ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Blowfish Encryption Using Key Secured Block Based Transformation

Mrs.Dhanashri M.Torgalkar[*1], Prof.Mr.Nitin B. Sambre[2]

[*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

dhanashritorgalkar@gmail.com

Abstract

Encryption is a process of converting a one form of information in another form which is hard to understand .Now a days, a large amount of information get transfer with wired or wireless network. Information contents may be textual data or image data. Therefore encryption of text or image is most important during secure transmission of information. Images are widely used in several processes like military field, medical imaging, video conferencing where confidentiality about image information is very important. As we know, pixels in plain image are strongly correlated. Image information get perceive due to this high correlation. Most of available image encryption algorithms are used for encryption of pixel information only but key secured block based transformation technique change the position of pixels and provide low correlation among image pixels so that less amount of information get perceived . 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. Here we used Blowfish image encryption algorithm because of variable and longest key size. At the receiver side these blocks are retransformed in to their original position and performed a decryption process which gives the original image.

Keywords: Image Encryption, Blowfish encryption, Image Correlation, Decryption, Image Entropy, Hash of key, Permutation.

Introduction

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.

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 that correlation, histograms, entropy, Peak signal to noise ratio and mean absolute error has used to measure the security level of image. This process results in lower correlation, higher entropy, and uniform histogram as compared to encryption algorithm alone. It also results in lower PSNR(Peak signal to nise ratio) and higher MAE(Mean absolute error) which proves better security for image.

In this paper we are implementing blowfish algorithm which is strongest and fastest in data processing/storing compare to other algorithms. Blowfish algorithm is highly secured because it has

ISSN: 2277-9655
Impact Factor: 1.852

variable longer key length (more no of key size).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 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.

Background

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.

Literature Survey

[1] A new image Encryption Approach using a combination of permutation techniques, 2006[1]

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.

[2] An Image Encryption Approach using a Combination of Permutation Technique Followed by Encryption [4]

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. The results showed that the correlation between the image elements was significantly decreased by using the combination technique and higher entropy was achieved

[3] A Novel Image Encryption Algorithm Based on Hash Function, 2010[5]

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

[4] Permutation based Image Encryption Technique, 2011 [6]

Sesha 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.

[5] Image encryption using permutation and rotational xor technique, 2012[8]

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.

[6]Image encryption and decryption using blowfish algorithm,April 2012[9]

Irfan.Landge, 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

[7] Image Encryption Using Shuffling Technique, August 2013[10]

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.

[8] Comparative Image Encryption Method Analysis Using New Transformed - Mapped Technique 2013[11]

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 and High MAE for better security of image.

ISSN: 2277-9655
Impact Factor: 1.852

Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here.

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 in to random 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 blowfish encryption process. 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

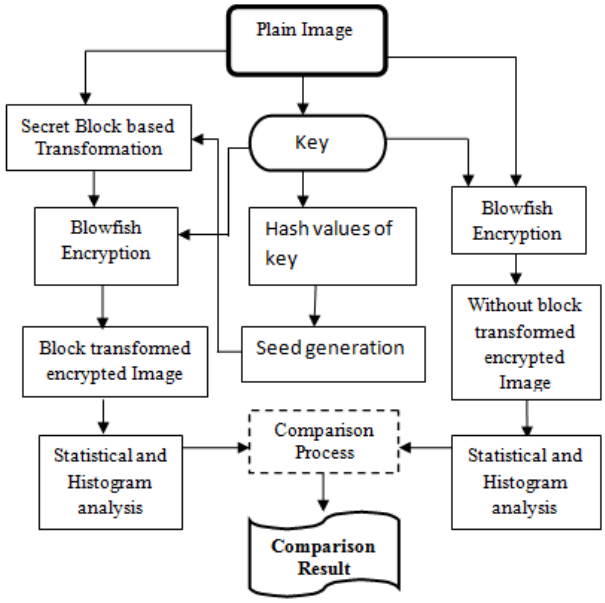


Fig.-2:
Algorithm selection_transformation

TABLE
1. Input Image.
1.1 Get size of Image as X, Y
1.2 LowerHorizontalNoBlocks = Int(X /10)
1.3 LowerVerticalNoBlocks = Int(Y /10)
1.4 No Blocks = HorizontalNoBlocks * VerticalNoBlocks
1.5 Calculate KEY from X, Y
1.6 Divide Key in two parts KEY1, KEY 2
1.7 Find HASH Values of keys as HASH1, HASH 2
If HASH 1 > HASH 2 then
SEED =1
Else
SEED =2
1.5 For SEED =1
Get Inverse Image Matrix
RANDOM TRANSFORMATION TABLE 1
For SEED =2
RANDOM TRANSFORMATION TABLE 2
END SELECTION_TRANSFORMATION TABLE

ALGORITHM PERFORM_TRANSFORMATION
1: For I = 0 to No Blocks -1
1.1: Get the new location of block I from the
RANDOM TRANSFORMATION TABLE 1(For SEED 1)
Or
RANDOM TRANSFORMATION TABLE 2(For SEED 2)
1.2: Set block I in its new location
END PERFORM_TRANSFORMATION
End perform transformation

ISSN: 2277-9655
Impact Factor: 1.852

Input: Original Image and Transformation table

***Output*:** Transformed Image.

[B] Encryption and Decryption Process

Blowfish encryption algorithm is a symmetric block cipher that can be effectively used for encryption and Decryption.

The block size is 64 bits blocks and key can be any length up to 448 bits before encrypting them. It takes a variable length key from 32 to 448 bits. This algorithm has 16 rounds and each round consists of a key-dependent permutation and a key and data dependent substitution. All operations are XORs and additions on 32-bit words. A feistal network is a general method of transforming any function into a permutation.

a. **In the encryption process,** data image as a plaintext and the encryption key are two inputs of encryption process. In this case, original image data bit stream is divided into the blocks length of Blowfish algorithm

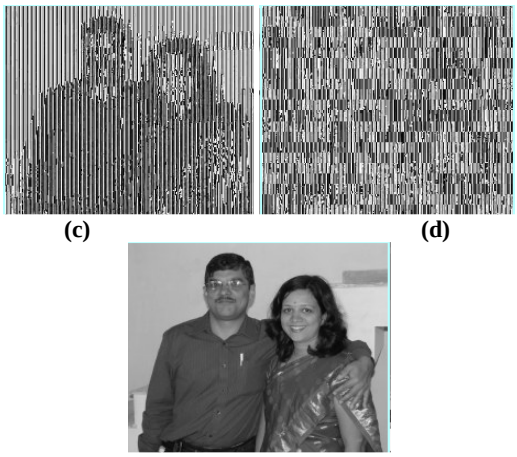
b. **In the decryption process**, the encrypted image is divided into the same block length of Blowfish algorithm from top to bottom. The first block is entered to the decryption function and the same encryption key is used to decrypt the image but the application of sub keys is reversed. The process of decryption is continued with other blocks of the image from top to bottom.

Results

The algorithm was applied on a bit mapped (bmp) 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 (gray scale) and Image 2.bmp (color) respectively.

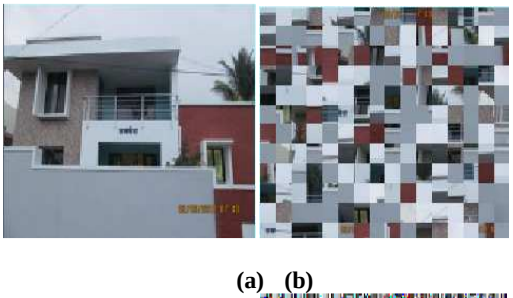
(a) (b)



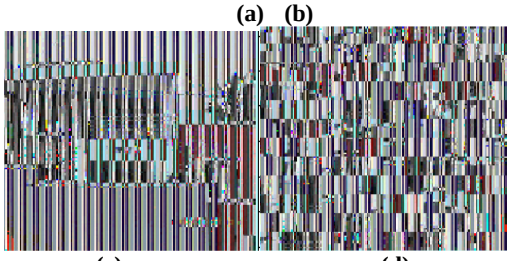
(c) (d)

(e)

Fig-.2 :(a) Plain Image1.bmp gray scale image (b) Block transformed image. (c)Without block transformed encrypted image(d)With block transformed encrypted image(e) Decrypted image.



(a) (b)



(c) (d)

(e)

Fig.-3: (a) Plain Image1.bmp gray scale image (b) Block transformed image. (c)Without block transformed encrypted image(d)With block transformed encrypted image(e) Decrypted image

ISSN: 2277-9655
Impact Factor: 1.852

Statistical Analysi

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

Table 1: Secret transformation table selected by proposed algorithm

Image	Image size	Generated Seed from key	Secret transformation table
Image 1.bmp	300 x 300	Seed 2	Transformation table 2
Image 2.bmp	230 x 230	Seed 1	Transformation table 1

Analytical parameters (correlation, entropy, PSNR and MAE) 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.

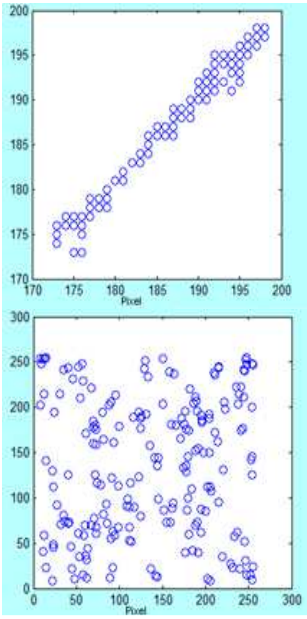


Fig.4 Distribution of two adjacent pixel of original image (a) and Encrypted image (b)

Table 2: Average Correlation of Two adjacent pixels

Image	Plain Image	Encrypted Without Block Transformed	Encrypted With Block Transformed	
			10 pixels/ block	5 pixels/ block
Image 1.bmp	0.95	0.15	0.02	0.017
Image 2.bmp	0.71	-0.25	-0.08	-0.06

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:

$$H_e = \sum_{K=0}^{256}(P(K).\log_2(P(K))$$

Here: He= Entropy of image

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

P (k) = Probability of the occurrence of symbol k.

Table 4: Result of image Entropy

ISSN: 2277-9655
Impact Factor: 1.852

Image	Plain Image Entropy	Encrypted Without Block Transformed	Encrypted With Block Transformed	
			10 pixels/ block	5 pixels/ block
Image 1.bmp	7.2524	7.9044	7.9060	7.9063
Image 2.bmp	7.6125	7.9328	7.9345	7.9355

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.

d. Mean absolute error:. It is used to measure how close predictions are to the eventual outcomes. The larger the value of MAE better is the image security.

Table 5: PSNR and MAE for Image1.bmp

Analytical parameter	Encrypted Without Block transformed	Encrypted With Block transformed
PSNR	10.69	8.973
MAE	52.60	69.07

Table 5: PSNR and MAE for Image2.bmp

Analytical parameter	Encrypted Without Block transformed	Encrypted With Block transformed
PSNR	10.14	9.27
MAE	53.79	65.28

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.

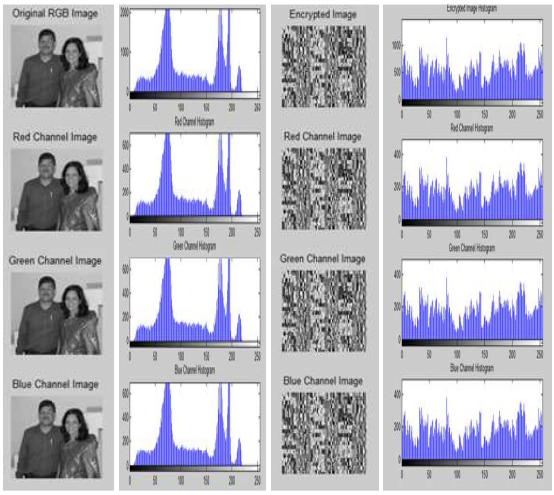


Fig.-4: Histogram of red, blue and greens of the original image and Encrypted image1.bmp

Visual observation

A number of images are encrypted by the proposed method and visual test is performed. By comparing the original and the encrypted images, there is no visual information observed in the encrypted image also following figure shows encryption by proposed algorithm gives no visual information where as encryption by commercial algorithm gives some amount of information about object in image

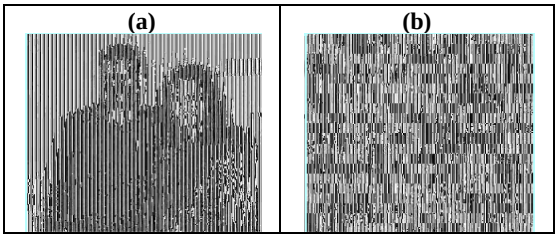


Fig.-5 : Image encrypted by without block transformed (a) and Encrypted with block transformed (b)

Conclusions

This technique aims at enhancing the security level of the encrypted images by reducing the correlation among image elements and increasing its entropy value. 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,

ISSN: 2277-9655
Impact Factor: 1.852

proposed algorithm provide high security about using of secret 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. MAE (Mean absolute error) is also high for Block transformed encrypted image than without block transformed encrypted image. High value of MAE means image security is more.

References

[1] *Mitra, Y. V. Subba Rao and S. R. M. Prasanna,"A New Image Encryption Approach using combinational permutation Techniques" International Journal of Electrical and Computer Engineering , 2006*

[2] *Kevin Allison, Keith Feldman, Ethan Mick "Blowfish Algorithm".*

[3] *Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block-Based Transformation Algorithm" IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03, 2008.*

[4] *Mohammad Ali Bani Younes and Aman Jantan , "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" Mohammad Ali Bani Younes and Aman Jantan , IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.4, April 2008*

[5] *Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki, "Novel Image Encryption Algorithm Based on Hash Function", 2010 proposed a novel algorithm for image encryption based on SHA-512 hash function.*

[6] *Sesha Pallavi Indrakanti and P.S.Avadhani, "Permutation based Image Encryption Technique", 2011*

[7] *Avi Dixit, Pratik Dhruve and Dahale Bhagwan, " Image encryption using permutation And rotational xor technique" Natarajan Meghanathan, et al. (Eds): SIPM, FCST, ITCA, WSE, ACSIT, CS & IT 06, pp. 01–09, 2012.*

[8] *Irfan.Landge1, Burhanuddin Contractor2, Aamna Patel3 and Rozina Choudhary4, "Image encryption and decryption using blowfish algorithm" World Journal of Science and Technology 2012, 2(3):151-156 www.worldjournalofscience.com.*

[9] *Mohammad Ali Bani Younes Department of computer Science National University of Ajloun, Irbid, Jordan, " Image Encryption Using Shuffling Technique" International Journal of Computer Science Research & Technology (IJCSRT) Vol. 1 Issue 3, August - 2013*

[10] *Nidhi Sethi and Sandip Vijay, "Comparative Image Encryption Method Analysis Using New Transformed - Mapped Technique". Conference on Advances in Communication and Control Systems 2013*