016, IEEE