International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Modified Playfair Cipher for Encrypting Images

Faisal Mohammed Abdalla[1], Khadiga Mohammed Adam Babiker[2]
[1]Collage of computer science and information technology, Karary University, Omdurman, Sudan
[2]collage of graduate studies, Sudan University of science and technology / Khartoum , Sudan

ABSTRACT

In this paper, a new extension of the Playfair cipher algorithm to encrypt images safer manner. The new method is created matrix of 16 × 16 based on the key being entered by the user to become more secretive, and then is taken image data byte by byte. In addition, the increasing complexity of the algorithm using masking and an XOR. That is, the key is used to generate XORed with the image to encrypt it. The experimental results showed that the use of slightly different secret keys, and the resulting encoded images makes it a completely different picture, and also encrypts the data that contain alphanumeric characters, integers, and most symbols

Keywords: Playfair , Matrix, XOR operation

I. INTRODUCTION

As the general public became more aware of cryptographic uses, the personal and social need for privacy is increased. The Playfair cipher is one of the ways to protect information is the method of encryption and decryption whereby the sender encrypts the message with a secret key which is known only to the receiver. Once the receiver gets the message the message is decrypted using the same secret key.

The Playfair cipher uses a 5 by 5 table containing a key word or phrase. Memorization of the keyword and 4 simple rules was all that was required to create the 5 by 5 table and use the cipher. The existing playfair technique is based on the use of a 5X5 matrix of letters constructed using a keyword. This algorithm can only allow the text that contains alphabets only. But many algorithms have been proposed that allow text which contains alphabets, integers as well as special symbols using 6 * 6 matrixes and 10 * 9 matrixes etc.

suggested using a 6 x 6 matrix instead of 5 x 5. The matrix is constructed in a similar way to the classic technique except that beside the set of alphabets this matrix is large enough to accommodate numerical digits (0 to 9) as well. Furthermore, the I/J was not counted as one l letter. Instead, Kamal et al.in [2].placed I and J in two separate cells in order to avoid ambiguity at decryption time.

2.2 Currently, a new extension of classical Playfair cipher was presented by Hamad et al. in [3]. The proposed ciphering technique provides 8 × 8 amino acid codons substitution matrix. Furthermore, an interweaving step was added for more secured results.

Playfair Cipher

Playfair cipher algorithm is based on with use of 5 X 5 matrix of letters constructed using a keyword. The 5 X 5 matrix can only allow 25 characters, hence the letters I/J count as one. If we encrypt the plaintext which is having the

CSEIT1833311 | Received : 20 March 2018 | Accepted : 31 March 2018 | March-April-2018 [(3) 3 : 1063-1068]

All above versions can't encrypt Digital Images, because it does not include all the values of colors.

II.II.Related Works:

2.1 Ravindra et al in [1].proposed an extension to the traditional Playfair algorithm . Their approach

TABLE 1: PLAYFAIR 5×5 MATRIX

s	i/j	m	p	l
e	a	b	c	d
f	g	h	k	n
o	q	r	t	u
v	w	x	y	z

Table (1) show Playfair matrix with key =simple

III.Proposed Method

4.1 Encryption algorithm: image encryption

input : Plain image and Secret key

output: Cipher image

1. Read the plain image as RED, GREEN and BLUE matrices.
2. If the plain image has an odd-number dimension append a row or column of zeros to the end to make it even.
3. Construct a Key Square: 16 x16 matrix of random integer numbers between 0 and 255 using the secret key.
4. For each pair of colors components in the RED plane of the plain- image do the following:
   (a) If the values are in different rows and columns, replace the pair with the values at the opposite corners of the rectangle defined by the original pair and maintain their order.
   (b) If the values appear on the same row of the matrix, replace them with the values to their immediate right respectively (wrapping around

letter I/J and when we decrypt the ciphertext at the receive end, the receiver will be under ambiguity whether to consider I or J in his text, because the meaning can be changed with the change of the letters. This algorithm can only useful for the plain text containing of alphabets but it is failed for the plain text containing of alphanumeric values.

4.2. Decryption algorithm: image decryption

input : Cipher image and Secret key

output: Plain image

1. Read the Cipher image as RED, GREEN and BLUE matrices.
2. Use the secret Key to generate a mask made up with a random permutation of the numbers between 0 and 255.
3. XOR the RED color plane of the Cipher image with the generated random mask.
4. Construct a Key Square: 16 ×16 matrix of random integer numbers between 0 and 255 using the secret key.
5. For each pair of the resultant XORed RED plane of the Cipher image do the following:
   (a) If the values are in different rows and columns, replace the pair with the values at the opposite corners of the rectangle defined by the original pair and maintain their order.
   (b) If the values appear on the same row of the matrix, replace them with the values to their immediate right respectively (wrapping around to the left side).
   (c) If the values appear on the same column of the matrix, replace them with the values immediately below respectively (wrapping around to the top side of the column).
6. Repeat step 3 to 5 for GREEN and BLUE

CSEIT1833311 | Received : 20 March 2018 | Accepted : 31 March 2018 | March-April-2018 [(3) 3 : 1063-1068]

to the left side).

(c) If the values appear on the same column of the matrix, replace them with the values immediately below respectively (wrapping around to the top side of the column).

5. Use the secret Key to generate a mask made up with a random permutation of the numbers between 0 and 255.
6. XOR the resultant scrambled image with the generated random mask.
7. Repeat step 4 to 6 for GREEN and BLUE color planes of the plain image.
8. Return the resultant image as the cipher-image.

color planes of the cipher image.

7. Return the resultant image as the Plain-image.

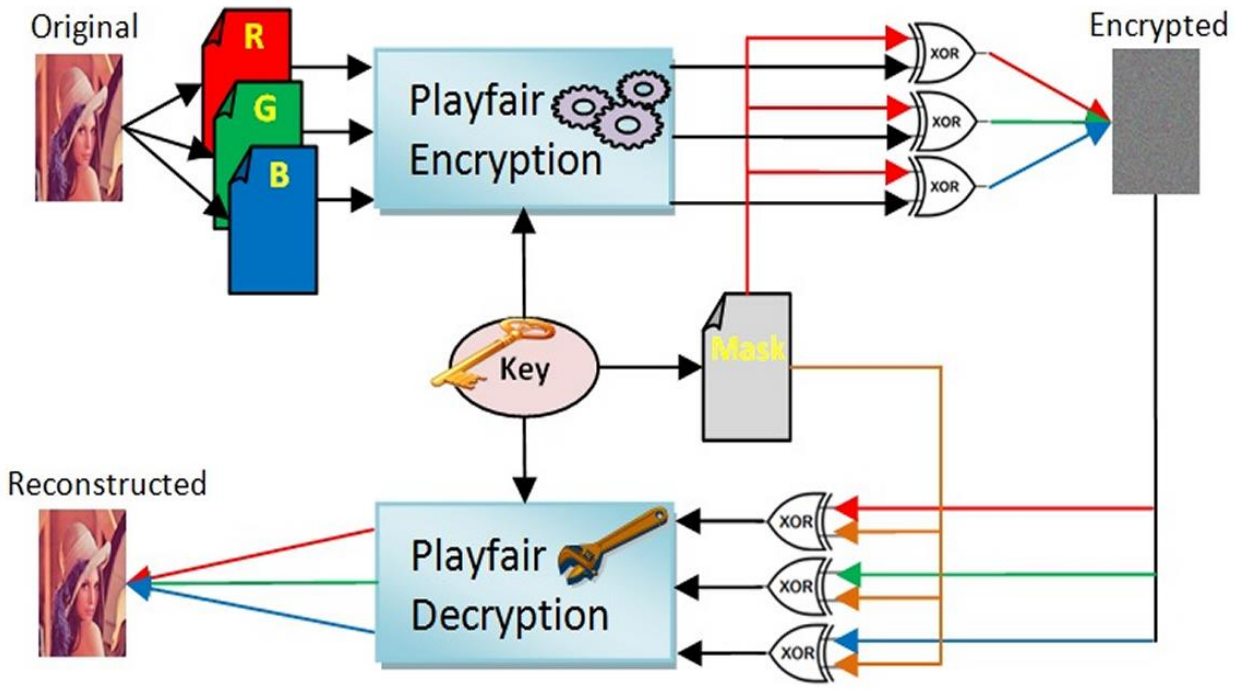


Figure 1: Show steps of encryption and decryption operations

CSEIT1833311 | Received : 20 March 2018 | Accepted : 31 March 2018 | March-April-2018 [(3) 3 : 1063-1068]

V.Implementation

The new method was implemented using java and MATLAB for analysis. Three standards RGB colors images were used for benchmark comparisons in different sizes.

Table [4:1] shows the result of new encryption method using one secret key on the images. Obviously the results showed the Decipher Image and original image is same.

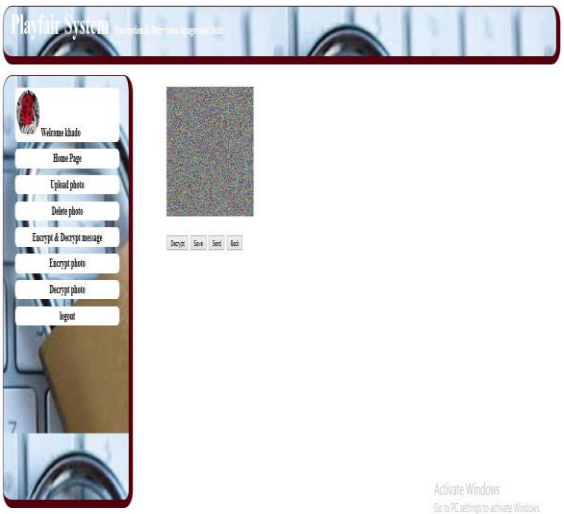


Figure 3: Show encrypted image:

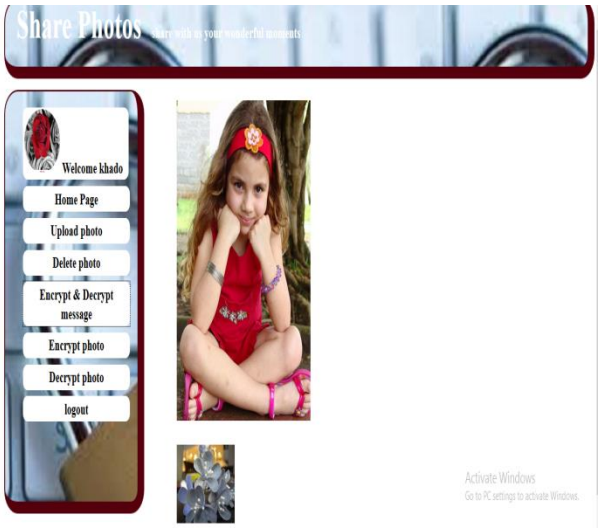
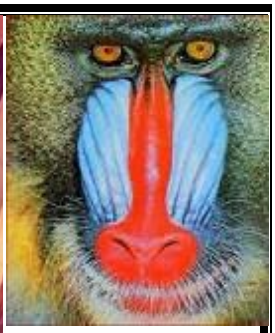


Figure 2: Show how Home page after loin user (khado) in the System.

Original Image				

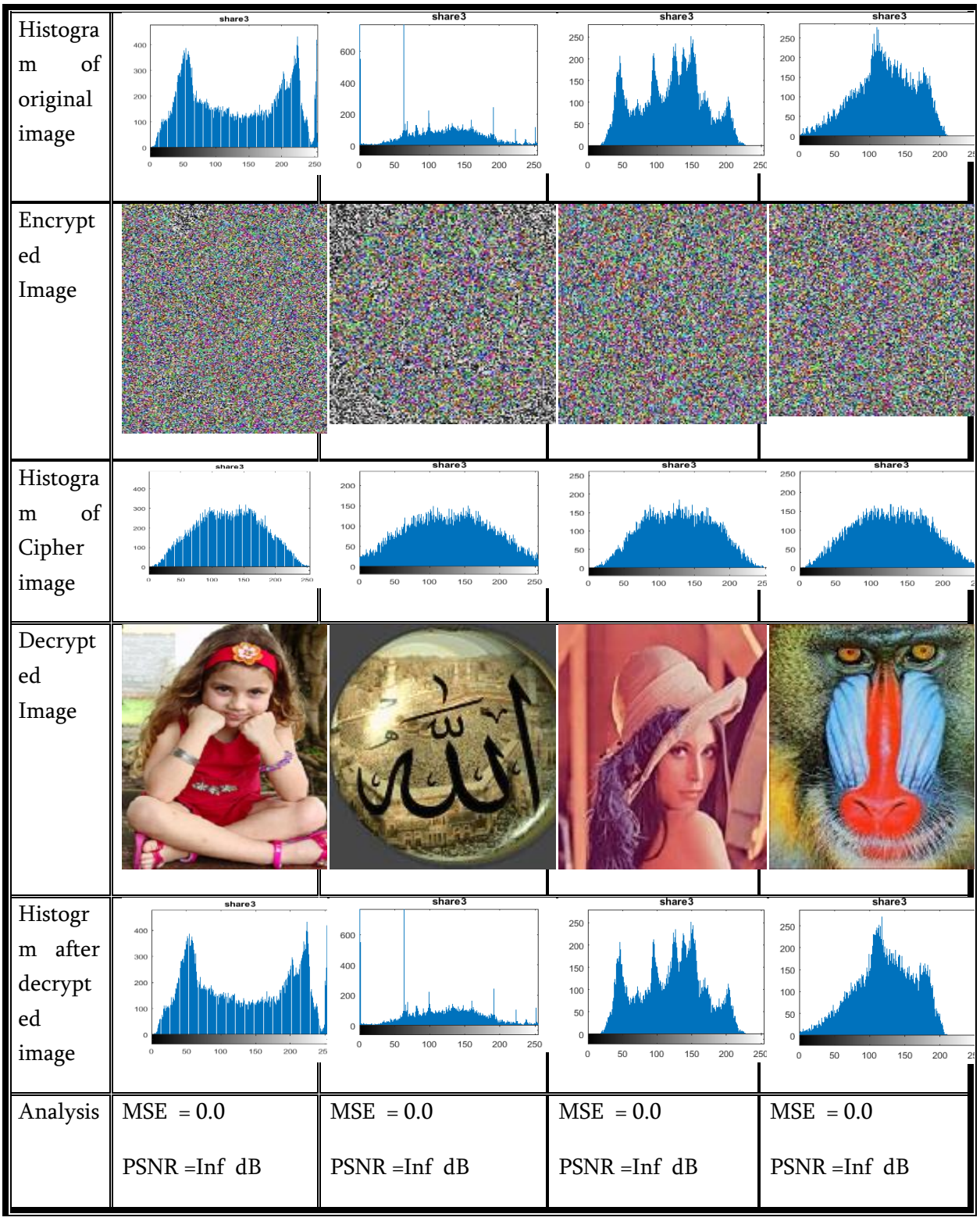


Figure 4 : The result of Modified Playfair Cipher for Encryption, Decryption images and (PSNR& MSE) Values for Standard Images and Cipher Images using same key.

CSEIT1833311 | Received : 20 March 2018 | Accepted : 31 March 2018 | March-April-2018 [(3) 3 : 1063-1068]

IV. CONCLUSION

The classic Playfair Cipher can only be useful for a plain-text consisting of alphabets. However, a number of recently proposed extensions succeeded to encrypt alphanumeric data using different approaches.

In this research a new method for encrypting images using playfair algorithm is introduced. So, instead of the classical 5 × 5 matrix, the new method constructs 16 × 16 key matrix for a better alignment with image pixel data. In addition, an XOR procedure has been adopted for a more secure and yet scrambled results.

The experimental results showed that the key space of the new technique makes it hard for the attacker to perform a frequency analysis based on the used pixel digraphs.

Analysis demonstrated that little change in the secret key leads to a very big change in the image. Obviously the results the randomness of the resultant ciphered images,

PSNR values and histogram comparisons were also deployed to show the robustness of the new cipher.

V. REFERENCES

[1]. Enhancing the Security of Playfair Square Cipher by Double Substitution and Transpositiontechniques Jawad Ahmad Dar1 , AmitVerma

[2]. A Modified Version of Playfair Cipher Using 7x4 Matrix. August 2013. Alam, A. Aftab; Khalid, B. Shah; Salam, C. Muhammad

[3]. Enhanced the Security of Playfair Technique using Excess 3 Code (XS3) and Ceasar Cipher. October 2014. ZubairIqbalBhumika Gupta Kamal Kr. GolaPrachi Gupta

[4]. S. Hamad, A Novel Implementation of an Extended 8x8 Playfair Cipher Using Interweaving on DNA-encoded Data, (IJECE) 4(1) (2014).

[5]. A Novel Approach to Security using Extended Playfair Cipher, Shiv Shakti Srivastava, Nitin Gupta, International Journal of Computer Applications (0975 – 8887) Volume 20– No.6, April 2011.

[6]. William Stallings, "Cryptography and Network Security: Principles and Practice", 4th Edition, Prentice Hall,2006.

[7]. Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth) (Publisher: John Wiley & Sons, Inc.)Author(s): Bruce Schneier ISBN: 0471128457 Publication Date: 01/01/96

[8]. Enhanced the Security of Playfair Technique using Excess 3 Code (XS3) and Caesar Cipher .Ravindra Babu K, S.Uday Kumar, A. Vinay Babu,I.V.N.S. Aditya, P.Komuraiah, "An Extension toTraditional Playfair Cryptographic Method".International Journal of Computer Applications (0975 –8887), Volume 17- No.5, March 2011.

[9]. Ramaraju PV, Nagaraju G, Chaitanya RK. Image Encryption and Decryption using Advanced Encryption Algorithm. Discovery, 2015, 29(107), 22-28

[10]. A Modified Version Of Extended Plafair Cipher (8x8).

CSEIT1833311 | Received : 20 March 2018 | Accepted : 31 March 2018 | March-April-2018 [(3) 3 : 1063-1068]