Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.561 – 567

RESEARCH ARTICLE

A NOVEL THRESHOLD BASED IMAGE ENCRYPTION FOR BITMAP IMAGES

K.Berlin[1], A.Padmapriya[2]

[1]M.Phil Research Scholar, [2]Faculty-Computer Science & Engineering
[1]Alagappa University, [2]Alagappa University
Karaikudi, Pin no.630003
[1] berlinjenson@gmail.com, [2] mailtopadhu@yahool.co.in

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. In this proposed method, a new image encryption method is placed. According to proposed methodology, the given image is encrypted as stream ciphers based on the threshold value computed. Two stages were being defined for proposed methodology, first one is the threshold computation, and second one is encryption. This method remains securable and quick access of data is taken place.

Keywords: Stream Cipher, Threshold, Encryption, Confidentiality, Bitmap Images

1. INTRODUCTION

This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website. Security of data, in communication spectrum becomes serious issue. To ensure the security of data, various algorithms and techniques were evolved, so as to retain the authentication of the data. Particularly the image security in transmission spectrum is considerably peak in research.

Cryptography is the art as well as the science of encryption process, which allows the data to convert into unreadable format. This, traditional data encryption algorithms is divided into two major category namely Symmetric Key algorithm and Asymmetric Key algorithm. There exists number of encryption algorithms that have been proposed to protect images. These encryption algorithms can be classified into several categories such as value transformation, pixel position permutation, and chaotic systems.[1]

Visual Cryptography is more useful to transfer the image, also protecting it against reading, alteration of its content, adding false information or deleting part of its content while transmitting through the networks. Rijndael

was chosen as the AES algorithm. It is a very strong block cipher for its simplicity, efficient structure, and its strength against linear and differential cryptanalysis [3].

The encryption of the images is categorized into two ways, block cipher encryption and the stream cipher encryption. In the block cipher mode each of the data is divided into blocks and each block is included for the encryption, whereas in the stream cipher mode each bit is encrypted.

In this paper, a new threshold based image encryption technique is proposed. It has two parts, the first part of the proposed methodology is threshold computation and the second part is encryption based on the stream cipher method.

The paper is structured as follows. Section 2 briefly discusses the background study for the proposed technique. Section 3 comprises of description about the proposed technique and the procedure for the proposed methodology. The experimental results and their evaluations also present in section 4. Section 5 gives the conclusion.

2. RELATED WORK

In the work proposed by Pavan Kumar, Goswami, Namita Tiwari, Meenu Chawla[7], increases the entropy and reduces the correlation by using block shuffling and encryption using iterative Arnold transformation. According to this plain image is first divided into blocks. All these blocks are then shuffled which work on the row wise block shuffling and column wise block shuffling then shuffled image is then encrypted using transformation.

It provides the keyless framework for image encryption. The images are scrambled using algorithm and then transformation using key. High key sensitivity is required by secure image cryptosystems, which means that the cipher image cannot be decrypted correctly.

Liu et al. [3] proposed an image encryption algorithm based on an iterative random phase encoding in gyrator transform domains. Two-dimensional chaotic mapping is used to create much random data for iterative random stage encoding.

Tao et al. [8] proposed an image encryption algorithm based on the fractional Fourier transform which can be applied to double or more image encryptions. The encrypted image is achieved by the summation of different orders of inverse discrete fractional Fourier transforms of the interpolated sub-images. The complete transform orders of the employed FRFT are used as the secret keys for the decryption of each sub-image.

In the work proposed by Nawal El-Fishawy and Osama M. Abu Zaid, [6] different Bitmap images are encrypted with RC6, MRC6, and Rijndael algorithms. The quality of the encrypted images are tested with visual inspection and evaluated with different quality of measuring algorithms. Four evaluating measuring factors are considered, in addition to visual inspection.

In the work proposed by Mohammad Ali Bani Younes and Aman Jantan,[4] an Image Encryption Using Block-Based Transformation Algorithm is proposed. A block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm.

The results showed that the correlation between image elements was significantly decreased by using [4]. The results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.

Zhi-Hong Guan et al. [9] have presented a new image encryption scheme, in which shuffling the positions and changing the grey values of image pixels are combined to confuse the relationship between the cipher image and the plain image.

Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma [2], proposes a new Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm(Hyper Image Encryption Algorithm), introduce a new permutation technique based on the combination of image permutation and a new developed encryption algorithm called "Hyper Image Encryption Algorithm (HIEA)". From the selected image binary value blocks, which will be rearranged into a permuted image using a permutation process, and then the generated image will be encrypted using the "Hyper Image Encryption Algorithm.

Narendra K Pareek.[5] proposes the image encryption scheme for color images, here the use of bitwise operation each and every color components are modified based on the secret key and also most significant bits of its previous and next color component. After encrypted each block a feedback mechanism applied to make cipher more robust.

3. PROPOSED METHODOLOGY

The following sections describe the newly proposed technique based on the threshold value and matrix transposition. The working procedure for this is as follows: The given image is converted into gray scale images. After the conversion the image is divided into 16 X 16 blocks. Division of 16 X 16 block is done only for calculating threshold, not for encryption. In which pre-process contains the conversion of colour image into gray scale images and transpose every image. Post process consists of inverse transpose of image while decryption. It is also explained in block diagram.

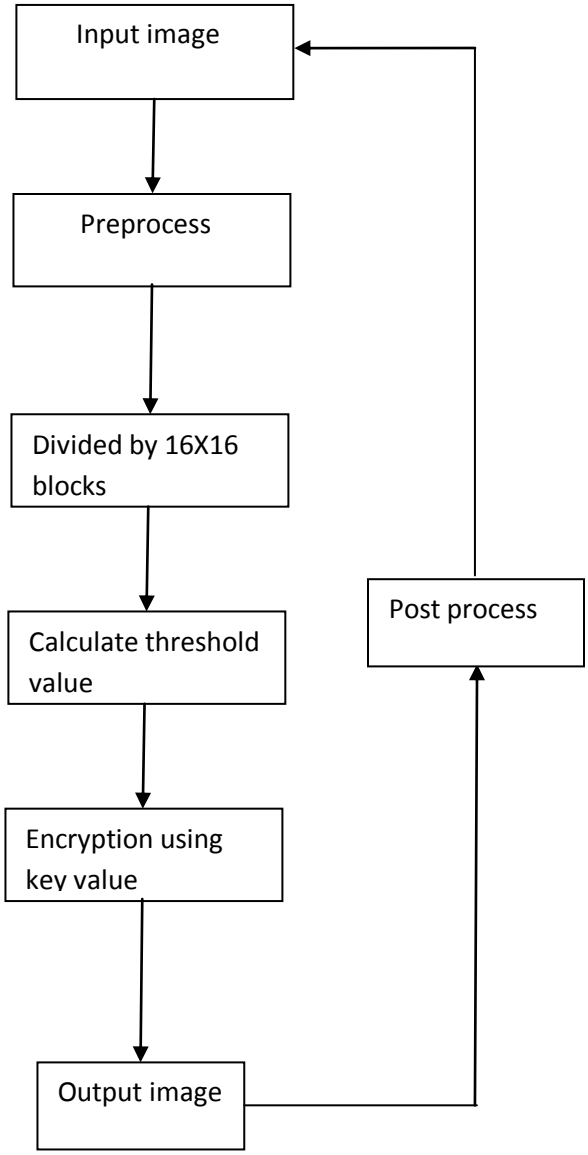

Figure 1: proposed architecture

3.1 Threshold Calculation

The divided image now consists of 16 blocks of each in row and column order. Within each block the threshold value is calculated. In which the pixels, whose value is not repeated, is called as unique value. The unique value is selected within each 16X16 blocks. The unique values from every block is summed up and divided by total count of

the unique values. The value calculated is the threshold value for that block. Similarly find the threshold for all blocks. Find the sum of threshold values of the blocks. And finally calculate the average threshold value. This is the key to be used for encryption. The stepwise procedure is as follows:

Step 1: Read the given input image
Step 2: Convert the given image into greyscale format
Step 3: The Greyscale image is transformed into matrix
Step 4: Now, the matrix is divided into 16 X 16 matrices
Step 5: The unique values are calculated for each block independently.
Step 6: Find the average of unique value within each block
Step 7: The resultant value of the above step is the threshold value for that block.
Step 8: Similarly find the threshold of all the Blocks are summed and divided by 256 to find the key for encryption.

3.2 Threshold based Encryption

The encryption of the given image is taken place here. The converted gray scale image is modified to matrix format. The divided blocks now encrypted by transpositioning its order. The stepwise procedure is as follows:

Step 1: Read the given input image.
Step 2: Transpose the input image
Step 3: Calculate the key for encryption using the threshold algorithm.
Step 4: For each pixel in image, repeat steps 5-8.
Step 5: Find the product of the pixel co-ordinates.
Step 6: Find C= product of pixel co-ordinates mod 128
Step 7: Find encryption key of the pixel C+T mod 128.
Step 8: Encryption is done by adding the encryption key to the pixel value.
Step 9: Now, the completely encrypted image is found.
Step10: Send encrypted image with key value for decryption.

3.3 Decryption procedure

The decryption process is done as follows:

Step 1: Read the encrypted image.
Step 2: For each pixel in image repeat steps 3-6.
Step 3: Find the product of the pixel co-ordinates.
Step 4: Find C= product of pixel co-ordinates mod 128.
Step 5: Find decryption key of the pixel C+T mod 128.
Step 6: Decryption is done by subtracting the decryption key of the pixel.
Step 7: Inverse transpose of the decrypted image.
Step 8: Now, the completely decrypted image(original image) is retrieve

4. EXPREMENTAL RESULTS

The following section consists of the experimentally analysed results for the above described procedure.

Fig 2(a) Input Image

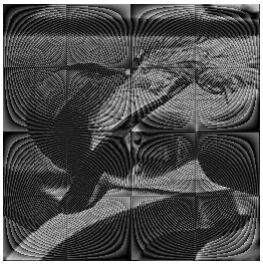

Fig2(b) encrypted Image

Fig 2 (c) Decrypted Image

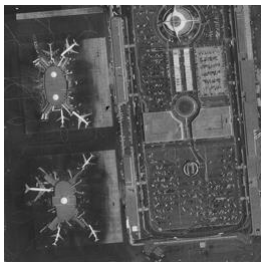

Fig .3(a) Input Image

Fig3bEncrypted Image

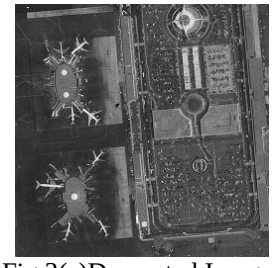

Fig.3(c)Decrypted Images

Fig .4(a)Input Image

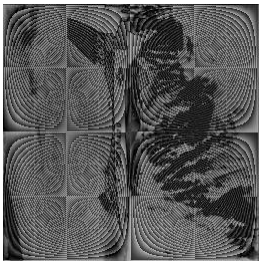

Fig 4(b)Encrypted Image

Fig 4 (c) Decrypted Image

The image encryption process in the experimental results shows, the original images are encrypted by using the threshold calculation and the matrix transposition methodology. The above figure shows the images original input image, the encrypted image and the decrypted image.

5. CONCLUSION

In this proposed work, a simple and strong method has been proposed for image security using stream cipher based image encryption techniques and matrix transposition method. From the encrypted images, it looks like the block cipher is used for encryption, but here we are using only stream cipher. The proposed threshold algorithm provided better results, in terms of metrics lowest correlation and highest encryption entropy.

References

[1] Ahmed Bashir Abugharsa1, Abd Samad Bin Hasan Basari2 and Hamida Almangush, "A Novel Image Encryptionusing an Integration Technique ofBlocks Rotationbased on the Magic cube and the AES Algorithm", pp:1 – 7.

[2] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, "Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm) ", in International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3, pp: 7 -13.

[3] Liu, Z., et al., Image encryption scheme by using iterative random phase encoding in gyrator transform domains. Optics and Lasers in Engineering, 2011. 49(4): p. 542-546.

[4] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block-Based Transformation Algorithm", in IAENG International Journal of Computer Science, No .35 , Vol 1 pp:-1-9.

[5] Narendra K Pareek, "Design And Analysis Of A Novel Digital Image Encryption Scheme", In International Journal Of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012, pp: 95 -108.

[6] Nawal El-Fishawy1 and Osama M. Abu Zaid, "Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael BlockCipher Algorithms", in International Journal of Network Security, Vol.5, No.3, PP.241–251, Nov. 2007.

[7] Pavan Kumar Goswami, Namita Tiwari, Meenu Chawla, "Block Based Image Encryption Using Iterative Arnold Transformation", in International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 8, August 2013.

[8] R. Tao, X. Y. Meng, and Y.Wang. Image encryption with multi orders of fractional fourier transforms, in Information Forensics and Security. 2010: IEEE Transactions on Image Processing .

[9] G. Zhi-Hong, H. Fangjun, and G.We n j i e ,""Chaos - based image encryption algorithm, Published by: Elsevier, 2005, pp. 153-157.

