ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

Image Encryption using bit-slice rotation method- for an image security

S.Sathya
Assistant Professor
Department of Electronics and Communication Engineering
Bharathiyar Institute of Engineering for Women
Tamilnadu,India
sathyaa43@gmail.com

***Abstract*–Image encryption plays a major role in information security. It is mainly used to convert the original image into another form. In this work, we propose a bit plane slicing of digital image to provide the more security. The main aim of BPS is used to divide the digital image into 8 bit planes. The bit plane is further rotated in order to provide better encrypted image and to make hacking more difficult. It focuses on two techniques such as bit plane slicing and image rotation for efficient image encryption. The classification of bit plane is used for analyzing the importance played by each bit of an image. It is used to estimate the each pixel of an image. The proposed technique involves rotation of bit planes is employed to make highly secure image encryption. By this method scrambling of an imageis based on efficient technique even it is intercepted, the information cannot be understood. It is mainly useful for image compression because it exhibits high coding efficiency. This method which makes the decryption of an image more difficult compared to other techniques.**

Index Terms – Image Encryption, Bit Plane Slicing, Rotation, Scrambling.

I. INTRODUCTION

Cryptography is an efficient method of transferring information in a secure way. It scrambles the image before transmitting in order to change the structure of an image. Even the attacker cannot able to hack because it is difficult for him to retrieve the original image. It only provides the modified form of an image but it does not hide the image even though it is better secure method. The main intention is to provide better protection of the original image. Bit plane slicing is mainly used for splitting images into binary planes. Each bit is used to represent the intensity of each pixel of an image. Image scrambling is always based on pixel values of an image. The digital image is divided into 8 bit planes because it is useful for analyzing the importance of each bit in an image. Whereas a small change in color affect bit value of an image. The color image is composed of many pixels is decomposed into 8 bit planes. It is used to represent the highest order and lower order bits to specify the contribution of each bit in an image. It achieves better image encryption than the other least significant bit, perceptual masking technique. This process is done on without changing the overall image quality.

II. METHODS

Consider a color image which is composed of a number of pixels. Each pixel is represented in terms of bits. The image consists of 8 bit planes from plane 1 to plane 8. Plane 8 contains all lowest order bits and plane 1 constitutes all higher order bits in an image.

The slices of the 8 planes contain the information of an image. While we modify the positions, values and more it will result in a scrambled output.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

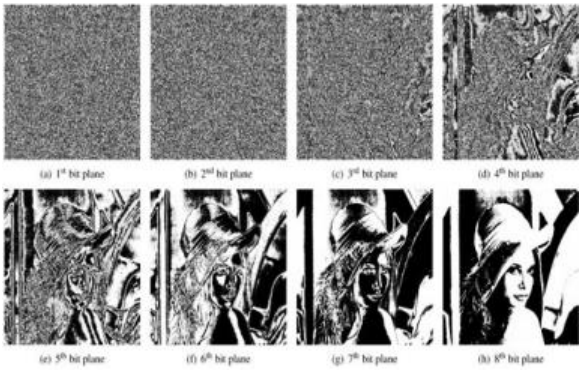

Fig. 1. Information in 8bit planes

Consider 3x3 matrix

160	162	164
166	168	170
172	174	176

The binary values for above pixel value are shown in 8 bit representation

10100000	10100010	10100100
10100110	10101000	10101010
10101010	10101110	10110000

Bit plane is used to exhibit the significant information of an image. It is composed of 8 bit planes In above example LSB bits of a binary form constitute lowest order bits and MSB bits represent high order bits of all the pixels in an image. The concept of bit plane slicing is to determine whether the image contains noise or significant information in terms of bit plane. When the replacement of MSB bit is done it causes more distortion than LSB bits. It is easy to encode less significant bits and it is essential to preserve the most significant bits [4].

A.*Bit Plane Slicing*

Bit plane slicing is used to slice the image into different bit planes. It is composed into higher order and lower order bits. MSB [5] has the significant addition to the total image it contributes the majority of the information of an image. LSB contributes only less details of an image. It plays a major role in image processing and compression [4] [6]. The major influence of this method is used to furnish the essential of each bit of an image [7].It also ensures the beneficence of specific pieces. Bit plane is mainly possessed of many layers where each layer exhibitsthe specific range of bit planes in an image. Level of security also depends on the number of bit planes used to decompose the image. Loss of higher order bit planes leads to much darker image therefore MSB is most essential in bit plane slicing. Encrypting the less significant bit will result in degrading the image quality slightly than encrypting in the most significant bit its cause more degradation [3]. Encryption is done for each three individual color planes according to a bit plane slicing method.

B.*Bit Rotation*

The simple method to provide image encryption is a rotation of bit planes. It is more effective than the other method as bit shifting. After the image is decomposed into the bit plane and then applied the rotation on each of the bit planes in different angles [1]. Rotation of bit planes is rearranged to provide the original bit plane of an image at the receiver end. The rotation of a bit plane is processed at different angles such as 90,180,270 in order to make image encryption to be more difficult. It is difficult for an attacker to retrieve the image without knowing what type of technique is employed [2]. This includes the rotated form of a bit planes in order to make the transformed shape of an image.The important information of an image is extracted using bit plane slicing [9].

Bit rotation is applied after bit plane slicing according to a various angle in 8 bit planes. Each pixel of planes is rotated by the different angle in order to provide an encrypted image [8] [10]. A rotation of planes does not lose any bits. This technique is obtained by rotation of bits in high dimensional space. Finally all the rotated bit planes are combined to generate an original bit plane. By using this method the original image can be retrieved without any loss of information [11]. Christo Ananth et al. [12] proposed a system in which the cross-diamond search algorithm employs two diamond search patterns (a large and small) and a halfway-stop technique. It finds small motion vectors with fewer search points than the DS algorithm while maintaining similar or even better search quality. The efficient Three Step Search (E3SS) algorithm requires less computation and performs better in terms of PSNR. Modified objected block-base vector search algorithm (MOBS) fully utilizes the correlations existing in motion vectors to reduce the computations. Fast Objected - Base Efficient (FOBE) Three Step Search algorithm combines E3SS and MOBS. By combining these two existing algorithms CDS and MOBS, a new algorithm is proposed with reduced computational complexity without degradation in quality.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

This work describes about the image encryption that uses both the rotation of bits combined with various degrees of rotations used as a secret key that operates on an image [13]. This encryption is getting by providing a rotation angle for the 8 bit planes. Repeating these steps for every bit planes it gives an encrypted image. The result reveals that this encryption achieves better security than the other approaches.

III. IMPLEMENTATION

In this work we proposed a method for encryption and decryption based on bit plane slicing in which image is divided into bit planes. It is rotated at different angles to form the encrypted image. This enhances the robustness of the encryption of an image. The original image is retrieved by again using bit plane slicing and a rotation of bits. Combining bit plane slicing and rotation added as a layer of security to protect an image. The retrieved image will have exactly the same pixel value as the original image. By this method encrypted image is unrecognizable and scrambling is done. Increasing the different technique will result in more secure encryption method.

Consider a 2x2 image

160	172
184	196

The above pixels of an image is represented in binary form

10100000	10101100
10111000	11000100

It is divided into individual bit plane using the slicing method in order to provide better encryption. Each bit plane represents the significant information of an image

1st bit plane

1	1
1	1

2nd bit plane

0	0
0	1

3rd bit plane

1	1
1	0

4th bit plane

0	0
1	0

5th bit plane

0	1
1	0

6th bit plane

0	1
0	1

7th bit plane

0	0
0	0

8th bit plane

0	0
0	0

The above bit plane is further rotated at different angles to make more difficult to decrypt

1st bit plane [Rotated by 90^0]

1	1
1	1

2nd bit plane [Rotated by 180^0]

1	0
0	0

3rd bit plane [Rotated by 270^0]

1	1
0	1

4th bit plane [Rotated by 90^0]

0	0
0	1

5th bit plane [Rotated by 180^0]

0	1
1	0

6th bit plane [rotated by 270^0]

0	0
1	1

7th bit plane [Rotated by 90^0]

0	0
0	0

8th bit plane [rotated by 180^0]

0	0
0	0

After a bit rotation a new pixel value is obtained that is encrypted image is exploited. The encrypted image is created by combining each bit from eight pixels of an image. It is further represented in decimal form of an image.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

11100000	10101100
10100000	10011100

Encrypted 2x2 image

224	172
160	156

The decryption process is done as the reverse process of the above encryption method. The encrypted image is decrypted using the same method as above

224	172
160	156

Pixels of an image are represented in binary form as follows

11100000	10101100
10100000	10011100

The above cipher image is decrypted by splitting eight bits into individual bit planes in the form of 2x2 matrix.

1st bit plane [Rotate it by 270^0]

1	1
1	1

2nd bit plane [Rotate it by 180^0]

1	0
0	0

3rd bit plane [Rotate it by 90^0]

1	1
0	1

4th bit plane [Rotate it by 270^0]

0	0
0	1

5th bit plane [Rotate it by 180^0]

0	1
1	0

6th bit plane [rotate it by 90^0]

0	0
1	1

7th bit plane [Rotate it by 270^0]

0	0
0	0

8th bit plane [Rotate it by 90^0]

0	0
0	0

The process is done by taking each first bit from the every 8 bit planes which form 2x2 matrixes it is repeated for the entire second to eight bits it is formed into 8 bit planes by combining every first bit of all 2x2 matrixes and second bit, the third bitrepeatedly up to the eighth bit from all matrices. It is exploited in binary form

10100000	10101100
10111000	11000100

The decimal form of an above image is obtained by doing bit plane slicing and bit rotation. The original image is finally decrypted using different methods.

160	172

184 196

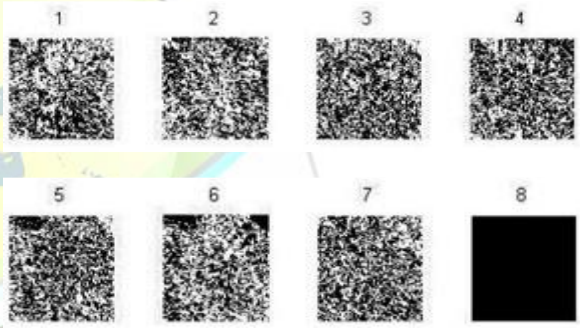

Fig. 2. Bit slices of an original image

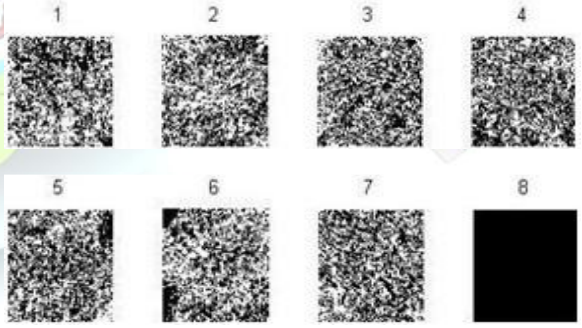

Fig. 3. Images of rotated bit slices

IV. RESULTS

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

Fig.4. Secret

Fig.5. Encrypted

Fig.6. Decrypted

TABLE I. TABULATION FOR ENCRYPTED IMAGE

Name	MSE (r)	MSE (g)	MSE (b)
Pears.png	5.2382e+06 + 8.4969e+02i	5.2659e+06 + 1.2823e+03i	1.5662e+06 + 4.1499e+02i
Autumn.tif	7.5718e+05 + 8.5799e+02i	6.7439e+05 + 5.5547e+02i	6.8233e+05 + 2.5352e+03i
Football.jpg	8.1891e+05 + 1.0678e+01i	6.0200e+05 + 1.3924e+01i	7.3208e+05 - 5.3079e+01i

Name	PSNR (r)	PSNR (g)	PSNR (b)	MSSIM
Pears.png	19.0270 - 0.0007i	19.0499 - 0.0011i	13.7837 - 0.0012i	0.0154 - 0.0000i
Autumn.tif	10.6272 - 0.0049i	10.1243 - 0.0036i	10.1752 - 0.0161i	0.0140 - 0.0000i
Football.jpg	10.9675 - 0.0001i	9.6311 - 0.0001i	10.4808 + 0.0003i	0.0172- 0.0000i

TABLE II.TABULATION FOR DECRYPTED IMAGE

Name	MSE (r)	MSE (g)	MSE (b)
Pears.png	0	0	0
Autumn.tif	0	0	0
Football.jpg	0.0015	4.5980e-04	7.5277e-04

Name	MSE (b)	PSNR (r)	PSNR (g)	PSNR (b)
Pears.png	0	Inf	Inf	Inf
Autumn.tif	0	Inf	Inf	Inf
Football.jpg	7.5277e-04	76.5069	81.5391	79.3982

V. CONCLUSION

In this work, bit plane slicing and rotation of the bits is combined into one secure algorithm. This method may not be more secure but it is difficult to decrypt. To achieve this goal we design a scrambling method using bit plane rotation with the help of bit plane slicing. The performance of this method is measured by using MSE and PSNR values. The decryption of an image is robust because it does not lose any data. Bit plane slicing preserves the significant information of degraded image. Image encryption based on bit plane slicing and rotation can improve significantly the level of security. The results show that it provides a better level of encryption without affecting the overall image quality. Thus the mode such as bit rotation used for efficient encryption requirements it is applicablefor any type of image formats. The experimental results show that the proposed scheme leads to an improved security level and its proved in terms of MSE, PSNR and MSSIM parameters.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

References

[1] D. Schneier, Applied Cryptography, John Wiley & Son, Inc., New York, NY, 1996.

[2] Gonzalez, R.C., R.E. Woods, S.L. Eddins, Digital Image Processing, Second Edition, Prentice Hall, 2007.

[3] V. Namias,The fractional order Fourier transform and its application in quantum mechanics,Journal of the Institute of Mathematics and its Applications 25(1980)241–265.

[4] Y.Wang,K.-W.Wong,X.Liao,G.Chen, A new chaos-based fast image encryption algorithm,Applied Soft Computing 11 (January (1)) (2011)514–522.

[5] J.B. Lima, R.M. Campello de Souza, The fractional Fourier transform over finite fields, Signal Processing 92 (February (2)) (2012)465–476.

[6] Fridrich Jiri. Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurcat Chaos 1998;8(6):1259–84.

[7] Chen Guanrong, Mao Yaobin, Chui Charles K. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos SolitonFract 2004;21(3):749–61.

[8] GaoTiegang, Chen Zengqiang. A new image encryption algorithm based on hyper-chaos. Phys Lett A 2008;372(4):394–400.

[9] Zhang Wei, Wong Kwok-wo, Hai Yu, Zhu Zhi-liang. An image encryption scheme using lightweight bit-level confusion and cascade cross circular diffusion. Optics Commun 2012;285(9):2343–54.

[10] Wang Yong, Wong Kwok-wo, Liao Xiaofeng, Chen Guanrong.A new chaos-based fast image encryption algorithm.Appl Soft Comput 2011;11(1):514–22.

[11] Li Chengqing, Li Shujun, Alvarenz Gonzalo, Chen Guanrong, Lo Kwok-Tung. Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations. Phys Lett A 2007;369(1–2):23–30.

[12] Christo Ananth, A.Sujitha Nandhini, A.Subha Shree, S.V.Ramyaa, J.Princess, "Fobe Algorithm for Video Processing", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE), Vol. 3, Issue 3,March 2014 , pp 7569-7574

[13] Zhenjun Tang and Xianquan Zhang, Secure Image Encryption without Size Limitation Using Arnold Transform and Random Strategies, Journal of Multimedia, VOL. 6, NO. 2, APRIL 2011, 202-206.