IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 13, Issue 2, Ver. II (Mar. - Apr. 2018), PP 65-71
www.iosrjournals.org

Image Encryption and Decryption Using Diagonal Scan Pattern and XTEA Encryption Algorithm

Krishna Raj A[1], Sharathchandra N R[2]
[1](Electronics and Communication Engineering, Sahyadri College Of Engineering And Management, India)
[2](Electronics and Communication Engineering, Sahyadri College Of Engineering And Management, India)
Corresponding Author: Krishna Raj A

Abstract : *In today's world network security is a paramount because of presence of hackers, viruses and electronic frauds. A cryptographic system is necessary to keep the data secure. Cryptography is a technique in which information is hidden in such a way that only certain users can access it. It has some algorithms, keys for security and facility for key management. There are several algorithms which will vary depending on the size, security and time required to encrypt and decrypt data. This project focuses on image encryption and decryption using SCAN patterns as well as extended tiny encryption algorithm. Here using SCAN patterns image pixels are rearranged. Then rearranged image is encrypted and decrypted using Extended Tiny Encryption algorithm.*

Keywords – *Cryptography, Decryption, Encipher, Encryption, SCAN.*

Date of Submission: 11-04-2018 Date of acceptance: 26-04-2018

I. Introduction

Network security is primary issue in any wireless systems. To keep data secure cryptographic system is necessary. Cryptography is a method of keeping information secure where certain people can only view it. There several cryptographic algorithms which are used for protecting the stored data and network transmission. In cryptography there are two types of algorithms, symmetric key based and asymmetric key based algorithms. In symmetric type algorithm same type of key is used for encryption as well as decryption process whereas in asymmetric distinct types of keys are used for encryption and decryption process. Security of symmetric crypto system is dependent on strength of algorithm and length of key. Several algorithms are present and suitable algorithm is selected based on required constraints. The selected algorithm must be secure, small in size and capability of overcoming possible network attacks on it. The TEA (Wheeler and Needham 1994) and the XTEAs (XTEAs) (Needham and Wheeler 1997; Russell 2004; Kelsey et al. 1997; Moon et al. 2002) are suitable among other algorithms for security purpose. Block cipher consists of block of n bits which will encrypt the plain text as blocks. The decryption algorithm coverts block of n cipher bits to original block of plain text. The size of block cipher differs depending on the algorithms, for example in International Data Encryption Algorithm (IDEA) plain text is splits into blocks of size 32 but it is 64 in Data Encryption Standard (DES) algorithm. The XTEA algorithm is applicable for Radio-Frequency Identification tags and sensor networks.

SCAN based algorithm is used to generate scan patterns in which pixels are rearranged. SCAN is a 2-D spatial pixel accessing methodologies which can generate and represent huge number of different scanning paths. There are six basic scan pattern transformations. The proposed image encryption system uses extended tiny encryption algorithm and diagonal scan pattern.

II. Proposed Methodology

SCAN pattern and XTEA encryption algorithm encrypt input image and produce encrypted image. The encrypted image is decrypted using same algorithms to get original image. In the proposed methodology diagonal scan pattern and XTEA encryption algorithm used together to encipher and decipher the image. Diagonal scan pattern is one of the basic scan patterns of SCAN language. The use of two algorithms together will increase system security. Figure 1 shows diagram for proposed methodology.

Input image

The input image file is selected with the help of MATLAB. The image can be of any size but it should be in the format of .jpg, .bmp etc. Color or gray scale image can be taken as input for encryption. The image is resized in to 64*64 pixels. Color to gray scale transformation process is done first, because it easy to convert gray scale image in to text file. The conversion is done using MATLAB. The converted text file is given as input to diagonal scan encryption.

Image to text conversion

First input image is resized to 64*64 pixels. First Color to gray scale transformation is done. The gray scale image has pixel value in between 0 to 256. Using MATLAB code resized gray scale picture is transformed in to text file. The text file consists of hexadecimal values between 0 to FF. This text file is given as input to diagonal scan method.

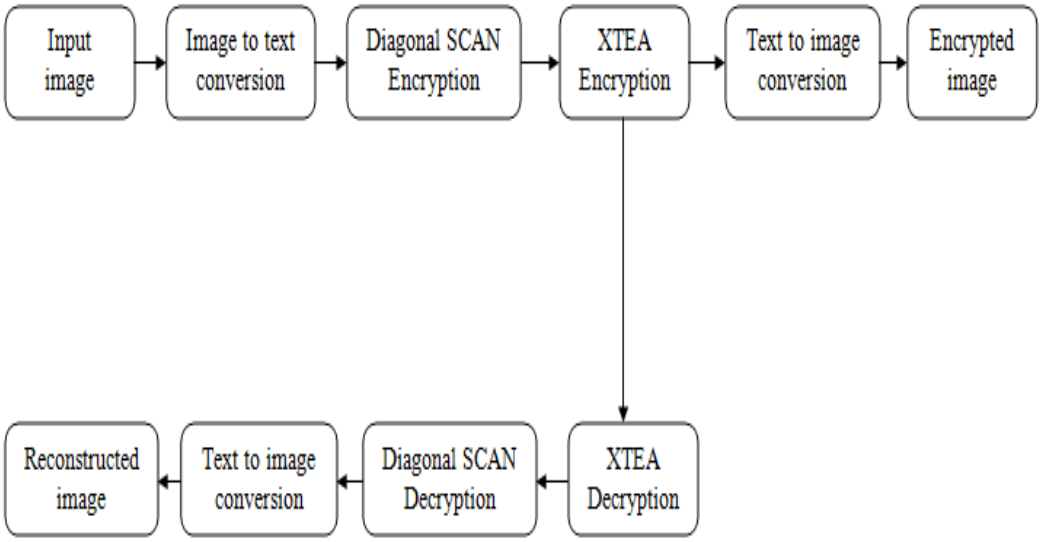

Fig. 1 Diagram for proposed system

Diagonal SCAN Encryption

SCAN is a method where pixels are rearranged. There are six basic scan patterns. In the proposed method pixels are arranged in the form of continues diagonal scan patterns. It is implemented using Verilog code. Here input image pixels are rearranged using diagonal scan pattern. The output of diagonal encryption is given as input to XTEA encryption.

XTEA Encryption

XTEA encryption technique is a 64 bit block cipher where block is divided in to left 32 and right 32 bits. The rearranged image text is given as input to XTEA encryption. The text values are encrypted using XTEA algorithm with 128 bit key. This technique is implemented using Verilog code. The encrypted text will be converted to image which is not in the recognizable form.

XTEA Decryption

The encrypted output is given as input to 64 bit block cipher. It is divided in to left 32 bits and right 32 bits. The key used in encryption is used for decryption process as well and it is of 128 bit in size. Output of decryption process is in text file form and it has text values similar to XTEA input values. The decrypted output is inputted to diagonal scan decryption to obtain original text values.

Diagonal SCAN Decryption

In diagonal scan decryption the encrypted scan values are rearranged to get original image text file. The XTEA decryption output is the input for diagonal scan decryption. The output of diagonal scan decryption is in text file form and it has text file similar to diagonal scan encryption input. Text file is converted to image using text to image conversion process.

Text to image conversion

The text values obtained from diagonal scan decryption are converted to image using text to image conversion process to reconstruct the original image. The image is displayed using MATLAB.

Reconstructed image

The output of diagonal scan decryption is converted to image file with the help of text to image conversion. Output of text to image conversion is an image that was reconstructed after completing all encryption and decryption processes.

III. Extended Tiny Encryption Algorithm (Xtea)

The XTEA algorithm is also a block cipher which encrypts or decrypts 64 bits of data blocks using 128 bits of cryptographic key. Input block is divided into two equal parts left Ln and right Rn. These blocks inputted to a Feistel network of N number rounds, where value of N is 32. In XTEA the operations performed are additions, shifts, and exclusive-or.

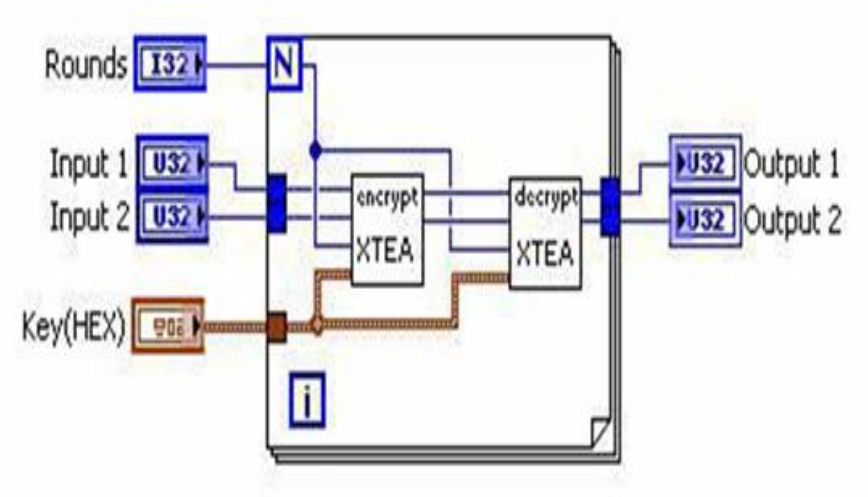

Fig. 2 Block diagram of XTEA

XTEA performs addition modulo 32 for enciphering and subtraction modulo 32 for deciphering. Here input block is divided in to variables Ln and Rn which are 32 bits in size. Logical left shift by Ln in to 4 bits is indicated by Ln<<4 and logical shift right Rn in to 5 bits is denoted by Rn>>5. Term "⊕" indicates the XOR operation which is bitwise and value of δ is 9e3779b9x which is constant.

IV. Scan Patterns

SCAN technique is a language, which is a two dimensional spatial accessing method and it can create large number of scanning routs efficiently. It is a technique which creates different scanning patterns. SCAN method consists of six basic scan patterns which are defined by a grammar. Compiling simple scan patterns a set of scan patterns transformations and a set of rules to recursively acquire intricate scan patterns. Depending on the need of specific application reduction in basic scan patterns can be done.

There are six basic scan pattern transformations. They are parallel and perpendicular reflection, uniqueness, rotation by 90, 180 and 270 degree. SCAN based algorithm is based on rearrangement of pixels. There are different ways of pixel arrangement it may be continuous diagonal D, continuous spiral S, continuous orthogonal O, and continuous raster C. In proposed system continuous diagonal scan pattern is used for pixel rearrangement. Bellow figure continues diagonal scan pattern.

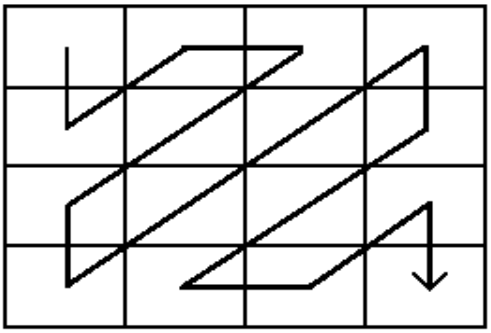

Fig. 3 Continues diagonal scan pattern

V. Results

The programming is done in Xilinx and MATLAB and both softwares are interfaced using modelsim to get results.

Input image

Input image file for encryption is selected using MATLAB. Conversion of color to gray scale is done first and then resized in to 64*64 pixels. Image resizing and color to gray scale image conversion is done using MATLAB.

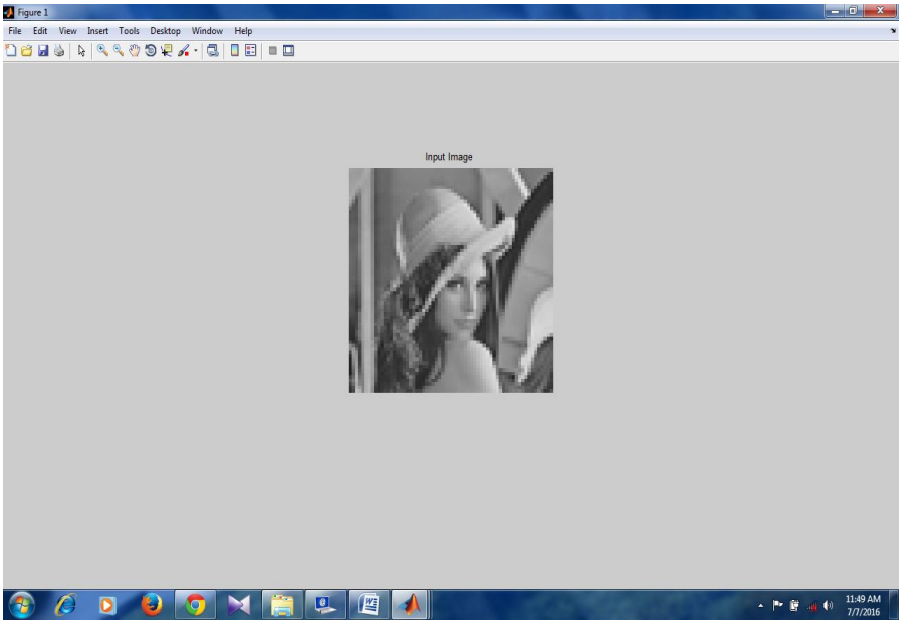

Fig. 4 Input image

Diagonal SCAN encryption output

The gray scale input image is given for diagonal scan encryption. This method will rearrange the pixel in diagonal scan pattern. The image is converted to text format using image to text conversion MATLAB code. Verilog code will convert the input image text file to rearranged image text file which is in encrypted form. The diagonal scan encrypted image difficult to recognize due to pixels rearrangement.

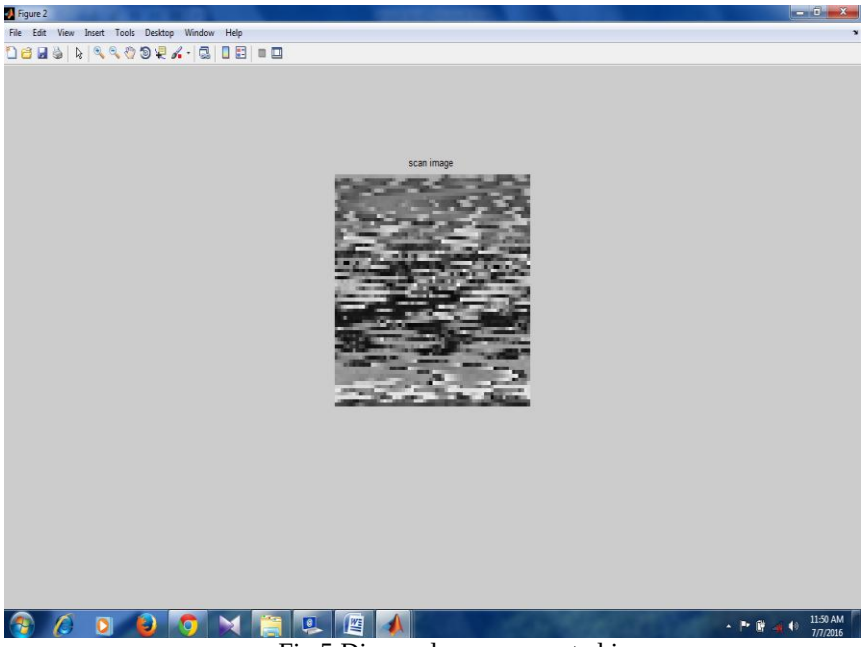

Fig.5 Diagonal scan encrypted image

XTEA encryption output

The diagonal scan encrypted image is given as input to XTEA encryption. Here image is converted to text and it is given to XTEA encryption module to get encrypted text file. The XTEA encryption module is coded with verilog and it is simulated to get encrypted text file. The encrypted text file is converted to image using text to image conversion.

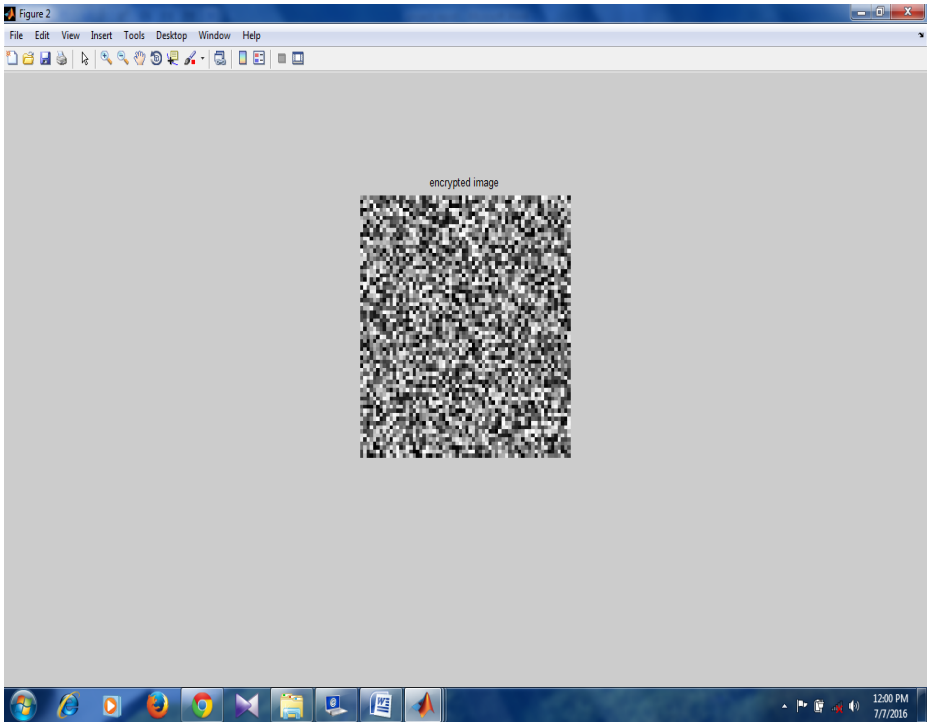

Fig. 6 XTEA encrypted image

XTEA decryption output

The enciphered image output is inputted to XTEA deciphering to get decrypted output. Encrypted image is converted to text form and given to XTEA decryption to get decrypted output.

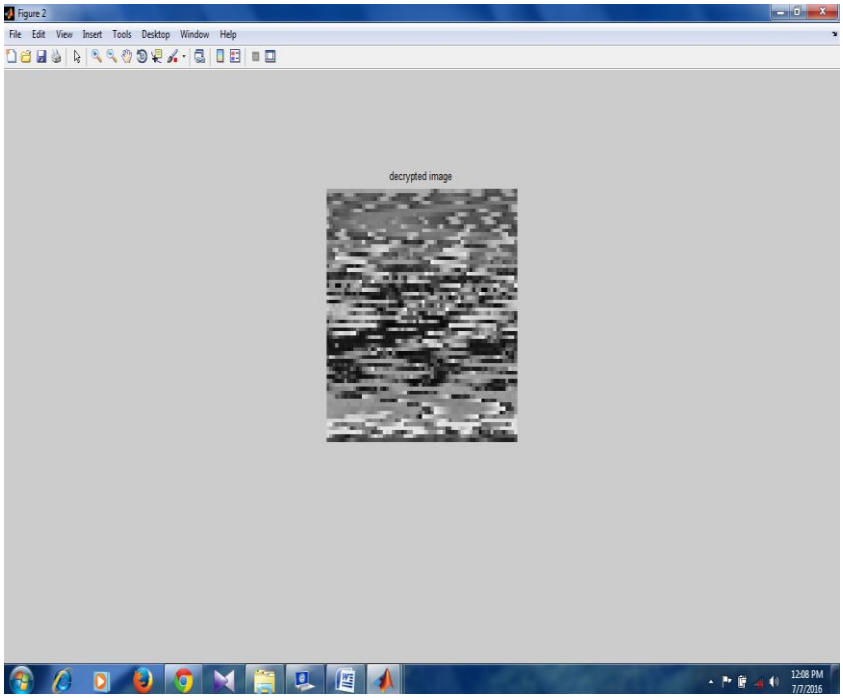

Fig. 7 XTEA decrypted image

Diagonal SCAN decryption output

The output of XTEA decryption is given as input to diagonal scan deciphering to obtain original input image. Here the diagonally arranged image pixels are rearranged to get reconstructed image.

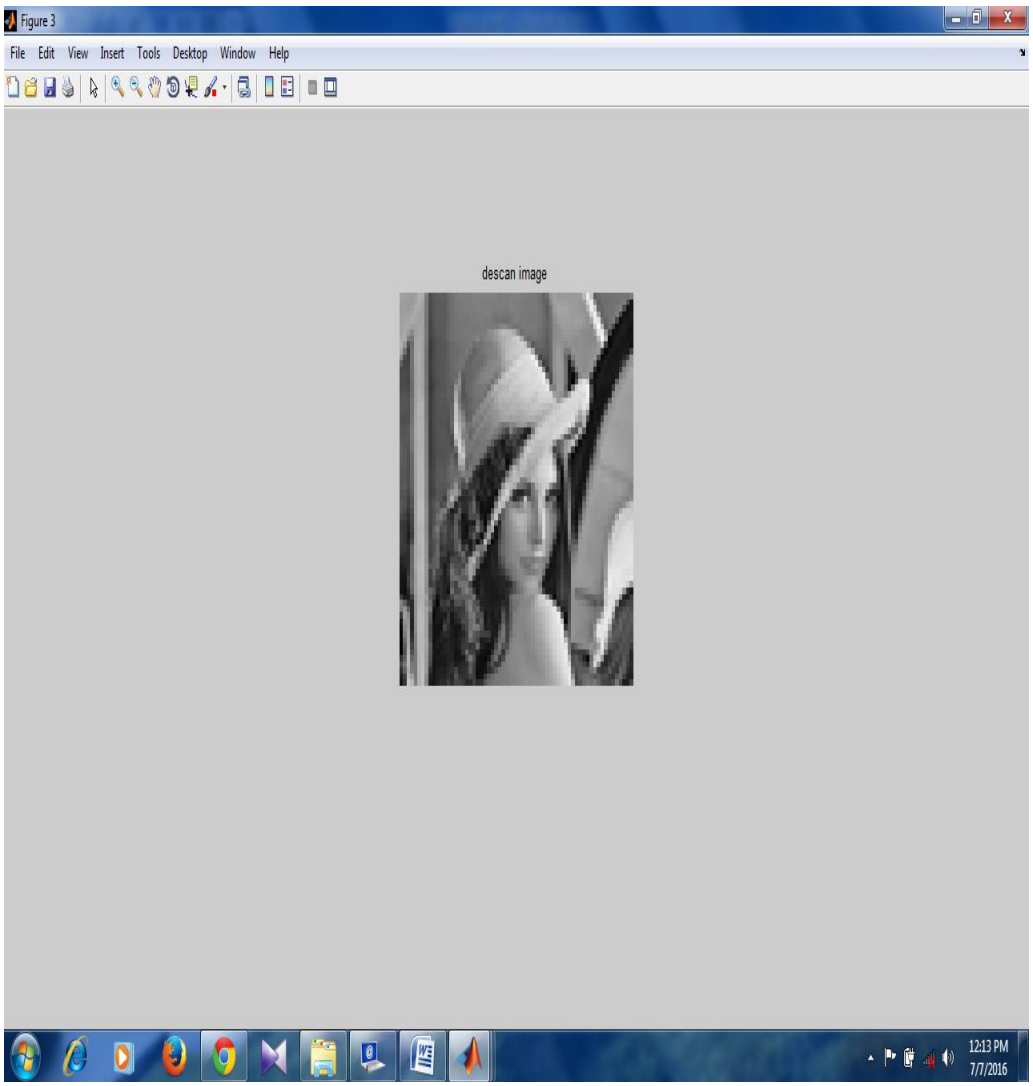

Fig. 8 Reconstructed image

VI. Conclusion

The proposed system will increase the data or image security by encrypting the data using SCAN method as well as XTEA encryption algorithm. The hacker should require key and scan pattern to get the data. Without key and scan pattern it is difficult to get the image. The security can be increased by adding more number of scan patterns. In future addition of more number of scan patterns and modification of encryption algorithms can be done to increase security. This system can be implemented in FPGA. Proposed system can be used in various wireless network systems like emails, WhatsApp, hike etc., where images are transferred. In future it can be modified by adding different algorithms that may help to increase the network security.

References

[1] SandipanBasu"International Data Encryption Algorithm (IDEA) - a typical illustration" Journal of Global Research in Computer Science Volume 2, No. 7, July 2011.

[2] ShwetaGaba, ItiAggarwal, Dr. SujataPandey "Design of efficient XTEA using verilog" International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012 .

[3] Chao-Shen Chen, and Rong-Jian Chen "Image Encryption and Decryption Using SCAN Methodology" Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06) 0-7695-2736-1/06 IEEE 2006.

[4] Saisubha v, Priyanka u, Remya k r &Reenu r "Image encryption using scan pattern" International Journal of Soft Computing and Artificial Intelligence, Volume- 1, Issue- 1.

[5] M.NatheeraBanu "FPGA Based Hardware Implementation of Encryption Algorithm" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014.
[6] KiranKumar.V.G, SudeshJeevanMascarenhas, Sanath Kumar, VivenRakesh J Pais "Design and Implementation of Tiny Encryption Algorithm" Int. Journal of Engineering Research and Applications ISSN: 2248-9622, Vol. 5, Issue 6, (Part -2) June 2015, pp.94-97.
[7] C.Kachriset.el.,"A reconfigurable logic based processor for the scan image and video encryption algorithm",IJPP,vol.31,No.6,Dec 2003,pp.489-506.
[8] BibhundendraAcharya et .el.,"Image encryption using advanced hill cipher algorithm", International Journal of recent trends in engineering,ACEEE,vol.1,o.1,May2009.
[9] Said E.El-Khamy, "A partial image encryption sheme based on the DWT and ELKNZ chaotic stream cipher", MASAUM Journal of basic and applied science,vol.1,No.3,October2009
[10] Derek Williams CPSC 6128- Network Security Columbus State University "The Tiny Encryption Algorithm (TEA)" April 26, 2008.

IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) is UGC approved Journal with Sl. No. 5016, Journal no. 49082.

Krishna Raj A "Image Encryption and Decryption Using Diagonal Scan Pattern and Xtea Encryption Algorithm." IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) 13.2 (2018): 65-71.