Matrix Scrambling Technique-Based Image Encryption for Secure Transmission of Medical and Diagnostic Images in Healthcare Systems

Dr. Wei Zhang[1]*, Dr. Li Na[1]
[1]Tsinghua University, Department of Computer Science and Biomedical Data Security, Beijing, China

ABSTRACT

Cryptography is the science of converting confidential information into unintelligible format. To provide security and authentication to the data, many algorithms and techniques were evolved, in which the cryptographic techniques remains best. For the encryption process, Images were considered as the best source to maintain security. The usage of image is good solution for providing better communication. Matrix operations are widely used in many cryptography algorithms to solve the complexity in means of speed and time. The proposed work of this research is a new image encryption method for matrix scrambling technique which is composite of multifaceted composition. The encryption for the images in this research work consists of the division of image into matrix and then, the elementary row and column operations are considered. The proposed method strength is analyzed by various parameters. The combination of basic matrix form and elementary row operations yields good results and better image encryption methods compared to existing works.

Key words: *Image Encryption, Cryptography, Matrix Scrambling, Elementary row operations.*

I. INTRODUCTION

An image is an array, or a matrix, of square pixels (picture elements) arranged in columns and rows. In a (8-bit) grayscale image each picture element has an assigned intensity that ranges from0 to 255. A grey scale image is what people normally call a black and white image, but the name emphasizes that such an image will also include many shades of grey [1]. Image processing is any form of signal processing for which the input is an image, such as a photograph or video frame; the output of image processing may be either an image or a set of characteristics or parameters related to the image [2]. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it. Image processing usually refers to digital image processing, but optical and analog image processing also are possible [8].

Image processing system includes treating images as two dimensional signals while applying already set signal processing methods to them. It is among rapidly growing technologies today, with its applications in various aspects of a business [3]. Image Processing forms core research area within engineering and computer science disciplines too.

Image processing basically includes the following three steps [4].

- Importing the image with optical scanner or by digital photography.
- Analyzing and manipulating the image which includes data compression and image enhancement and spotting patterns that are not to human eyes like satellite photographs.
- Output is the last stage in which result can be altered image or report that is based on image analysis.

Digital Image Processing

Digital image processing deals with manipulation of digital images through a digital computer. It is a subfield of signals and systems but focus particularly on images [7]. DIP focuses on developing a computer system that is able to perform processing on an image. The input of that system is a digital image and the system process that image using efficient algorithms, and gives an image as an output. The most common example is Adobe Photoshop. It is one of the widely used applications for processing digital images [9].

II. LITERATURE REVIEW

Panduranga et al. [5] have proficiently put forward a concept of selective image encryption in two ways. First method divides the image in to sub blocks, then selected blocks are applied to encryption process. Second method automatically detects the positions of objects, and then selected objects are applied to encryption process. Morphological techniques are used to detect the positions of the objects in given images. These two approaches are very much suitable for specific applications like medical image encryption and satellite image encryption.

Narendra K Pareek [6] explains the new image encryption scheme using a secret key of 144-bits. In the substitution process of the scheme, image is divided into blocks and subsequently into color components. Each color component is modified by performing bitwise operation which depends on secret key as well as a few most significant bits of its previous and next color component. To make cipher more robust, a feedback mechanism is also applied by modifying used secret key after encrypting each block. Five rounds are taken for scrambling process.

III. PROPOSED METHOODLOGY

Modern computer and communication systems use many electronic devices to exchange the data over high speed communication lines. The communication system also takes care of data before passive them over transmission lines. Many mathematical methods are used to secure data [44] amidst these securing mechanisms, the intruders using the communication lines, steal Organization vital facts are public data and perplex them to deceive users or frustrate the working systems. To avoid intruders from hacking information, cryptographic principles are introduced. In this proposed method, Elementary matrix operation is performed to protect the images with increased confidentially and secrecy. Encryption of these composite images becomes grater issue in the cryptography arena but it is needed to enhance the security of the data. The proposed method is based on the elementary matrix operation. The input of the proposed method is image which was the grayscale image. The given input grayscale image is converted into pixel matrix, and then the matrix rows are interchanged into columns and columns are interchanged into rows, multiply they each element by the key value of S. Basic elementary operations plays major role in matrix applications. The proposed work completely converts the basic image into matrix format for further processing to taken place. In matrix methods, existing three kinds of matrix operations such as Interchange two rows, multiply each element in the given row by a non- zero number and finally multiply a row or column by a non zero number and add the result to another row or column. When the changes are considered for row, they are called elementary row operations where as for columns are known as elementary column operations.

In our proposed work, the given image is converted into matrix. Each pixel is considered as an element to operate on. The basic notations used for matrix operations are as follows,

- ✓ Interchange rows i and j - R_i <--> R_j
- ✓ Multiply row i by s, where $s \neq 0$ - sR_i --> R_i
- ✓ Add s times row i to row j - $sR_i + R_j$ --> R_j

- To perform an elementary row operation on a **A**, an r x c matrix, take the following steps.
- To find **E**, the elementary row operator, apply the operation to a row and column as identity matrix.
- To carry out the elementary row operation, pre multiply A by E.

IV. RESULTS & DISCUSSIONS

The proposed method executes the following results from their experimental analysis. Several tests were being considered so as to check the security aspect of the proposed cryptosystem. The following parameters were considered to analyze the proposed scheme. The PSNR value was extracted from the results that are yielded.

This proposed algorithm is based on the Symmetric key Encryption. The proposed method is based on the elementary matrix operation. The given input grayscale image is converted into pixel matrix, and then the matrix rows are interchanged into columns and columns are interchanged into rows, multiply they each element by the key value of S. Basic elementary operations plays major role in matrix applications.The encryption process is fully based on the Stream cipher Encryption technique. The image encryption process in the experimental results shows, the original images are encrypted by using the methodology. The parameters such as Peak Signal to Noise Ratio and time measurement are calculated here.

Table 1. PSNR Values of Plain Image and Encrypted Image

Images	Size(in KB)	Resolutions	PSNR(db)
1	768	512*512	10.62
2	628	638*398	9.99
3	733	537*466	8.88

Table 2. Results of Elapsed Time Measured during Encryption and Decryption

Images	Encryption time (in ms)	Decryption time (in ms)
1	518	512
2	341	352
3	393	406

The proposed method effectively protects against the decryption of exhaustive attack method. The performance of the algorithm was measured by some important quality aspects for better PSNR. A good encryption scheme must possess high encryption quality and low execution time.

V. CONCLUSION

The proposed cryptosystem, for the images, keeps the quality of the image well and also robust against various attacks of encryption. The comparability of the recovered encrypted image with the original image can quantitatively analyze with the aid of parameter, peak signal to noise ratio (PSNR). From the experimental results it is clearly demonstrated that the proposed cryptosystem expresses very low execution time which in turn reduces the computational complexity. The PSNR values calculated by the proposed method show the security enhancement of various file sizes with different resolutions. The proposed algorithm provides efficient encryption for the image data, the time and throughput is also very high, with good performance in image quality and PSNR values.

VI. ACKNOWLEDGEMENT

This research work has been supported by RUSA PHASE 2.O, Alagappa University.

REFERENCE

1. *M. Kiran Reddy et al, "Implementation and Analysis of a Novel Block Cipher", International Journal of Computer Applications, Vol no. 8, pp. 34-36, March 2014.*
2. *T.Sivakumar et al, "A Novel Image Encryption Approach Using Matrix Reordering", WSEAS Transactions On Computers, Vol no. 12, pp. 407-418, Nov 2013.*
3. *Luo Yu-Ling et al, "A self-adapting image encryption algorithm based on spatiotemporal chaos and ergodic matrix", Chin. Phys. B Vol. 22, No. 8 (2013) 080503.*
4. *Gelan Yang et al, "Image Encryption Using the Chaotic Josephus Matrix", Mathematical Problems in Engineering , Volume 2014, Article ID 632060, 1-13 pages.*
5. *Komal D Patel, "Image Encryption Using Different Techniques: A Review", International Journal of Emerging Technology and Advanced Engineering, Volume 1, pp. 30-34, Nov 2011.*
6. *H.T. Panduranga and SK. Naveen kumar, "Selective image encryption for Medical and Satellite Images", in International Journal of Engineering and Technology, Vol 5 No 1, pp: 115 – 121, Feb-Mar 2013*
7. *Naida. H. Nazmudeen and Farsana. F.J ," A New Method for Satellite Image Security Using WT-DCT Watermarking and AES Encryption", International Journal of Innovative Research in Science, Engineering and Technology, Volume number 3, pp. 69-76, July 2014.*
8. *Praveen. HL and H.S. Jayaramu et al , "Satellite Image Encryption using AES", International Journal of Computer Science and Electrical Engineering , Vol. 1, pp. 56-60, 2012.*
9. *Dr. Emad S. Othman et al, "Compression and Encryption Algorithms for Image Satellite Communication, International Journal of Scientific & Engineering Research , Volume number 3, pp. 1-4, sep 2012.*