International Journal of Emerging Engineering Research and Technology
Volume 3, Issue 4, April 2015, PP 52-59
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

Advanced Image Encryption using Combination of Permutation Technique

Praveen Kumar Sheri, Prof. A. Thyagaraja Murthy

Department of Electronics &Communication Engineering, Sri Jayachamarajendra College of Engineering, Mysore

ABSTRACT

Encryption is used to securely transmit data in open networks. Each type of data has its own features, therefore different techniques should be used to protect confidential image data from unauthorized access. Most of the available encryption algorithms are mainly used for textual data and may not be suitable for multimedia data such as images. In this research, proposed technique is used for image security using combination of permutation technique and SCAN patterns and a well known encryption and decryption algorithm called Blowfish. The experimental results have shown that the combination of permutation technique resulted in a lower correlation, a higher entropy value, and a more uniform histogram, compared to using the Blowfish algorithm alone; resulting in an enhancement to the security level of the encrypted images. The results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.

Keywords: Image Correlation, Image encryption, Image entropy, Image Histogram, Permutation.

INTRODUCTION

The rapid growth of computer networks allowed large files, such as digital images, to be easily transmitted over the internet. Data encryption is widely used to ensure security however, most of the available encryption algorithms are used for text data. Due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data. In most of the natural images, the values of the neighboring pixels are strongly correlated. This means that the value of any given pixel can be reasonably predicted from the values of its neighbors. In order to dissipate the high correlation among pixels and increase the entropy value, we propose two techniques one is permutation process based on the combination of the image permutation second one is permutation technique and SCAN patterns and a well known encryption algorithm called Blowfish. The permutation process is applied to original image (64 pixel x 64 pixel) that are then shuffled their positions within the image on the basis of pixel shuffling. In second technique we taken original image (64 pixel x 64 pixel) plus carrier image then permutation at last scan pattern. By using the correlation and entropy as a measure of security, the permutation process and permutation technique and SCAN patterns will be expected to result in a lower correlation and a higher entropy value when compared to using the Blowfish algorithm alone, and thus improving the security level of the encrypted images. A similar or different encryption variable-length secret key is needed in the permutation and encryption processes. The secret key must be known to the sender and the receiver.

The rest of this paper is organized as follows. Section 2 gives a background about the current image encryption schemes. In Section 3, the description of the proposed permutation algorithm is presented. Section 4 presents overview of SCAN pattern, section 5 presents the experimental results and discussion. Finally, section 6 concludes the paper.

BACKGROUND

Cryptography is the science of using mathematics to encrypt and decrypt data, and thus it provides a way to store sensitive information or transmit it across insecure networks such as the internet, so that it cannot be read by anyone except the intended recipient. According to while cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure

***Address for correspondence:**

praveenksheri@gmail.com

communication. In general, conventional textual cryptography algorithms such as DES, Triple-DES, AES and RSA cannot be used to encrypt images directly. Images are different from texts in many aspects such as high correlation among pixels and high redundancy. Thus, a variety of new image encryption schemes have been proposed. According to image encryption techniques try to convert an image to another one that is hard to understand. On the other side, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types. The decrypted text must be equal to the original text, but this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable.

Most of the algorithms specifically designed to encrypt digital images are proposed in the mid-1990s. There are two major groups of image encryption algorithms: (a) nonchaos selective methods and (b) Chaos-based selective or non-selective methods. Most of these algorithms are designed for a specific image format compressed or uncompressed, and some of them are even format compliant. There are methods that offer light encryption (degradation), while others offer strong form of encryption. Some of the algorithms are scalable and have different modes ranging from degradation to strong encryption. Shujun Li *et al* have pointed out that all permutation only image ciphers were insecure against known/chosen plaintext attacks. In conclusion, they suggested that secret permutations have to be combined with other encryption techniques to design highly secured images. Mitra A *et al*. have proposed a random combinational image encryption approach with bit, pixel and block permutations.

Zhi-Hong Guan *et al*. 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. Maniccam S.S. and Bourbakis N G. proposed image and video encryption using SCAN patterns. The image encryption is performed by SCAN based permutation of pixels and a carrier image which together form an iterated product cipher. Maniccam S.S., Nikolaos G. and Bourbakis. have presented a new methodology, which performs both lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology.

PROPOSED TECHNIQUES

The permutation technique works as follows: The plain image can be decomposed into blocks; each one contains a specific number of pixels (64 pixels × 64 pixels blocks). Increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy. The blocks are transformed into new locations. The generated image is then fed to the Blowfish encryption algorithm. In this case, the permutation process refers to the operation of dividing and replacing an arrangement of the original image, and thus the generated one can be viewed as an arrangement of blocks. The intelligible information present in an image is due to the correlation among the image elements in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the image elements using certain permutation techniques. As a result, the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbors. Furthermore, this process of dividing and shuffling the positions of image blocks will confuse the relationship between the original image and the generated one.

The permutation technique and SCAN patterns technique works as follows: the original image and the carrier image both are added then the permutation technique is applied to that image .After that the c scan pattern is applied to that permuted image. The correlation and entropy value of c scan permuted are calculated which provide high entropy and low correlation.

Description of the Transformation Algorithm

The transformation technique works as follows: the *original* image is divided into a random number of blocks that are then shuffled within the image. The generated (or transformed) image is then fed to the Blowfish encryption algorithm. The main idea is that an image can be viewed as an arrangement of blocks. The intelligible information present in an image is due to the correlation among the image elements in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the image elements using certain transformation techniques. The secret key of this approach is used to determine the seed. The seed plays a main role in building the transformation table, which is then used to generate the transformed image with different random number of block sizes. The transformation process refers to the operation of dividing and replacing an arrangement of the original image. The image can be decomposed into blocks; each one contains a specific number of pixels. The blocks are transformed into new locations. For better transformation the block size should be small, because fewer pixels keep their neighbors. In this case, the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbors. At the receiver side, the original image can be obtained by the inverse transformation of the blocks. A general block diagram of the transformation method is shown in Fig. 1.

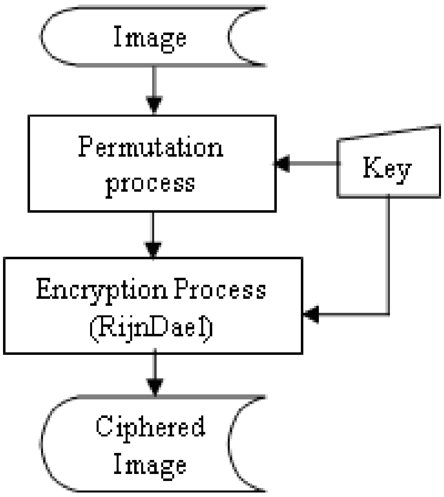

Fig1. General Block Diagram of the Permutation Technique

ALGORITHM CREATE_TRANSFORMATION_TABLE

```
1: Load Image
2: Input key
3: Get Image Width and Image Height
4:
4.1: Lower Horizontal No Blocks = Int(Image Width /10)
4.2: Lower Vertical No Blocks = Int(Image Height /10)
5: Randomize ()
6:
6.1: Horizontal No Blocks = Random Num between
(Lower Horizontal No Blocks and Image Width)
6.2: Vertical No Blocks = Random Num between
(Lower Vertical No Blocks and Image Height)
7: No Blocks = Horizontal No Blocks * Vertical No Blocks
8: Seed = | Hash value (Key) |
9: HashValue1 = |Hash value (first half of the Key)|
HashValue2 = |Hash value (second half of the Key)|
10: Randomize using seed
11: If HashValue1 > HashValue2 Then
SEEDALTERNATE = 1
Else
SEEDALTERNATE = 2
```

```
End If
12: I = 0
Number-of-seed-changes (N) = 1
13: While I < No Blocks
R = Random Num between (zero and No Blocks -1)
If R is not selected Then
Assign location R to the block I
I +=1
Else
If SEEDALTERNATE = 1 Then
seed = seed + (HashValue1 Mod I) +1
SEEDALTERNATE = 2
Else
seed = seed + (HashValue2 Mod I) + 1
SEEDALTERNATE = 1
Randomize (seed)
End If
Else
Number-of-seed-changes += 1
If Number-of-seed-changes > 500,000 then
For K = 0 to No Blocks -1
If K not selected then
Assign location K to Block I
I=I+1
End if
Next K
End if
End if
End While
END CREATE_TRANSFORMATION_TABLE
```

Input: plain Image (BMP image file) and permutation

Table Output: permuted Image.

Description of the Combination Technique

The block-based transformation algorithm is based on the combination of image transformation followed by encryption The transformation algorithm and the Blowfish algorithm use the original image to produce three output images; (a) a ciphered image using Blowfish, (b) a transformed image using a transformation process and (c) a transformed image encrypted using proposed technique.

The correlation and entropy of the three images are computed and compared with each other. This technique aims at enhancing the security level of the encrypted images by reducing the correlation among image elements and increasing its entropy value. Image measurements (correlation and entropy) will be carried out on the original image and the encrypted images with and without transformation algorithm the results are then analyzed. The overview model of the proposed technique is shown in Fig.2.

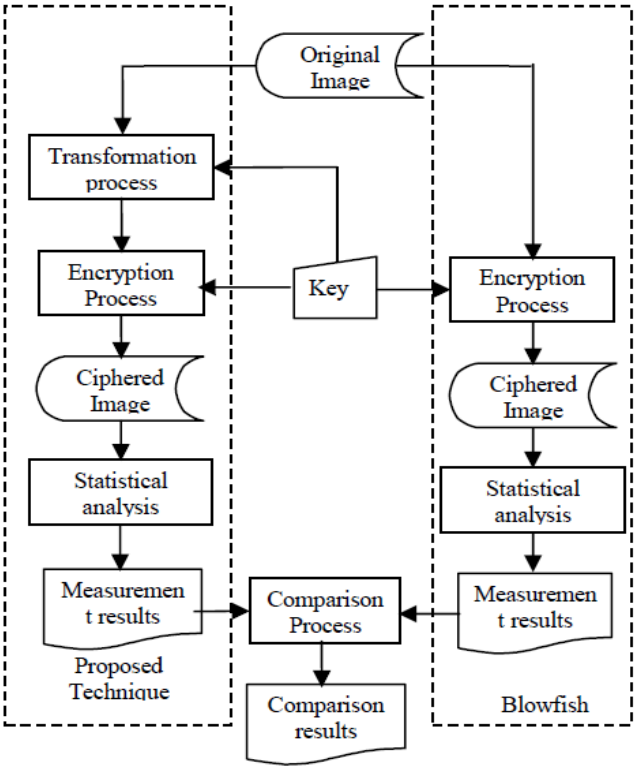

Fig2. *An Overview Diagram of the Proposed Technique*

BRIEF OVERVIEW OF SCAN PATTERNS

A scanning of a two dimensional array is an order in which each element of the array is accessed exactly once. The SCAN is a formal language-based two dimensional spatial accessing methodology which can represent and generate a large number of wide varieties of scanning paths. SCAN language uses four basic scan patterns. They are continuous raster C, continuous diagonal D, continuous orthogonal O, and spiral S. Each basic pattern has eight transformations numbered from 0 to 7. For each basic scan pattern, the transformations 1, 3, 5, 7 are reverses of transformations 0, 2, 4, 6, respectively. The basic scan patterns and transformations are shown in Fig.3.

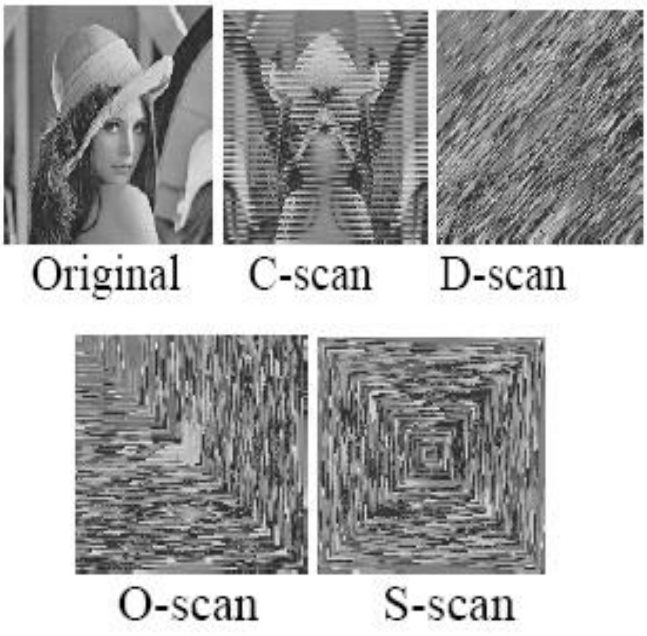

Fig3. *Original Image and Encrypted Image with Different SCAN Pattern*

EXPERIMENTS

The method used to evaluate the present technique is described in Fig. 2. The algorithm was applied on a bit mapped (bmp) image that has the size of 256 pixels x 256 pixels with 256 colors. In order to evaluate the impact of the number of blocks on the correlation and entropy, two different cases were tested.

Each case of block size produces three output images; (a) a ciphered image using the Blowfish algorithm, (b) carrier image (c) a ciphered image using the proposed algorithm followed by the Blowfish algorithm. For the rest of this paper, we use image A, image B, image C, and image D to denote the original image, the ciphered image using the Blowfish algorithm, the transformed image. And the ciphered image using the proposed algorithm followed by the Blowfish algorithm respectively.

Correlation and entropy are computed for each case according to equation (1) and equation (2)

$$r = \frac{n\sum(xy) - \sum x \sum y}{\sqrt{\left[n\sum(x^2) - (\sum x)^2\right]\left[n\sum(y^2) - (\sum y)^2\right]}} \qquad (1)$$

Where
r: correlation value
n: the number of pairs of data
$\sum xy$: sum of the products of paired data
$\sum x$: sum of x data
$\sum y$: sum of y data
$\sum x^2$: sum of squared x data
$\sum y^2$: sum of squared y data

Entropy defined as follows [18]-[19].

$$H_e = -\sum_{k=0}^{G-1} P(k) \log_2 (P(k))$$

Where:
H_e: entropy.
G: gray value of input image (0... 255).
$P(k)$: is the probability of the occurrence of symbol k.

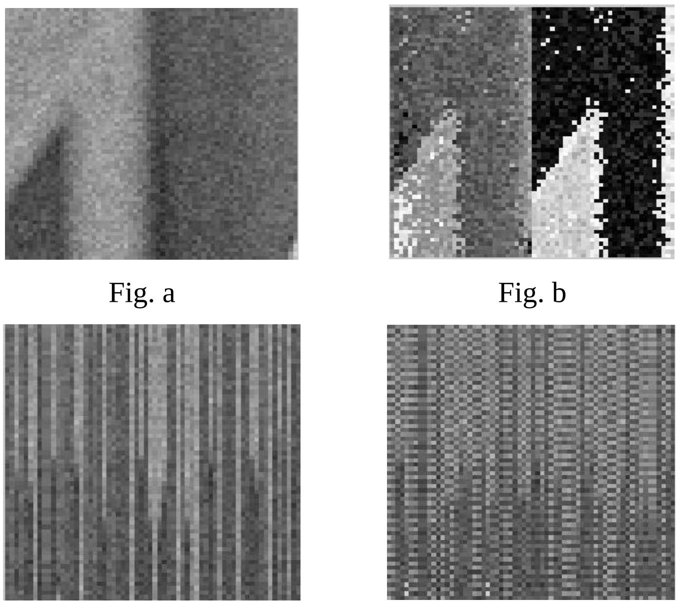

Fig. a

Fig. b

Fig. c

Fig. d

Fig3. *Results of Encryption by using 64 pixels × 64 pixels Blocks. (a) Original Image. (b) Encrypted Image using Blowfish. (c) Permutation Technique. (d) Proposed Technique*

The correlation and entropy results of this case are summarized in fig.4

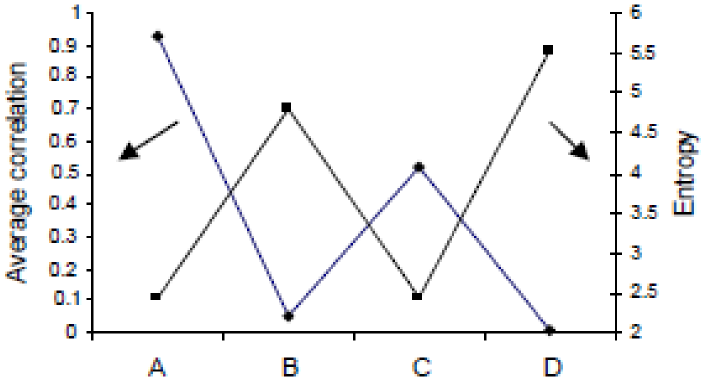

Fig4. *Average Correlation and Entropy*

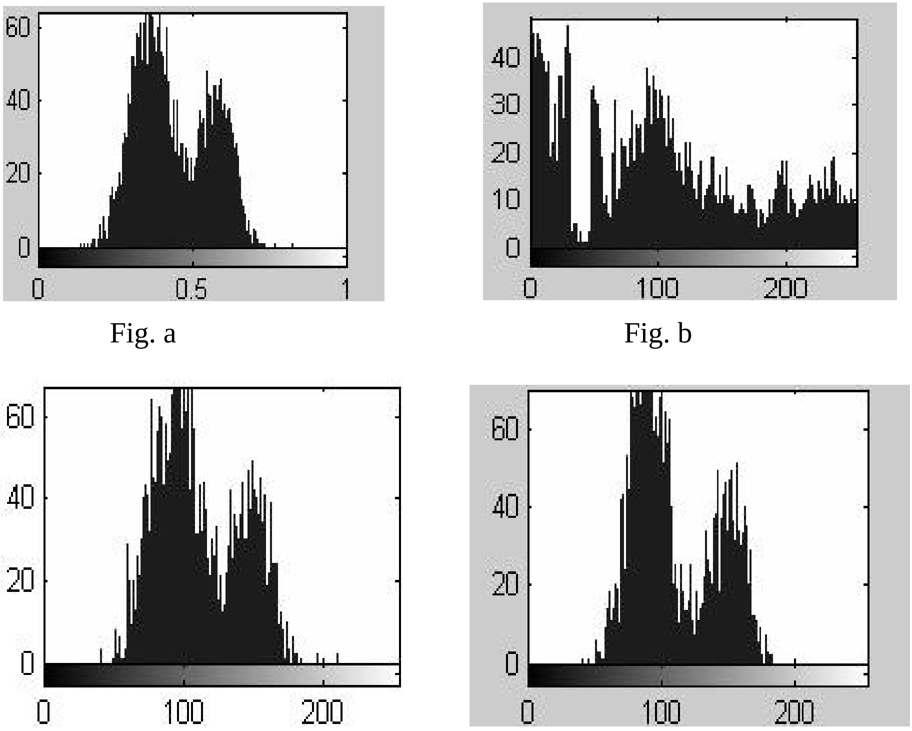

Fig. a

Fig. b

Fig. c

Fig. d

Fig5. *Results of Histogram of 64 pixels × 64 pixels Blocks (a) Original Image. (b) Encrypted Image using Blowfish. (c) Permutation Technique (d) Proposed Technique*

Table1. *Results of Correlation and Entropy Values*

image	No of pixel	Original	Permuted	Blowfish	Proposed
Entropy	64x64	5.68	6.7305	0.0857	6.701
Correlation		0.09	0.0012	0.52	0.003

CONCLUSION

In this paper a simple and strong method has been proposed for image security using a combination of permutation technique followed by encryption. The cases showed that the correlation was decreased when the proposed algorithm was applied to them. Experimental results of the proposed technique showed that an inverse relationship exists between number of blocks and correlation, and a direct relationship between number of blocks and entropy. When compared to many commonly used algorithms, the proposed algorithm resulted in the best performance; the lowest correlation and the highest entropy.

REFERENCES

[1] William Stalling. Handbook of "Cryptography and Network Security*,"* 4th Edition, Prentice Hall of India.

[2] B. Y. Mohammad Ali and J. Aman," Image EncryptionUsing Block-Based Transformation Algorithm," *IAENG International Journal of Computer Science, Vol. 35, Issue. 1, 2008, pp. 15-23.*

[3] B. Schneier, "Applied Cryptography," John Wiley & Sons, New York, 1994.

[4] Panduranga H.T. et al. *IJCSE International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010, 297-300.*

[5] Jawahar Thakur,Nagesh Kumar, "DES,AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis," *International Journal of Emerging Technology and Engg.Vol.1.* 2011.

AUTHORS' BIOGRAPHY

PRAVEEN KUMAR SHERI is working as a System Administrator in AGMR College of Engineering & Technology,Varur-Hubli-Karnataka. He has completed his B.E in Electronics & Communication Engineering from SJCE, Mysore, affiliated to VTU, Belgaum, Karnataka-INDIA. His area of interest is Wireless Sensor Networks, Network Security.

Prof. A. Tyagaraja Murthy Is working as an Associate professor at Sri Jayachamarajendra College of Engineering, Mysore, Katnataka-INDIA