Indian Journal of Science and Technology, *Vol 8(36), DOI: 10.17485/ijst/2015/v8i36/87852, December 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Image Encryption based on the Reflected Binary Code Method with the Combination of FFT

R. Vijayaraghavan*, S. Sathya and N. R. Raajan

Department of Electronics and Communication Engineering, School of Electrical and Electronics Communication, SASTRA University, Thanjavur - 613401, Tamil Nadu, India; ragavtanjore@gmail.com, sathyaa43@gmail.com, nrraajan@ece.sastra.edu

Abstract

Image encryption is used to protect the data of an image in the most secure way. In this paper, we perform encryption and decryption of the three color planes based on gray code effect and fast Fourier transform. Gray level codes indicate that occurrence of one bit changes from a previous state of current. This process allows the system to detect the error when more than one bit changes occur. It is more efficient than binary bit plane decomposition. The Fourier transform is mainly used to represent the frequency characteristic of a spatial domain image. The color plane scrambling process is done by combining three individual encrypted planes into one composite image. This method which is applicable for any type of image formats as bmp, JPEG, GIF. This paper gives a simple way to scramble the image in unpredictable way. It provides more security than other encryption algorithm. The original images can be retrieved using a correct security key which achieves better results than the other existing methods. By exploiting gray code and Fourier transforms it increases the difficulty of decoding.

Keywords: Bit Plane Decomposition, Color Plane Scrambling, Fast Fourier Transform, Gray Code, Image Encryption

1. Introduction

It is very important to communicate the information personally which is prevented from the interception of third parties[1]. Nowadays technology has improved a lot so security issues become more important to protect the information. There are many ways to transfer the information in ensuringway. Transferring the information from sender to receiver is to be very confidential so encryption is essential[2]. In this paper, we focus on color image encryption. Scrambling is used to provide a high security level. It ensures a privacy protection of images from the attack of hackers. There are various image encryption schemes are proposed. The security of digital images plays a major role in the field of communication[3]. Here encryption is done based on the gray code method which is very potent to secure the information. Color plane scrambling makes the retrieve of information at receiver more difficult by shuffling the data[4]. Image encryption is used to scramble the pixels of an image and reduce the correlation among the pixels in order to make difficult to hack the information. High level encryption is based on the choice of security key used[5]. Image encryption techniques based on DCT, Wavelet, Transparent encryption and advanced techniques such as permutations[6]. Images are permuted in random order based on three methods like bit, pixel and block permutation. No single encryption can satisfy all types of image formats. In our proposed method, scrambling of three RGB plane is depleted by means of gray code and Fourier transform. By using this it provides a high level of security in the field of image analysis, image encryption and image compression.

2. Outline of the Proposed Method

Consider the color image which is divided into three individual RGB planes. Each pixel of the image is indicated

*Author for correspondence

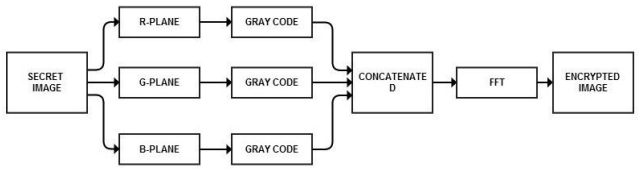

Figure 1. Encryption.

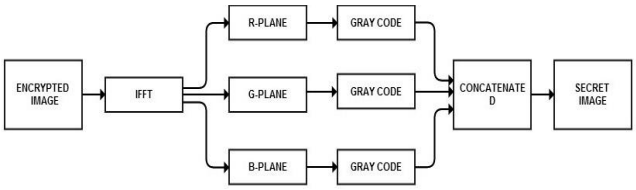

Figure 2. Deccryption.

Figure 3. Original image.

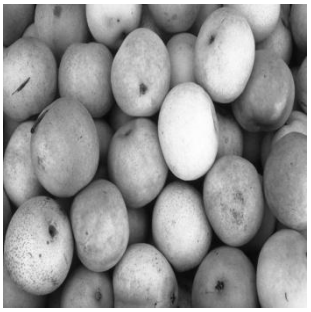

Figure 4. Separated R.

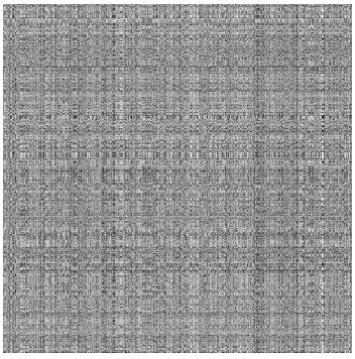

Figure 5. Gray coded & FFT- R

Figure 6. Separated G.

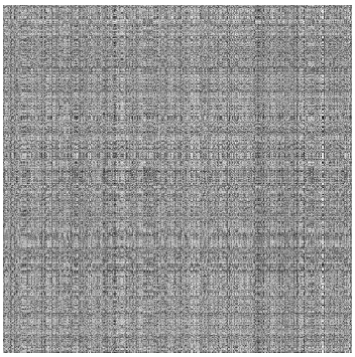

Figure 7. Gray coded & FFT- G.

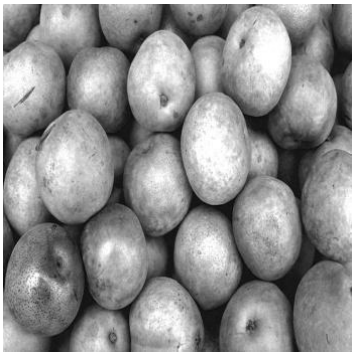

Figure 8. Separated B.

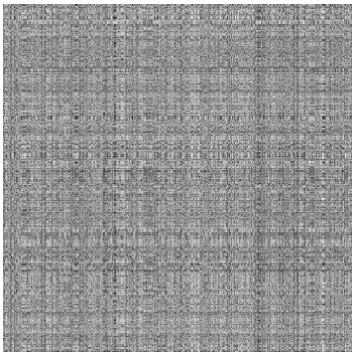

Figure 9. Gray coded & FFT- B.

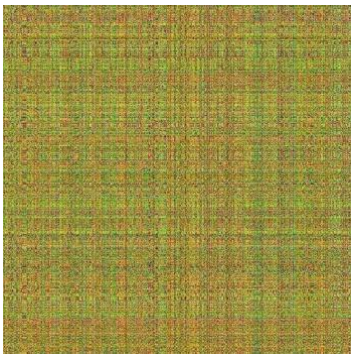

Figure 10. Protected image.

by RGB plane. Random permutation is based on shuffling the pixels of an image by two transforms. Gray code is used for pixel scrambling to obtain the scrambled image in order to protect the image. Further enhancing the level of encryption is again encrypted using fast Fourier transform. Encrypted individual RGB plane image is obtained using this two transform. Finally it is combined to get the encrypted single color image.

At the decryption end the reverse process of encryption is done. Encrypted color image is split into three individual encrypted RGB plane. Using inverse fast Fourier transforms to decrypt the RGB plane and further by using gray code transform is again decrypted. The decrypted individual RGB plane is obtained which is combined to get the original color image.

3. Methods

3.1 Gray code

Gray code is used as the secret key to encrypt the images which produce a scrambled image and then this encrypted image is further modified by applying Fourier transform. By using of gray code it increases the security of an image. The intruder cannot hack the information without knowing what type of security method is used.

In this paper two methods are involved for scrambling such as substitution and transposition[7]. Gray code is a form of binary representation which is used to indicate the change of one bit[8] in each current state compared to previous state. It produces lossless encryption for all types of image formats. Gray coding is a technique for scrambling the pixel of an image. It exhibits only a minimum change of codes only one bit change will occur[9]. The change of bit is always occurring from LSB to MSB and changes occur in the form of binary 0 or 1.

It indicates the confidentiality of secret method of scrambling. It is used to prevent the error in the data which is a very efficient secure method. This method elevates the need of robustness[10] against image scrambling.

3.2 Encryption Process

Take an input as any type of image format. Each pixel in the image is represented in decimal form.

- Values are converted into binary representation.
- Binary to gray code conversion is applied.
- Gray code form is obtained by only changing one bit in each step it occurs from right to left.

This code is attained by considering the first bit of the binary number as the MSB[11] of gray code

The Second bit of gray code will be XORing[12] of first and second bit of binary number and third bit of gray code is obtained as XORing of second and third bit and this process is repeated on until the last bit. Decimal form of a gray code is obtained as final result which is used as the secret key for scrambling an image.

3.3 Decryption Process

On the receiver side decimal form of gray code is converted to binary.

Take MSB of gray code as the first bit of binary numbers and the second bit of gray code is 0 then the second bit of binary number same as the first bit gray code.

If the gray bit is 1, second binary bit will change and this process is repeated for all the bits. Decimal form of a binary number indicates the pixel of an image.

3.4 Transform Domain Approach

Image scrambling is further extended by applying the transform domain approach[13]. In this paper we employ FFT to transform the image into another form. The Fourier transform is generally used to access information about geometric characteristics of the spatial domain image[14]. It is applicable for all types of image format. It provides flexibility in shuffling the pixel of an image. This transform will be applicable to many areas including image processing, radar and optics[15]. It is used to switch the magnitude and phase represented in the form of the frequency domain. If Fourier transform is done then color plane limits is adjusted to display the sufficient amount of information in an image.

The pixel value of an image represents an intensity value which is encrypted using gray code before doing FFT. After applying a transform most of the information on Fourier domain is available in the central part of an image[16]. By this it corresponds to linear changes in the images. It is used to switch the magnitude and phase of an image in Fourier domain where phase holds more information which is mainly used to reconstruct an original image. The color image is to be converted to gray image before running the transform because fft is mostly applicable for grayscale images.

Here scrambling of an image is done by shuffling the rows and columns of an image using a Fourier transform. FFT is also used for noise removal in image processing. It represents the number of frequencies correspond to the number of pixels in an image. It exhibits in the form of sinusoidal components in the mode of magnitude and phase. It is easy to analyze the certain frequencies of an image. The pace of an image does not hold more information but without this component resultant magnitude[17] of an image result in corruption. The process involved in scrambling is to compute the keyed FFT of the original image. After computing gray code encryption applies FFT in order to further encrypt an image using the following code.

Fast Fourier Transform is generally used to map spatial domain functions into frequency characteristics.

The input is an image which is used to represent the frequency characteristics of the pixels of an image in the spatial domain.

The FFT of a signal f (n) is given in the form of an equation

$$F(X,Y)=\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}f(m,n)e^{-j2\pi(x\frac{m}{M}+y\frac{n}{N})}$$

$$f(m,n)=\frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}F(x,y)e^{j2\pi(x\frac{m}{M}+y\frac{n}{N})}$$

Where F (x, y) is the frequency domain of an image corresponding to the coordinates x and y. F (m, n) represents the pixel characteristics of an original image. M and N are the dimensions of the original image

The Fourier transform is characterized into real and imaginary components is used to characterize the value of an image in the frequency domain

The inverse transform is used to transpose the frequencies to the spatial domain. The inverse fft is used to reconstruct the original image

The output of Fourier transforms represent the image which has a greater range than in spatial domain it represents the frequency characteristics of an image more accurately

Steps involved in applying the Fourier transform of an image to further encrypt an image.

- Take Fourier transforms for 2D image (spatial domain).
- Apply convolution operations.
- Analyze the results using filters.

Take Fourier transform of an original image which is used to exploit a magnitude and phase of an image.

Magnitude component represents the major portion of the information in an image to construct an image

The phase does not reveal more information but it is essential to reconstruct.

- Convert image into the spatial domain (back to original format) using simple reverse operation of faith.

4. Implementation

Consider a color plane of an image which is isolated into three RGB color planes. Each pixel of an image is represented by the individual RGB planes. Scrambling of a color image is done by applying two methods such as gray code and Fourier transform. Gray code is a most popular encoder output type which is used to prevent data errors. It specifies the minimum change in the code from the previous state. After decomposing into three color planes exploit encryption using gray code. It is used to excerpt a binary sequence in which an only one bit changes value when shift between adjacent states.

Consider 3 × 3 pixel of an image

160	162	164
166	168	170
172	174	176

Example of Encryption Function:
1st pixel decimal value –160
Binary value of 160 – 10100000
Gray code for 10100000 is 11110000

1 0 1 0 0 0 0 0	Binary
1 1+0 0+1 1+0 0+0 0+0 0+0 0+0	
1 1 1 1 0 0 0 0	Gray

Decimal value of 11110000 is –240 which is used as encryption keys.

Example of Decryption Function:
Gray code decimal value-240
240 is represented in 11110000

1 1 1 1 0 0 0 0 → Gray
1 0 1 0 0 0 0 0 → Binary

Decimal value of 10100000 is 160 which decrypted using gray to binary conversion.

The technique involves concede the pixel of an image which is generally represented in decimal form. It is first converted into binary form and then exploits binary to gray code conversion. The decimal form of gray code is obtained. It is used as a secret code to encrypt an image. The reverse process of decryption is done receiver side as encryption to obtain decimal form of binary numbers to retrieve the original image. It is very difficult to hack by the third party without knowing what key is employed. It is even able to attack but it takes much time to find even several years. Further to make more secure encryption again Fast Fourier Transform method is exploited. Because it is used in wide area of applications such as image analysis, image reconstruction, image filtering and image compression.

The Fourier transform is used to represent the frequency characteristic of spatial domain image. The advantage of representing in frequency space is that performs some better manipulation than in image space. The main use of Fourier transform is to remove the repeated noise from an image.

The matrix is obtained by after encrypting using binary to gray code conversion

Take 3 × 3 matrixes

240	243	246
245	252	255
250	249	232

Take Fourier transform of an original image and covert into sinusoidal components

It represents a frequency characteristic of spatial domain image it exhibits minimum changes in the image

7.35	7.44	7.33
–0.075 + 0.0433i	–0.075 – 0.026i	0.025 – 0.1992
–0.075 – 0.433i	–0.075 + 0.026i	0.025 + 0.1992i

The magnitude of an image reveals vertical and horizontal lines similar to the pattern in an original image.

Without the phase of an image it is difficult to reconstruct an original image

Exploit random permutation in transforming the image by shuffling the rows and columns of pixels of an image

240	243	246
245	252	255
250	249	232

Apply inverse Fourier transform to reconstruct an original image where phase of an image is essential to retrieve an image

The result of the Fourier transform consists of two channels. The first channel is used to specify the intensity values of an image where DC component displays in the central part of an image in Fourier domain. Incase low frequencies contain more details than higher frequencies because the intensity value of a pixel is too large to exhibit on the screen. In this paper implementation of Fourier Transform is done on RGB color plane. It produces magnitude and phase component in different channel such as RED and GREEN channel. After exploiting Fourier transform RED channel will contain the magnitude information which is also referred to as power spectrum while the green channel involves phase information. Both channels are required to retrieve an original image. Once the Fourier transform has done, combine the RGB channel module into a single image. Finally we obtain the scrambled three color planes of Fourier transform of an image.

By applying inverse Fourier transforms reconstruct an encrypted image and further it is again decrypted by using gray to binary code. Decimal form of gray code is converted into binary numbers to recover the pixel of an image. The pixels of an original color image are represented in decimal form of binary numbers in image analysis purposes. Thus finally three RGB color plane is reconstructed and lastly converts back into the original color image. By this method of encryption it is very difficult to predict the information only the sender and receiver know the type of secure method is employed. In Gray code method no data error is possible which is more reliable than binary bit plane decomposition. Fourier transforms which performs better than slower DFT and it also reduces the operational complexity compared to other methods. By the method of Fourier transform further increasing its difficulty of decoding techniques. Gray code transform is applicable for bit plane shuffling and pixel scrambling in image encryption. By employing Fourier transform to encrypt the image it is more secure and robust against attacks. We concluded that this image

encryption technique is better than the other security level of existing bit plane decomposition encryption methods.

5. Comparison of Results with Existing Methods

There are a number of methods are available in today's security systems. In this paper we considered a Bit Level Permutation (BLP) method to compare our proposed method results.

5.1 Bit Level Permutation

This method consists the effect of scrambling in the bit constitution of the each pixel. Although it aims to do modification on bits, it is restricted on each bit plane to make its operation.

Let we analyze the results with the help of the correlation coefficient method

$$r_{x,y} = \frac{E\{[x - E(x)][y - E(y)]\}}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$E(x) = \frac{1}{S}\sum_{i-1}^{S} x_i$$

$$D(x) = \frac{1}{S}\sum_{i-1}^{S}[x_i - E(x)]^2$$

Correlation coefficient examines the relation between the two images. As per the aim of our work cipher image should contain no relation between its original plain images. Our results show the cipher image contains fewer relations with its plain image.

Table 1. Correlation coefficient results for plain and encrypted images

		Original	Proposed method	BLP method
R plane	*Horizontal*	0.980011	–0.00213	–0.00032
	Vertical	0.980910	–0.00142	–0.00412
	Diagonal	0.967012	0.00203	0.00039
G plane	*Horizontal*	0.962214	–0.00132	0.00217
	Vertical	0.987105	0.00149	0.00110
	Diagonal	0.955482	–0.00315	0.00392
B plane	*Horizontal*	0.933412	–0.00049	0.00156
	Vertical	0.954142	–0.00021	0.00174
	Diagonal	0.912482	0.00029	0.00036

6. Results

Color image which is divided into three RGB planes it represent the each pixel of an image. Scrambled image is done by using two methods such as gray code and fast Fourier transform. The original image is scrambled using gray code to preserve the secret information. The following images used for encryption and decryption process is shown below

Three individual RGB planes are encrypted using gray code and which is concatenated to obtain a single color image. The Gray coded image indicates the change in the one bit position from the previous state.

Figure 11. Secret Image.

Figure 12. Gray Coded.

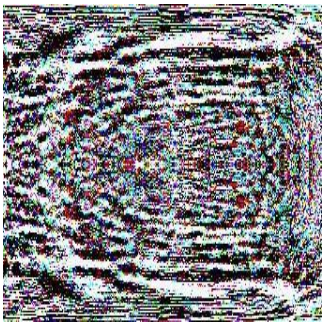

Figure 13. FFT image.

Further it is again scrambled by using fast Fourier transform to increase the level of security which exploit the encrypted image. It encrypts the image in the form of sinusoidal components which achieves the better security level.

In decryption end it is descrambled by inverse Fourier transform to obtain three individual RGB planes which are further decrypted by using a gray code effect to obtain the secret image

It is concatenated to obtain the original color image which is decrypted by using above two methods. The retrieved image is obtained as same as the original color image it is more secure than other methods.

The resulted MSE, PSNR and MSSIM values for three individual RGB color plane images are tabulated as above. Image quality is measured based on many aspects, there are different evaluation metrics are used to analyze the image quality. The performance metrics used here are Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Mean Structural Similarity Index Measure (MSSIM).

Figure 14. Decrypted1 (Gray Coded).

Figure 15. Decrypted2 (Secret).

Table 2. Tabulation for encrypted image

Name	MSE (r)	MSE (g)	MSE (b)	PSNR (r)	PSNR (g)	PSNR (b)	MSSIM
Pears.png	5.2382e+06 + 8.4969e+02i	5.2659e+06 + 1.2823e+03i	1.5662e+06 + 4.1499e+02i	19.0270 – 0.0007i	19.0499 – 0.0011i	13.7837 – 0.0012i	0.0154 – 0.0000i
Autumn.tif	7.5718e+05 + 8.5799e+02i	6.7439e+05 + 5.5547e+02i	6.8233e+05 + 2.5352e+03i	10.6272 – 0.0049i	10.1243 – 0.0036i	10.1752 – 0.0161i	0.0140 – 0.0000i
Football.jpg	8.1891e+05 + 1.0678e+01i	6.0200e+05 + 1.3924e+01i	7.3208e+05 – 5.3079e+01i	10.9675 – 0.0001i	9.6311 – 0.0001i	10.4808 + 0.0003i	0.0172 – 0.0000i
hallow.jpg	8.1260e+05 + 1.1531e+01i	6.6110e+05 + 1.5521e+01i	7.2290e+05 – 5.9080e+01i	11.8223 – 0.0001i	9.9717 – 0.0001i	10.6621 + 0.0003i	0.0627 – 0.0000i
Noao.png	9.2382e+05 + 1.1531e+01i	8.4579e+05 + 1.5521e+01i	9.48721e+05 – 5.9080e+01i	09.8471 – 0.0001i	10.0184 – 0.0001i	10.2248 + 0.0003i	0.0588 – 0.0000i
Organic.png	7.8997e+05 + 1.1697e+01i	6.5678e+05 + 1.5784e+01i	7.5879e+05 – 5.2247e+01i	10.4875 – 0.0001i	9.5697 – 0.0001i	10.7842 + 0.0003i	0.0426 – 0.0000i
Dancer.jpg	9.6974e+05 + 1.4472e+01i	6.1645e+05 + .1291e+01i	7. 9754e+05 – 5.5474e+01i	11.9697 – 0.0001i	9.8440– 0.0001i	10.9392+ 0.0003i	0.0264 – 0.0000i
Biker.jpg	9. 5093e+05 + 1. 8356e+01i	6.204e+05 + 1. 2492e+01i	7. 7075e+05 – 5. 678e+01i	11. 9817 – 0.0001i	9. 8386– 0.0001i	10. 8619+ 0.0003i	0.0033– 0.0000i
Basket.png	8. 7075e+05 + 1. 9817e+01i	6. 8386e+05 + 1. 4772e+01i	7. 9523e+05 – 5. 0779e+01i	10. 6719 – 0.0001i	9. 5116– 0.0001i	10. 5410 + 0.0003i	0.0704 – 0.0000i
Ground.jpg	8. 6865e+05 + 1. 3459e+01i	6. 3459e+05 + 1. 5415e+01i	7. 2334e+05 – 5. 6279e+01i	10. 4085 – 0.0001i	9. 5319 – 0.0001i	10. 8593 + 0.0003i	0. 0509 – 0.0000i

Table 3. Tabulation for decrypted image

Name	MSE (r)	MSE (g)	MSE (b)	PSNR (r)	PSNR (g)	PSNR (b)	MSSIM
Pears.png	0	0	0	Inf	Inf	Inf	1
Autumn.tif	0	0	0	Inf	Inf	Inf	1
Football.jpg	0	0	0	Inf	Inf	Inf	1
hallow.jpg	0	0	0	Inf	Inf	Inf	1
Noao.png	0	0	0	Inf	Inf	Inf	1
Organic.png	0	0	0	Inf	Inf	Inf	1
Dancer.jpg	0	0	0	Inf	Inf	Inf	1
Biker.jpg	0	0	0	Inf	Inf	Inf	1
Basket.png	0	0	0	Inf	Inf	Inf	1
Ground.jpg	0	0	0	Inf	Inf	Inf	1

6.1 PSNR

It is a quantitative measurement to compare a decrypted image with original image. Correlation between those two images should be same means the better quality of source image is reconstructed. Here we consider 8 bit gray scale image so that peak signal value is 255. So it is formulated to measure the similarity between gray image and its decrypted image. PSNR is always inversely proportional to the MSE. The values of PSNR should be high for retrieving higher quality image as same as original image. MSE should be low for providing effective degraded image with respect to the peak signal value. Similarly for measurement between the original and encrypted image, it should be low to assure the good encrypted image. Less correlation should exist between those images so that it is hard to predict the source image. It is measured in decibels where it converts float values into the integer. PSNR values with 0 dB means better image is encrypted. For example, the image with 10 dB results in good encryption than another image with higher decibel values. The range of PSNR varies for different types of image formats such as lossy and lossless image compression. Both PSNR and MSE metrics which use the intensity difference to measure the image quality that is decrypted image should be retrieved as the original image.

$$PSNR = 10\log_{10}\frac{\text{Maximum}^2}{\text{MSE}}$$

Generally PSNR should be low to assure the best quality of images. The encrypted image should be equal as original image when the PSNR value will be high. When both the images are identical then the PSNR value will reach infinity. Lower the PSNR then there is less correlation between original and cipher Image for good quality image.

6.2 MSE

MSE is mainly used to compute error signal based on the difference between the original image and encrypted image by calculating pixel by pixel difference values and it will be squared and added together which is then divided by the total number of pixels. It is measured for all the pixel values of an entire image for each individual RGB channel. The measurement between two identical images should be low so that the PSNR value will be infinity. The value of MSE taken over an original and degraded image should be zero. It is generally used to evaluate a quality of image. It is mostly depend on the intensity of an image. So it is better noticed for 10 bit image than 8 bit because of pixel values are in the range of 0 to 1023. It results in less error when the MSE value is lower. For the inverse form of PSNR, it transform to a higher value. It also ensures higher signal to noise ratio. Finally lower the MSE and higher the PSNR reveal that better image is reconstructed.

$$MSE = \frac{1}{lb}\sum_{i=0}^{l-1}.\sum_{n=0}^{b-1}(\mathrm{S(I,n)} - \mathrm{E((I,n))})^2$$

6.3 SSIM

The interrelation between source and modified image is assessed using Structure Similarity Index Measure (SSIM). The values of SSIM is more uniform with human recognition. In SSIM method, the retrieved image should match with the human perception. If the image is predicted as bad quality by human eye then it is cope with the result of SSIM. Unlike the MSE method, the blurred image should be analyzed to result as same as quality image. It is exploited to examine the several types of image defects. It is useful for various techniques such as image/video coding, watermarking, image encryption and biomedical image processing. The distortion introduced by encryption is analyzed using image quality metric of SSIM. The variation between distorted and original image is quantified better than the MSE and PSNR. These metric is used to access the change in the pixel intensity, cross correlation and variance between those images.

$$SSIM(w,r) = [l(w,r)]^{\alpha}[c(w,r)]^{\beta}[s(w,r)]^{r}$$

6.4 MSSIM

Mean Structural Similarity Index Measure (MSSIM) is used to calculate the weighted mean of the different images in SSIM. It is employed to assign different weights to various segmented areas of an image. Based on

$$MSSIM(B,T) = (1/p)\sum_{k=1}^{P}(B_k, T_k)$$

uniform weighting it is measured. MSSIM is exploited to measure the quality of an entire image. MSSIM is used for measuring the correlation between two images. The value of MSSIM lies between 1 and –1. When it reaches 1 there exists more similarity between encrypted and original image. When it reaches 0 there is a negligible correlation between the two images.

7. Conclusion

In this paper we introduced an image scrambling based on two techniques. First the image pixels are encoded using gray code also it give the scrambling effect them through the method of fast Fourier transform enhancing the difficulty of decoding. The original image can be reconstructed only by using a correct security key. The results show that image can be protected using two different secure levels. It can be achieved by random permutation which is used to shuffle the pixels of an image. This method of an image encryption achieves better results than other methods. The results of PSNR, MSE and MSSIM show that the better quality of image is retrieved. MSE values for decrypted image results in zero for different type of image formats. Next factor considered is PSNR values which reach infinity so that the decrypted image should be identical as original image. MSSIM also exist with value 1 it reveal that the image is reconstructed as same as source image. Similarly for encrypted image, the values of MSSIM range is 0 so there is less correlation exist between those images. MSE values results above 0 and also the PSNR values lies in between –19 to 0 it expose that image is better. encrypted.

8. References

1. Zhu WT. Towards secure and communication-efficient broadcast encryption systems. Journal of Network and Computer Applications. 2013 Jan; 36(1):178–86.
2. Vijayaraghavan R, Sathya S, Raajan NR. Encryption for an image using circular budge on bit-planes. International Journal of Applied Engineering Research. 2014; 9(2):153–60. ISSN 0973-4562.
3. Jiri F. Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurcat Chaos. 1998; 8(6):1259–84.
4. Fu C, Lin B-B, Miao Y-S, Liu X, Chen J-J. A novel chaos-based bit-level permutation scheme for digital image encryption. Optics Communications. 2011 Nov 1; 284(23):5415–23.
5. Gao T, Chen Z. Image encryption based on a new total shuffling algorithm. Chaos, Solitons and Fractals. 2008 Oct; 38(1):213–20.
6. Fang L, Susilo W, Ge C, Wang J. Public key encryption with keyword search secure against keyword guessing attacks without random oracle. Information Sciences. 2013 July 20; 238:221–41.
7. Oommen BJ, Loke RKS. Pattern recognition of strings with substitutions, insertions, deletions and generalized transpositions. Pattern Recognition. 1997 May; 30(5):789–800.
8. Vajnovszki V, Vernay R. Restricted compositions and permutations: From old to new Gray codes. Information Processing Letters. 2011 Jul 1; 111(13):650–5.
9. Zeger K, Gersho A. Pseudo-Gray coding. IEEE Transactions on Communications. 1990; 38(12):2147–58.
10. Tsai J-S, Huang W-B, Kuo Y-H, Horng M-F. Joint robustness and security enhancement for feature-based image watermarking using invariant feature regions. Signal Processing. 2012 Jun; 92(6):1431–45.
11. Wang X-Y, Yang H-Y, Li Y-W, Yang F-Y. Robust color image retrieval using visual interest point feature of significant bit-planes. Digital Signal Processing. 2013 Jul; 23(4):1136–53.
12. Han J-W, Park C-S, Ryu D-H, Kim E-S. Optical image encryption based on XOR operations. Optical Engineering. 1999; 38(1):47–54.
13. Mallat SG. Theory for multiresolution signal decomposition: the wavelet representation. IEEE Transactions on Pattern Analysis and Machine Intelligence. 1989; 11(7):674–93.
14. Calvin C. Implementation of parallel FFT algorithms on distributed memory machines with a minimum overhead of communication. Parallel Computing. 1996 Nov; 22(9):1255–79.
15. Lian Q-S, Chen S-Z. The translation invariant contourlet-like transform for image denoising. Acta Automatica Sinica. 2009 May; 35(5):505–8.
16. Raaf O, El Hamid Adane A. Pattern recognition filtering and bidimensional FFT-based detection of storms in meteorological radar images. Digital Signal Processing. 2012 Sep; 22(5):734–43.

17. Xie H, Hicks N, Randy Keller G, Huang H, Kreinovich V. An IDL/ENVI implementation of the FFT-based algorithm for automatic image registration. Computers and Geosciences. 2003 Oct; 29(8):1045–55.
18. Hacine-Gharbi A, Deriche M, Ravier P, Harba R, Mohamad T. A new histogram-based estimation technique of entropy and mutual information using mean squared error minimization. Computers and Electrical Engineering. 2013 Apr; 39(3):918–33.
19. Forchhammer S, Li H, Andersen JD. No-reference analysis of decoded MPEG images for PSNR estimation and post-processing. Journal of Visual Communication and Image Representation. 2011 May; 22(4):313–24.
20. Wang J, Zheng N, Liu Y, Zhou G. Parameter analysis of fractal image compression and its applications in image sharpening and smoothing. Signal Processing: Image Communication. 2013 Jul; 28(6):681–7.