KEY SECURED BLOCK BASED TRANSFORMATION FOR IMAGE ENCRYPTION

Mrs.Dhanashri M.Torgalkar 1, Prof.Mr.Nitin B. Sambre2

1 Student of Electronics and Tele-communication Department, KIT College of Engineering, Kolhapur, Maharashtra, India
2 Head of the Department of Electronics and Tele-communication, KIT College of Engineering, Kolhapur, Maharashtra, India

Abstract

Now a day, images are widely used in several processes. Therefore, secure transmission of image data is more important in many applications like military, medical imaging, video conferencing etc. Image encryption is mainly used for secure transmission of image data. Encryption is the process of transforming the information to another one which is hard to understand. Different security techniques have been used to provide the image encryption process. As we know, pixels in plain image are strongly correlated. In order to decrease this correlation, Block based transformation technique is specially used. The block transformation algorithm divides the image in to no. of blocks and shuffles their position of blocks to decrease the correlation and increase its entropy value. Divide an image in more no. of blocks gives the more security of image. Transformation table will decide new positions of blocks. The aim of Key secured block transformation is to enhance the security of an image. Here, key provide a security for transformation table .Different keys generated for different types of image so ,if input image data changed automatically key will also get change. Here key is used for two purposes, one for to build transformation table and second to encrypt image data. So as key changed, transformation table will also get change and image get transformed with this new transformation table. 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.

Key Words: Image Encryption, Image Correlation, Decryption, Image Entropy, Hash of key, Permutation. ...

1. INTRODUCTION

The security of digital images has become more and more important due to the rapid evolution of the Internet in the digital world today. Many different image encryption methods have been proposed to enhance the security of these images. Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data.

In most of the images, the values of the neighbouring pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbours). In order to dissipate the high correlation among pixels and increase the entropy value, we have introduced a transformation algorithm that divides the image into blocks and then shuffles their positions before it passes them to the encryption algorithm. In this case, correlation, histograms, entropy and Peak signal to noise ratio has used to measure the security level of image. This process results in lower correlation, higher entropy and uniformly distributed histogram as compared to encryption algorithm alone. It also results in lower PSNR (Peak signal to noise ratio) which proves better security for image.

In this process, Variable secret key is used for both purpose i.e. to build transformation table and encryption process. Variable key for transformation process is used to calculate hash values of key. These Hash value determines the seed, which is used to generate secret transformation table. If the key is changed, new Hash values will generates another seed, and then a different secret transformation table is obtained. So, Block transformation table will get changed as key get changed .Here key provide a security for transformation table.

1.1 Background

Nowadays, with the rapid growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. A large part of this information is either confidential or private. Information security is becoming more important in image storage and transmission. In order to achieve better security for image, many image encryption algorithms have been developed but no single encryption algorithm satisfies all type of images. Image encryption is mainly used to hide image data contents. Image information mostly perceived due to correlation among pixels. In order to disturb this correlation, block based transformation is commonly used. Here transformation table will decide new location of blocks of image data. This new technique Key...
secured block based transformation algorithm provides security about this transformation table.

1.2 Literature survey

In this paper, A.Mitra, Y.V. Subba Rao and S.R.M. Prasanna have proposed a new random combinational image encryption approach with bit, pixel and block permutations.

Mohammad Ali Bani Younes, and Aman Jantan have presented an image encryption algorithm in April 2008 which was the combination of permutation technique followed by encryption. They introduced a new permutation technique based on the combination of image permutation and the well known encryption algorithm called RijnDael.

Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki proposed a novel algorithm for image encryption based on SHA-512 hash function. The algorithm consists of two main sections: The first does preprocessing operation to shuffle one half of image. The second uses hash function to generate a random number mask. The mask is then XORed with the other part of the image which is going to be encrypted.

Sresh Pallavi Indrakanti and P.S.Avadhani[16] proposes a new image encryption algorithm based on random pixel permutation with the motivation to maintain the quality of the image. The technique involves three different phases in the encryption process. The first phase is the image encryption. The second phase is the key generation phase. The third phase is the identification process. This provides confidentiality to color image with less computations.

Avi Dixit, Pratik Dhruve and Dahale Bhagwan introduce an algorithm in September 2012. The binary code of the pixel values of a colour image is extracted and permuted according to the entered 8 bit key which is followed by the permutation of every 8 consecutive pixels.

Irfan.Landege, Burhanuddin Contractor, Aamna Patel and Rozina Choudhary introduce about encryption and decryption of images using a secret-key block cipher called 64-bits Blowfish which is an evolutionary improvement over DES, 3DES, etc designed to increase security and to improve performance.

Mohammad Ali Bani Younes proposed a new algorithm for image encryption in August 2013. This proposed algorithm uses the original image to shuffle and rearrange the pixels randomly within the image to build a newly transformed image using a transformation technique presented here. The transformed image is then XORed with the random variable key to produce the encrypted image.

In this paper, Nidhi Sethi, Sandip Vijay,a new encryption scheme proposed with two phases. In the first phase the input image is transformed using a new transformation technique whereas in the second phase Chirikov Standard Map is used for pixel shuffling and modified Logistic Map is used for diffusion. The results of experiments show that the proposed algorithm for image cryptosystems provides Low PSNR for better security of image.

1.3 Proposed Technique

[A] Transformation process

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 proposed technique is divided the image into number of blocks with predefined maximum and minimum number of pixels, resulting in a stronger encryption and a decreased correlation. Shuffle the position of all blocks within image.

New positions of blocks are as per mentioned in block transformation table. Here Transformation table get secure with the help of key .Secret key is generated from image data itself and it is used to determine the seed. Hash values of key are calculated using SHA 512 hash algorithm. Comparison of hash values will decide seed value 1 or 2. The seed plays a main role in building the transformation table. Now, Image gets transformed with these new location of blocks. This new transformed image is then fed to encryption block using a variable secret key which we used to select transformation table. If key is changed, Hash value and seed will also get change and it generates new transformation table. For better transformation, the block size should be small, because fewer pixels keep their neighbours. 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 neighbours. At the receiver side, the original image can be obtained by the inverse transformation of the blocks. Block diagram of proposed technique is shown in Fig.1
[B] Encryption and Decryption Process

a. In the encryption process, data image as a plaintext and the encryption key are two inputs of encryption process. Image data get encrypt with the help of key.

b. In the decryption process, encrypted image is entered to the decryption function and the same encryption key is used to decrypt the image. The process of decryption is continued with other blocks of the image from top to bottom.

2. RESULTS

The algorithm was applied on a bit mapped (bmp) image. Here, encrypted image without block transformation is compared with key secured block transformed encrypted image. In this case, the performance of the proposed image encryption scheme is analyzed including some important ones like statistical analysis, Histogram Analysis; visual observation etc. to prove the proposed image encryption is secure against the most common attacks.

Figure 2 and Figure 3 shows the result of proposed algorithm for Image1.bmp and Image 2.bmp respectively.
Fig. 3: (a) Plain Image1.bmp gray scale image (b) Block transformed image. (c) With block transformed encrypted image (d) Decrypted image

2.1 Statistical Analysis

Image 1.bmp and Image 2 .bmp are Plain images chosen for analysis

Table 1: Secret transformation table selected by proposed algorithm

<table>
<thead>
<tr>
<th>Image</th>
<th>Image size</th>
<th>Generated Seed from key</th>
<th>Secret transformation table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image 1.bmp</td>
<td>300 x 300</td>
<td>Seed 2</td>
<td>Transformation table 2</td>
</tr>
<tr>
<td>Image 2.bmp</td>
<td>230 x 230</td>
<td>Seed 1</td>
<td>Transformation table 1</td>
</tr>
</tbody>
</table>

Analytical parameters (correlation, entropy, PSNR) will be carried out on the selected block transformed encrypted image.

a. Correlation of two adjacent Pixels

Correlation is a measure of the relationship between two adjacent pixel values. There is a very good correlation between adjacent pixels in the image data. In these result showed that correlation between image elements is significantly decreasing by using the proposed algorithm. So, increasing number of blocks by using smaller block sizes are used in a lower correlation. Then, calculate their correlation coefficient using the following two formulas:

\[ C_r = \frac{N \sum_{j=1}^{N} (X_jY_j) - (\sum_{j=1}^{N} X_j)(\sum_{j=1}^{N} Y_j)}{\sqrt{[N \sum_{j=1}^{N} X_j^2 - (\sum_{j=1}^{N} X_j)^2][N \sum_{j=1}^{N} Y_j^2 - (\sum_{j=1}^{N} Y_j)^2]}} \]

Where,

X and Y are gray values of two adjacent pixels in the original and encrypted image.

N is the total number of adjacent pixels selected from the image.

b. Entropy

It is well known that entropy is measures the uncertainty association with random variable. As for gray scale Image in Block Based Image Encryption decreases the mutual information among encrypted image variables (i.e. high contrast) and thus increases the entropy value, if increasing number of blocks is resulted in higher entropy. It should fulfil a condition on the information entropy that is the ciphered image should not provide any information about the plain image. The information entropy is calculated using equation:

\[ H_e = \sum_{k=0}^{256} P(K) \cdot \log_2(P(K)) \]

Here: He= Entropy of image

G = Gray value of an input image (0-255).

\[ P(k) = \text{Probability of the occurrence of symbol } k \]

Table 2: Average Correlation of Two adjacent pixels

<table>
<thead>
<tr>
<th>Image</th>
<th>Plain Image</th>
<th>Encrypted Without Block Transformed</th>
<th>Encrypted With Block Transformed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>10 pixels/ block</td>
<td>5 pixels/ block</td>
</tr>
<tr>
<td>Image 1.bmp</td>
<td>0.90</td>
<td>0.05</td>
<td>0.03</td>
</tr>
<tr>
<td>Image 2.bmp</td>
<td>0.91</td>
<td>0.05</td>
<td>0.028</td>
</tr>
</tbody>
</table>
### Table 4: Result of image Entropy

<table>
<thead>
<tr>
<th>Image</th>
<th>Plain Image Entropy</th>
<th>Encrypted Without Block Transformed</th>
<th>Encrypted With Block Transformed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>10 pixels/block</td>
<td>5 pixels/block</td>
</tr>
<tr>
<td>Image 1.bmp</td>
<td>2.75</td>
<td>7.9980</td>
<td>7.9981</td>
</tr>
<tr>
<td>Image 2.bmp</td>
<td>7.6753</td>
<td>7.9981</td>
<td>7.9987</td>
</tr>
</tbody>
</table>

### c. Peak Signal-to-Noise Ratio

Peak signal to noise ratio is the ratio between the original image and the encrypted image. PSNR is calculated in decibels. The higher the PSNR, the closer the encrypted image is to the original. In general, a higher PSNR value should correlate to a higher quality image. For good encryption scheme the PSNR should be as low as possible.

### Table 5: PSNR for Image1.bmp and Image 2.bmp

<table>
<thead>
<tr>
<th>Image</th>
<th>Encrypted Without Block Transformed</th>
<th>Encrypted With Block Transformed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image 1</td>
<td>9.3104</td>
<td>9.3015</td>
</tr>
<tr>
<td>Image 2</td>
<td>6.8355</td>
<td>6.8205</td>
</tr>
</tbody>
</table>

### 2.2 Histograms Analysis

The original image and its corresponding encrypted image and their histograms of red, blue and green channels. It is clear that the histogram of the encrypted image is nearly uniformly distributed and significantly different for the respective histograms of the original image.
CONCLUSIONS

This technique aims at enhancing the security level of the encrypted image by using key secured block transformation and reducing the correlation among image elements. Dividing the image into a larger number of blocks made the performance even better to reduce correlation among pixels. For first image, transformation table 1 is getting selected according to its image size and key. Whereas for second image transformation table 2 is selected. It showed that, proposed algorithm provide high security about using of transformation table. The results of comparison of without block transformed encrypted image with block transformed encrypted image showed that: The correlation is decreased and Entropy increased due to increased number of block. It was found that PSNR (Peak signal to noise ratio) is lower for Block transformed encrypted image. Lower PSNR indicates better encryption.

REFERENCES


[2]. Kevin Allison, Keith Feldman, Ethan Mick “Blowfish Algorithm”.


BIOGRAPHIES

Appeared for M.E. (Electronics and Tele-communication) in KIT college of engineering, Kolhapur

[2] Prof. Nitin B. Sambre received M.E. degree in Electronics and currently working as Head of the Electronics and Tele-communication department of KIT college of engineering, Kolhapur.