TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 2744 - 2751

Image Encryption and Decryption using Chaotic Bit level Pixel Permutation

TejashwiniNeela, Department of ECE, GRIET, Hyderabad, Telangana, India.(E-mail: tejashwinineela@gmail.com)
Ch. UshaKumari, Department of ECE, GRIET, Hyderabad, Telangana, India. (E-mail: ushakumari.c@gmail.com)
SwapnaRaghunath, Department of ECE, GNITS, Hyderabad, Telangana, India.
AnkithaRathi, Department of ECE, GRIET, Hyderabad, Telangana, India.

Article Info
Volume 82
Page Number: 2744 - 2751
Publication Issue:
January-February 2020

Article History
Article Received*: 14 March 2019*
Revised*: 27 May 2019*
Accepted*: 16 October 2019*
Publication*: 18 January 2020*

Abstract:
Present day communication is tending towards the digital technologies for a faster, better and enhanced way of data transfer. The digital data transfer is an efficient way to spread the information which saves the time for the information exchange. Most of the data is transferred over the internet in the pictorial form rather than theoretical form to reduce the transfer time. Images are the best available pictorial way of data interpretation. The data transmitted over the internet are prone to security issues caused by internet hackers. In order to save the data from being exposed to unauthorized users, it is advisable to transfer the data, different from its original form. The process of changing the data in one form to another with the same information is referred as encryption and retrieving the information from its encrypted form is referred as decryption. Encryption and decryption are image processing techniques that help in efficient and secured data transfer over the internet. The paper illustrates an efficient method of encrypting and decrypting images using bit-level pixel permutation and pixel correlation techniques.

Keywords:*Bitwise XOR Operation, Data Security, Decryption, Encryption, Pixel Correlation, Pixel Permutation.*

I. INTRODUCTION

In trending and advanced communication techniques, data safety and security has become the most important issue to be addressed. Moreover, the revolution in digital technology helps in speedy exchange of information between various fields, including space, defence, multimedia, machine learning, civilian and economic etc., In such cases, data security plays a major role, and this motivates researchers to take a deep view over keeping data security and transfer systems more safe and secure. Cryptography is a distribution of algorithms which helps in storing and securing the information from being forged. Its absolute purpose is to authenticate and integrate the data and maintain its confidentiality. "A Key" is a main concept of cryptography used in encrypting and decrypting data. Encryption is permuting original data to chipper data by using encryption algorithms. Decryption is to regain the encrypted data to its original form.

Image encryption and decryption techniques include extracting the pixels from an image and hiding them to secure the data shown by the image and to get back to its former state. These techniques are based on various algorithms and methods, proposed by literature. Algorithms such as Triple DES, Blowfish, which use Private Key bulk encryption. However, image encryption cannot be carried out by conventional cryptographic algorithms such as DES due to image intrinsic properties that incudes redundancy, data capacity and correlation among pixels. Some of the most commonly used algorithms include Advanced Encryption Standard (AES) algorithm, RSA algorithm, Block based transformation algorithm, Sandwich Phase Diffuser technique, KA image cryptography, random key generation using Genetic Algorithm (GA), etc., Among them, Chaotic cryptography play a vital role

January - February 2020
ISSN: 0193 - 4120 Page No. 2744 - 2751

in conjunction with other cryptographic methods in a stand-alone fashion.

The segmentation of this paper is as follows, Section III gives the information about the crypto-system that is proposed and being adopted. Section IV describes the methodology that is followed to obtain the desired results. This section gives a brief idea of image pre-processing, encryption, decryption, pixel permutation and pixel correlation techniques. Section V shows all type of experimental results that were obtained by following the proposed method of image encryption and decryption. Section VI concludes the entire theme of the paper and section VII gives references.

II. BACKGROUND

In [1,3], the comparative study and the respective results of different encryption techniques are mentioned. All techniques, except watermarking, give an efficient outcome with a decrypted image that can be verified using various parameters. Obtaining higher Mean Square Error from AES algorithm illustrates that there exists a huge contrast between the target image and encrypted image providing larger data protection where-as for watermarking, PSNR is large but MSE is less there by showing it to be less protective.

Papers [2,5] describesthe method of combined image pixel shuffles and thus changes in grey valuesto ensure security of images. This paper also proposes an encryption algorithm with three merits. In [4,8], A sturdy image encryption method is suggested which is successfully examined over grayscale images and can be advanced to RGB images. This paper illustrates a method with three stages, generation of chaotic arrays, diffusion and pixel shuffles.

In [6,10], a new method of image hiding, called triple-key method using CNN, is proposed. The method requires a session key of 80 bit long along with initial and control parameter keys. Position of bits in the session key tells about the scrambled positions of individual pixels in encryptedoutput.The bits in the session key are circulated as shown in BRIE algorithm to impart higher chaos and the encryption process that is iterated to obtain zero-correlation. Papers [7,11] proposes an image encryption method founded on pixel shuffling with the use of skew tent map and text-based pixel replacement. [13,14] The PSNR and NPCR acquired shows that the used technique gives efficient results.

In [9,12], A coherent image encryption scheme on half-pixel-level interchange between the higher 4-bit plane part and the lower 4-bit plane part is proposed. A robust diffusion process is outlined to alter the gray values of the total target image pixels.

III. PROPOSED CRYPTOSYSTEM

The paper proposes a method of encrypting any type of images and decrypting the same image by creating a logistic function of the image and also building the confusion matrix there by creating the diffusion key to encrypt and decrypt the images selected. The pixel array is generated and pixel permutation is performed. The permuted array is then bitwise XORed with the initial grayscale array to attain the absolute encrypted image.

IV. METHODOLOGY

Encryption and decryption of an image is carried out in three steps. After the required data is collected, pre-processing of the image is to be done before encrypting the image and then, the decryption of the encrypted image is to be carried out. The following figure (1) describes the methodology adopted by this paper.

January - February 2020
ISSN: 0193 - 4120 Page No. 2744 - 2751

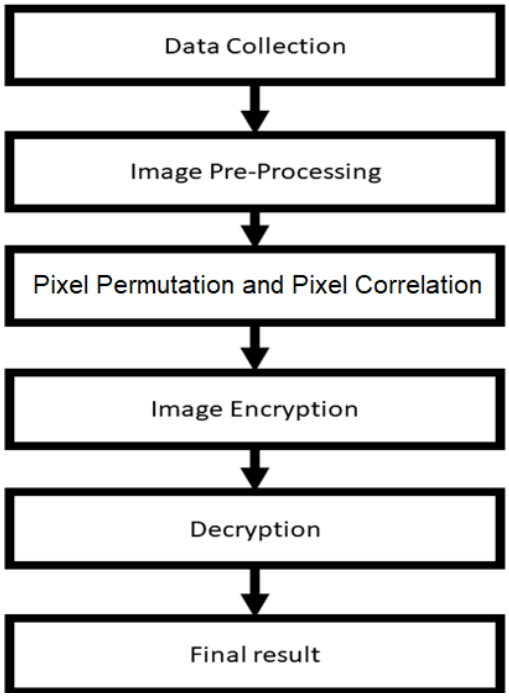

Figure (1): Methodology adopted

A. Pre-Processing:

Pre-processing of an image refers to an initial and desirable step in every image processing application and pattern recognition system to improve the performance of the operation and decrease the variations in the available consistent set of information regarding the target image being processed. This pre-processing phase of image processing is commonly considered as the lowest level of abstraction, which basically includes the collection of data regarding the target image such as feature extraction, pixelization, construction of the transition bit matrix for the image using pixels of the image, performing various transforms on the image data available, pixel brightness transformations, geometric changes, intensity variations, RGB to grayscale transformations etc. The main objective of image pre-processing is to enhance the image data by suppressing the distortions present (if any) and also improve the image features. It also helps in obtaining the raw data of the target image.

Steps:

a. Convert the target RGB image to grayscale for the further encryption process.

b. Create the logistic function of the target image by converting the target image to matrix and obtaining the length of columns and rows of the targeted image matrix and storing logistic function values into a variable by sorting them.

c. Build the confusion matrix using the image matrix. Obtain the size of each bit of image matrix and swapping it to a temporary variable by using the sorted values.

d. Generate a diffusion matrix by assuming an initial key value and preforming cosine operation using a predefined coefficient value. The absolute value of the result is considered and it is converted to binary form, circular shifted for one iteration and then converted into decimal number.

e. The obtained value is bit-XORed with the initial key to obtain the final diffusion key used for encryption and decryption processes.

f. Target image into a transition matrix by considering each pixel bit of the image to be encrypted using bit level pixel permutation.

g. Pixel correlation of the target image is done in three ways, horizontal, vertical and diagonal.

h. Image encryption is then carried out.

The step by step procedure of image pre-processing is demonstrated in figure (2).

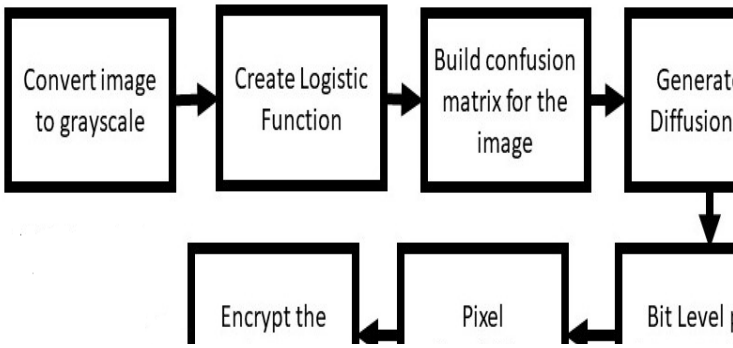

Figure (2): Image Pre-Processing process

B. Encryption:

Encryption is the way of translating any information or data into a new configuration such that only the authorized parties can have access to information. Encryption is one of the processes of image processing techniques to secure the data from

January - February 2020
ISSN: 0193 - 4120 Page No. 2744 - 2751

being misused or mis-interpreted. Encryption does not resist the intruders to steal the data, but it helps in securing the original data by exposing the encrypted or wrong data in the place of original one's by hiding the absolute data. The pure data is called "plain text" where-as the encrypted form of pure data is named as "chiper text" or "chiper data". There are two types of keys for data hiding. A symmetric key is same for both encryption and decryption processes and is known to authorized users only. An asymmetric key, also called a public key, is different for both encryption and decryption processes and it is accessible by any user who uses encrypted messages. These public keys are mostly predefined, some of such examples includes "0000", "1234", etc.,

Image encryption refers to the process of transforming the data in the form of images to the type that doesn't expose the exact data to the user who is not authorized. Image encryption techniques generally include image masking, image reshaping, image pixelization etc., Image encryption techniques using any encryption key implies the usage of various machine learning as well as optimization algorithms for an efficient key generation. Figure (3) describes the encryption process adopted.

Steps:

a. Obtain the final image matrix and perform its transpose and perform bit-XOR function with each pixel bit of the target image with bits of diffusion key.

b. Reshape the image matrix after a bit-XOR operation into a matrix form with the required number of rows and columns.

c. Store the reshaped image into another variable to display it to the user.

d. Obtain the histogram of the encrypted image to use if for comparison with the original and decrypted image histograms.

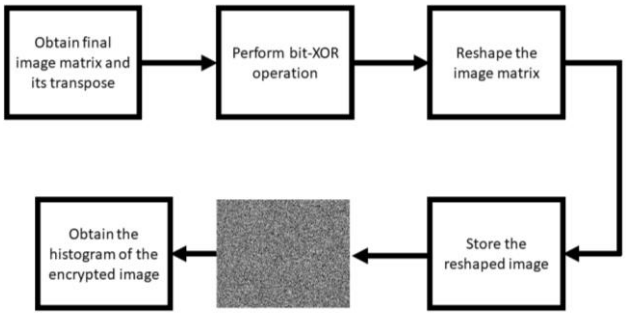

Figure (3): Encryption of the target image

C. Decryption:

Decryption is the way of decoding back the encrypted data to its former state. It can also be termed as the reversing the encryption. Decryption occurs only when the data or information encryption is performed. The key used to encrypt the data is in-turn used to decrypt it at the receiver side in symmetric key encryption technique. Whereas in asymmetric key type of encryption, decryption key will be different from the encryption one and it will be given to the receiver by the sender of the encrypted data. The more secured information exchange implies synchronized encryption and decryption techniques. Image decryption is a synchronized process, that is to be done by the end image user in coordination with the encryption done by the source of image information. The procedure is described by figure (4).

Steps:

a. Obtain the bit-XOR value of each pixel of the image.

b. Form a transition matrix with obtained bit-XOR values and obtain the size of each value and store it in a new variable.

c. Compare the size of encrypted image pixels to the bit-XOR values and store them in a variable to display.

d. Reshape the pixel values in the desired number of rows and columns to obtain a decrypted image which resembles the original encrypted image.

e. Obtain the histogram of the decrypted image.

January - February 2020
ISSN: 0193 - 4120 Page No. 2744 - 2751

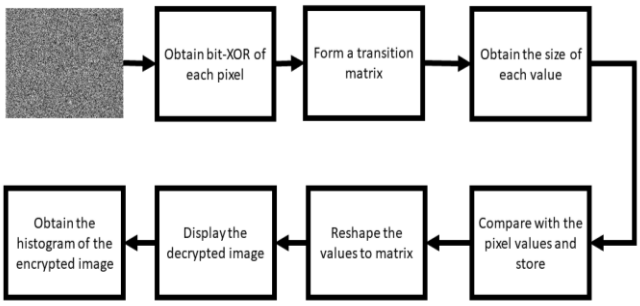

Figure (4): Decryption process of the encrypted image

D. Pixel Permutation:

Pixel permutation is the process of conversion of the 2D grayscale image to a 1D data using vertical up-down and horizontal scanning method. A pseudo random sequence is generated by permutating the pixels for variations, iterations and the sequence is arranged in increasing order, to get an array which in-turn related to the initial array to get a scrambling vector. The plane image matrix is now permuted with the scrambling vector. The text is then converted to binary form and then resized to the size of the original image. A bitwise XOR operation is performed on the resized data to generate an encrypted image which is of the same pixel length with that of the original image.

E. Mathematical Analysis:

(1) 8-bit grayscale image of size M*N pixels is converted from 2D to 1D data and is denoted as

$A= \{a_0, a_1, \ldots, a_{MN-1}\}$.

(2) The Iteration formula is given in equation (1)

$$F(a) = \begin{cases} a / p & a \in [0, p] \\ (1-a) / (1-p) & a \in (p, 1] \end{cases} \quad (1)$$

(3) Pseudo random sequence is denoted as

$R= \{r_0, r_1, \ldots, r_{MN-1}\}$.

(4) The Sorted pseudo random sequence is

$S= \{s_0, s_1, \ldots, s_{MN-1}\}$.

(5) Scrambling vector is given as $T= \{t_0, t_1, \ldots, t_{MN-1}\}$ where $s_i= r_{t_i}$, i=0, 1, …, MN-1.

(6) Plane image X is permuted with T to get

$B= \{b_0, b_1, \ldots, b_{MN-1}\}$

where $b= a_{t_i}$, i=0, 1, …, MN-1.

(7) The text converted to n-bit binary code and is represented as $P= \{p_i \mid 1 \le i \le n, p_i \in \{0,1\}\}$.

(8) Resize P to have the same dimension as B

(9) Perform bitwise XOR, store result as $Z= B \oplus K$, where $Z= \{z_{ij} \mid 1 \le i \le M, 1 \le i \le N, c \in \{0 \text{ to } 255\}$ and $z_i= b_i \oplus k_i$.

(10)The image Z indicates the encrypted image which is secure to be transferred.

F. Pixel Correlation:

Pixel correlation is relating the pixels of the image in different directions and plotting their position based on the direction observed. In the method adopted, the pixel correlation of the target image pixels and the obtained encrypted image are observed from three various directions from top to bottom, right to left and diagonal. The correlation values, thus obtained are plotted for both target image as well as encrypted image and they are compared for the clear analysis.

G. Histogram Analysis:

Histogram is a pictorial representation of a set of data. It summarizes the integrated and distributed data stored as a variable. The images used in the cryptographic processes are represented by their histogram to observe the change in the image features before and after encryption and also to show that the decrypted image resembles the target image after the image processing. The image histogram is a tonal distribution of a digital image. Image histogram can be used as a tool for thresholding which is used in image processing techniques like image-segmentation, edge-detection, etc., histogram can be plotted for any type of image and either a color image or a grey-scale image.

V. EXPREMENTAL RESULTS

An Application area: Image encryption and decryption technique can be applied in various areas where data security and integrity play an important role. The application area that we considered in this paper is security of question papers before transferring them from administration to examination.

TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 2744 - 2751

Figure (5a) shows the original image that is used as a target for the cryptographic process. Figure (5b) is the histogram of the target image. Figure (6a) is the obtained encryption output whereas figure (6b) is its histogram. Figure (7a) shows the decrypted image and its histogram is shown by figure (7b). Figure (8) shows the pixel correlation plot of the target image.

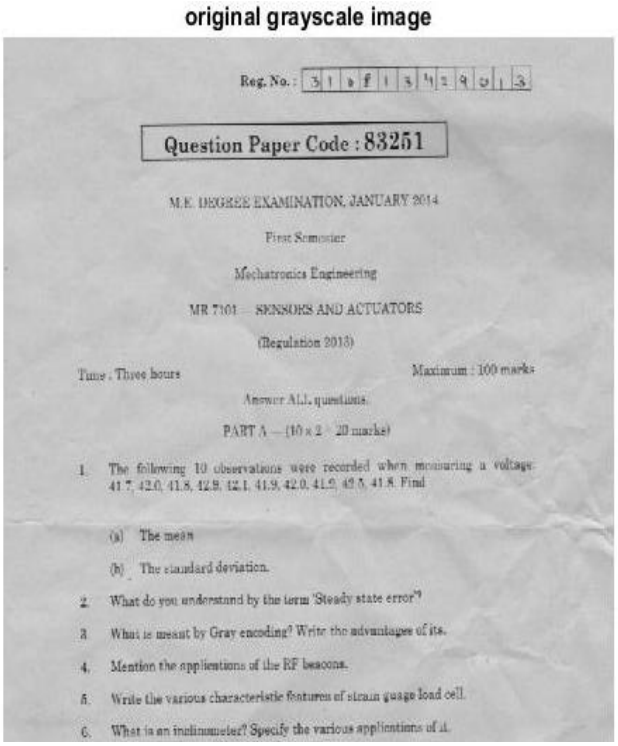

Figure (5a): Original Target Image

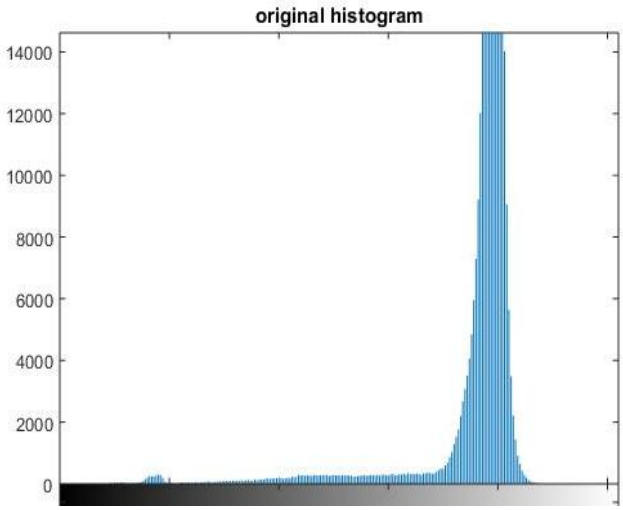

Figure (5b): Histogram of Target Image

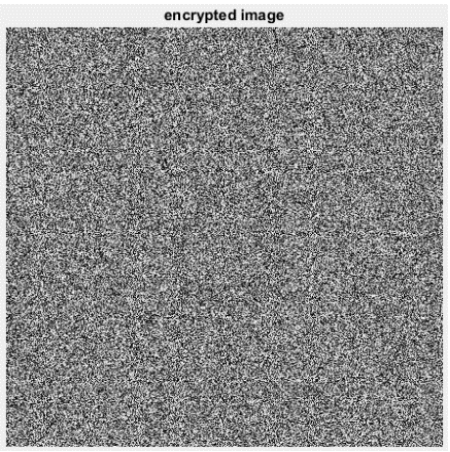

Figure (6a): Encrypted Output of Target Image

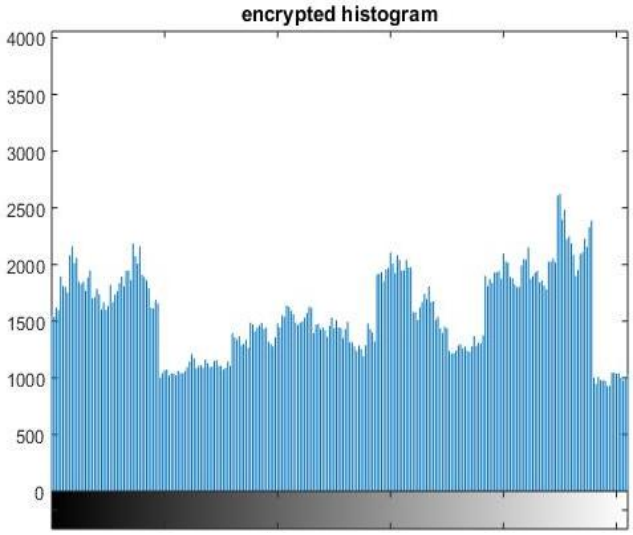

Figure (6b): Histogram of Encrypted Image

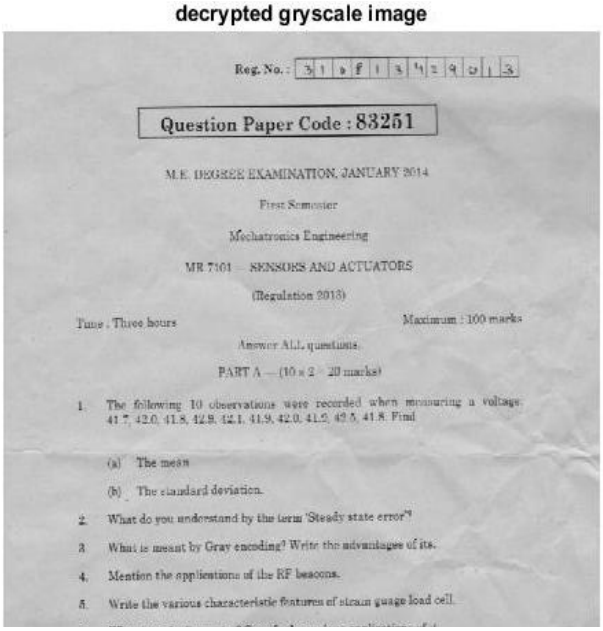

Figure (7a): Decrypted Image Output

January - February 2020
ISSN: 0193 - 4120 Page No. 2744 - 2751

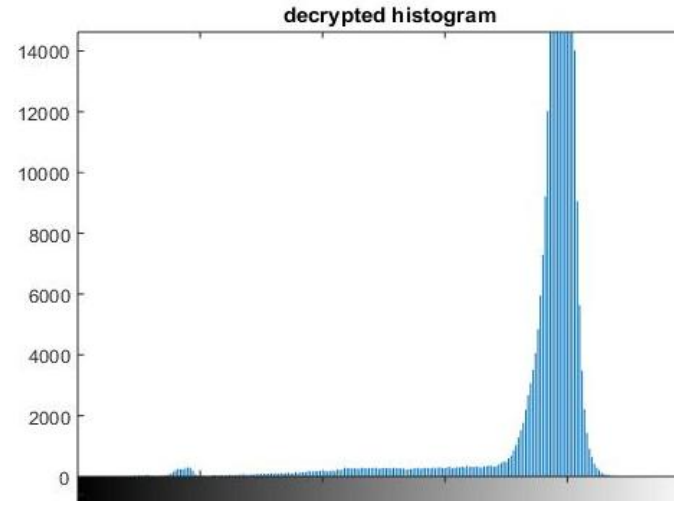

Figure (7b): Decrypted Image Histogram

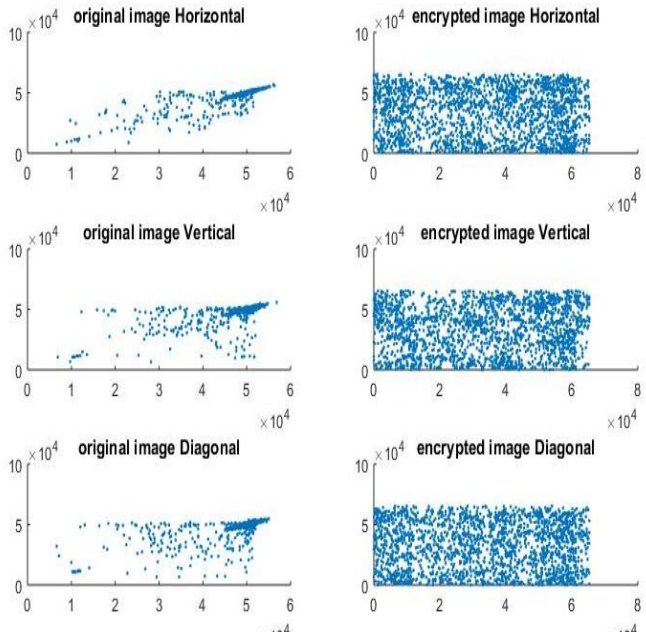

Figure (8): Pixel correlation of the target image

VI. CONCLUSION

Data security plays a vital role in present day communication where as, images acts as a major source of information. In the glance of improving the data security and integrity, this paper proposes an efficient and simple algorithm for image encryption and decryption. The algorithm is based on Chaotic Bit Level Pixel Permutation. This algorithm is used for the encryption of colour images of any format (i.e. jpeg image, png image, bit-map image, etc.,). The relation between pixels of input, encrypted and decrypted images are shown using pixel correlation graph. Histogram of the respective images show the pictorial representation of image data and shows the difference between the data of original image and the encrypted image. This algorithm is tested for many input images of different types and proven efficient. The further work on this concern includes development of a GUI based application to make the algorithm available in more simpler and eaily understandable way.

VII. REFERENCES

1. Ray, A., Potnis, A., Dwivedy, P., Soofi, S., &Bhade, U. (2017, October). Comparative study of AES, RSA, genetic, affine transform with XOR operation, and watermarking for image encryption. In 2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE) (pp. 274-278). IEEE.
2. Guan, Z. H., Huang, F., & Guan, W. (2005). Chaos-based image encryption algorithm. Physics Letters A, 346(1-3), 153-157.
3. Kumari, C. U., Rao, G. S. B., &Madhu, R. (2012). Erlang Capacity Evaluation InGsm And Cdma Cellular Systems. International Journal Of Mobile Network Communications & Telematics (Ijmnct) Vol2, (5).
4. Abdullah, H. N., & Abdullah, H. A. (2017, April). Image encryption using hybrid chaotic map. In 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT) (pp. 121-125). IEEE.
5. Kumari, C. U., Mounika, G., & Prasad, S. J. (2019, March). Identifying Obstructive, Central and Mixed Apnea Syndrome Using Discrete Wavelet Transform. In International Conference on E-Business and Telecommunications (pp. 16-22). Springer, Cham.
6. Srividya, G., &Nandakumar, P. (2011, February). A Triple-Key chaotic image encryption method. In 2011 International Conference on Communications and Signal Processing (pp. 266-270). IEEE.
7. Hardiya, P., & Gupta, R. Image Encryption Based on Pixel Permutation and Text Based Pixel Substitution.
8. Kumari, C. U., & Padma, T. (2019). Energy-Efficient Routing Protocols for Wireless Sensor

January - February 2020
ISSN: 0193 - 4120 Page No. 2744 - 2751

Networks. In Soft Computing and Signal Processing (pp. 377-384). Springer, Singapore.

9. Liu, L., Chen, Y., & Ye, R. (2017). A Plain Image Dependent Image Encryption Scheme Using Half Pixel Level Interchange Permutation Operation. Int. J. Netw. Secur. Appl, 9, 57-75.
10. Prasetyo, H. (2018, October). A New Image Encryption Technique Using Simple Chaotic Maps. In 2018 International Symposium on Electronics and Smart Devices (ISESD) (pp. 1-4). IEEE.
11. Kumari, C. U. (2018, April). Investigation: Life-Time and Stability Period in Wireless Sensor Network. In 2018 3rd International Conference for Convergence in Technology (I2CT) (pp. 1-5). IEEE.
12. Chopra, A., Ahmad, M., & Malik, M. (2015, March). An enhanced modulo-based image encryption using chaotic and fractal keys. In 2015 International Conference on Advances in Computer Engineering and Applications (pp. 501-506). IEEE.
13. Nini, B., &Melloul, C. (2011). Pixel permutation of a color image based on a projection from a rotated view. JDCTA: International Journal of Digital Content Technology and its Applications, 5(4), 302-312.
14. Kumari, C. U., & Krishna, R. M.: High performance wireless communication channel using LEACH protocols. Pak. J. Biotechnol, 13, 52-56.