Performance Analysis of Threshold based Image Encryption

K.Berlin
M.Phil Research Scholar
Alagappa University
Karaikudi

A.Padmapriya, Ph.D
Assistant Professor
Alagappa University
Karaikudil

ABSTRACT

Security of wireless transmission becomes considerable issue in present scenario. To overcome the issue, several algorithms were used. Among them cryptography remains as the efficient technique that converts the user provided information into unintelligible format. The cryptographic algorithms plays important role in providing security and confidentiality to the data. In this proposed work, the image encryption is done using the threshold technique. The performance factors such as the normalized cross correlation, structural content of the image, the mean square error in the image after encryption were calculated. To justify the efficiency of the proposed scheme the factors are analyzed and provided. The data format considered here is the image. By the threshold setting the entropy of the image gets increased It also reduces the execution time. Based on the results obtained the proposed algorithm yields better results.

Keywords

Secret Key encryption, threshold value, parameters, Block Cipher

1. INTRODUCTION

The concept of cryptography can kept the secret in unintelligible format for avoiding attacks from the unauthorized user access. The process of the encryption and decryption is known as cryptography. It is furthermore categorized into two topics namely (i) Symmetric Key Cryptography (ii) Asymmetric Key Cryptography. In Symmetric cryptography, the sender and receiver can use the same key for both encryption and decryption.

Asymmetric cryptography is also called as public key cryptography, where two different keys are used for encryption as well as decryption. Here, the key used by receiver is kept as secret. In this paper, a symmetric encryption method proposed for maintain the security of image that are given by the authorized users.

Images are considered as good source for data transmission. Being the data size is larger for the images, large amount of data can be easily embedded within the images. The encryption in images taken place via two ways either as block cipher or as stream cipher.

In block cipher the image pixels are divided into multiple blocks and encryption process is done for every block. Many divisions were there in block cipher mode. In the stream cipher mode, each and every a bit of the data should be encrypted resulted in extended time.

This proposed work is carried out in the images. Various performance metrics such as the Mean Square Error, PSNR value, Correlation coefficient, cross correlation etc were calculated for the output images. The rest of the paper is structured as follows. Section 2 consists of various algorithms related to the proposed algorithm. Section 3 consists of the detailed description of various parameters taken into account. Section 4 contains the experimental results obtained from the images. Section 5 shows the conclusion of the proposed work.

2. RELATED ALGORITHMS

This section consists of various encryption algorithms used for the image encryption process. In the paper proposed by

Ahmed Bashir Abugharsa[1], proposes an encryption algorithm for a new image protection scheme based on the rotation of the faces of a Magic Cube.

In the paper, the authors divide the images into number of blocks and attached to faces of magic cube. The faces are then scrambled using rotation methodology. Then the rotated image is fed to the AES algorithm which is applied to the pixels of the image to encrypt the scrambled image.

In the work proposed by Pia Singh[6] encryption and decryption of images using a secret-key block cipher called 64-bits. Blowfish designed to increase security and to improve performance. The provided algorithm will be used as a variable key size up to 448 bits. It employs Feistel network which iterates simple function 16 times. The blowfish algorithm is safe against unauthorized attack and runs faster than the popular existing algorithms.

Debasis Das and Abhishek Ray[3], in their work proposes, the Cellular Automata (CA) in cryptography for a class of Block Ciphers through a new block encryption algorithm based on Reversible Programmable Cellular Automata Theory. The proposed algorithm by the author belongs to the class of symmetric key systems.

Narendra K Pareek[5], 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. Three rounds are taken to complete substitution process. 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.

Mrs.Dhanashri M.Torgalkar ,Prof.Mr.Nitin B. Sambre[4] extends their views on Key Secured Block Based Transformation For Image Encryption, in which different keys generated for different types of image. If input image data gets converted automatically key will also get conversion. Here key is used for two purposes, one for to build transformation table and second to encrypt image data. Block Transformed image is then passed for encryption process. At the receiver side these blocks are retransformed in to their original position and performed a decryption process which gives the original image.

3. PROPOSED METHODOLOGY

The following sections describe the newly proposed methodology 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.

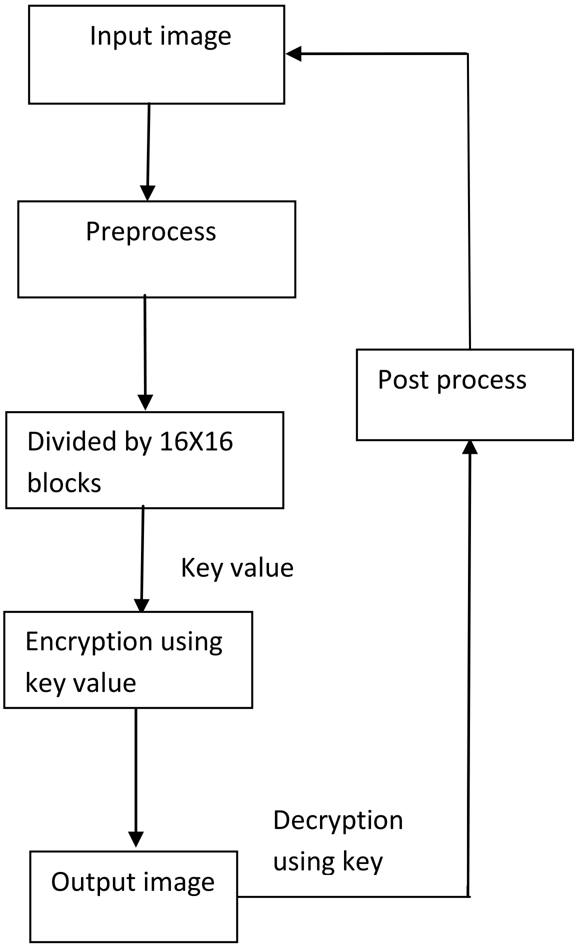

Fig1.Proposed Architecture

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[2].Paper 2 is explained here.

The stepwise procedure for threshold calculation 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.

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 for Encryption 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.

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. PERFORMANCE METRICS

In the proposed methodology, several kinds of parameters were calculated for every image, such as Mean Square Error, Peak Signal to Noise Ratio. There are more than 25 images are tested using these parameters. The detailed description about the parameters that are used by the proposed threshold algorithm is presented here.

4.1 Mean Square Error

The Mean Square Error (MSE) or Signal to Noise Ratio (SNR) is frequently used measure between the original image and encrypted image. The main goal of the MSE is to compare two images based on these similarities, in which the first image is considered as original image and another one is encrypted image. Depends upon the similarities of those images the MSE is calculated using the below formula.

$$\text{MSE}(X,Y) = 1/N \sum_{I=1}^{N}.(Xi\ - Yi\ )^2$$

4.2 Peak Signal to Noise Ratio

Peak Signal to Noise Ratio (PSNR) is used to point out the various differences between the original image and encrypted image. The main advantage of using this measure is to find out the noise level on the encrypted image. The important fact of PSNR is to shift an image but it can cause a numerical misrepresentation, and does not provide the visual distortion. The cumulative squared error is calculated between original image and encrypted image is done by MSE. The PSNR values of the given image is intended by the following equation,

$$\text{PSNR}= 10 \log_{10}(\ R2/\text{MSE})$$

4.3 Normalized Cross Correlation

The similarities between two different images can also be quantified with help of correlation function. The Normalized Correlation function measure the close relationship between two images, it may be original image and color image. All the correlation based measures is considered as 1, as the difference between two images are considered as zero. In each image the similarity measurement is done based on the linear brightness and contrast variations of using cross correlation. In which normalized correlation of the image is calculated by the given equation,

$$C.C\ E(x) = \frac{1}{N}\sum_{i=0}^{N} Xi$$

$$C.C = \frac{\sum_{i=0}^{n}(Xi - E(x))\ (Yi - E(y))}{\sqrt{\sum_{i=0}^{n}(Xi - E(x))}\ \sqrt{\sum_{i=0}^{n}(Yi - E(y))}}$$

The closeness between two digital images is this measure. The similarity between two images like original color space in the image other one converted color space image, hence in this sense they are complementary to the difference based measures.

All the correlation based measures tend to 1, as the differencbetween two images tend to zero

4.4 Average Difference

It is the measure of a lower value of cleaner image as more noise is reduced and it is computed.

4.5 Maximum Difference

It is preferred as a very simple measure as a reference for measuring conversion image quality in different color spaces. Large value of MD means that the image is of poor quality.

4.6 Normalized Absolute Error

Normalized absolute error computed is a measure of how far is the conversion image from the original image with the value of zero being the perfect fit. Large value of NAE indicates poor quality of the image.

4.7 Structural Content

This measure effectively compares the total weight of an original signal to that of a coded or given. It is therefore a global metric. This measure is also called as structural content, and if it is spread at 1, then the converted image is of better quality and large value of SC means that the image is poor quality.

5. EXPERIMENTAL RESULTS

This section brings out the results obtained from the proposed algorithm. The input image and the encrypted image are given the figures 4.1, 4.2. The performance metrics for the tested images are also given. The table shows the average value of each metrics for every image calculated.

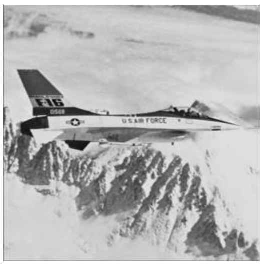

Fig 4.1 Input Images

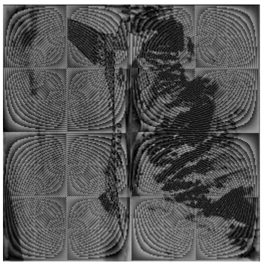

Fig 4.2 Encrypted Image

In the table 1 present the parameters calculation of the images that are applied in the proposed methodology.

The table 2 describes the average value for each metrics for about 25 test images, and their encrypted image. It consists of the factors structural content, Mean Square Error, Peak signal to noise ratio, normalized cross correlation, maximum difference, average difference and absolute error.

Table 1Calculation of parameters

Image	Mean Square Error	PSNR
Lenna	7.8679	9.1722
Jet	1.3487	6.8315
Gardan	8.0396	9.0785

Table 2 Avg calculation parameter

Parameters	Original image	Encrypted image
Mean Square Error	11.6992	4.5721
PSNR	66.7295	8.2688
Cross Correlation	1.0009	0.4810
Average Difference	-0.0911	60.0180
Structural Content	0.9975	2.5778

Maximum Difference	33.75	234
Normalized Absolute Error	0.0098	0.6187

6. CONCLUSION

In the proposed work, the images are encrypted using the threshold value formulated and their performance metrics were calculated. Based on the results obtained compared with the existing algorithms the new methods yields better results in mean square error, absolute error, and difference between the original to encrypted images. It is also found that the proposed scheme encrypts the image within minimum time and thus reduces the processing time complexity.

7. REFERENCES

[1] Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari and Hamida Almangush, “ A Novel Image Encryptionusing an Integration Technique ofBlocks Rotationbased on the Magic cube and the AES Algorithm”, pp: 1-7.

[7]

[2] K.Berlin Dr.A.Padmapriya , “A Novel Threshold based Image Encryption for Bitmap Images”, in International Journal of Computer Science and Mobile Computing(IJCSMC), Vol.3, Issue.7, July 2014, pp:561-567.

[3] Debasis Das and Abhishek Ray, “ A Parallel Encryption Algorithm for Block Ciphers Based on Reversible Programmable Cellular Automata”, in Journal Of Computer Science And Engineering, Volume 1, Issue 1, May 2010, PP: 82 – 90.

[4] Mrs.Dhanashri M.Torgalkar , Prof.Mr.Nitin B. Sambre, “ Key Secured Block Based Transformation For Image Encryption”, in International Journal of Computer Technology & Applications,Vol 5, No:2,pp:512-517.

[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] Pia Singh ,Prof. Karamjeet Singh, “ Image Encryption And Decryption Using Blowfish Algorithm In Matlab”, International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.