

Encryption Image Using Small Order Linear Systems and Repeated Modular Numbers

Adil Al-Rammahi

Abstract— Digital images became very important in our digital life. So, the operations of rearrangement image are very obligated for protection, compression, saving, gaming, and testing of image. In this paper, a new approach of digital image encryption is proposed based on the solution of low order linear systems and modular numbers technique. For each row of given digital image matrix, a linear system was built from two successive elements where the principle diagonal elements are imposed for value one, and the other represents the image values. The system matrix (a) was multiplied by public key (x) to deduce linear system $ax = b$, where b is a cipher of the two given image values. For more complexity against attacker, and for more integrity with decoder, a repeated modular numbers are implemented in order to transform three encryption images.

Index Terms— Linear Systems, image processing, cipher theory.

I. INTRODUCTION

NOW days our life has become digital. Indeed information security has become a central issue in data storage and transmission. Images are widely used on the Internet. Therefore, the protection of image data from unauthorized access is important and necessary. So researchers work hard in Cryptography of images. For examples Cao used hybrid chaotic map in application of image encryption and hiding [1]. Samson and Sastry proposed Cryptographic of Image Using Modern Advanced Hill Cipher [2]. Ogras and Turk introduced digital image encryption scheme using chaotic sequences with a nonlinear fixed functions [3]. Lang studied the method of multiple-parameter weighted fractional Fourier transform and its application to image encryption [4]. Mitra et al introduced a new image encryption approach using combinational permutation techniques [5]. In this investigation we have introduced a procedure for the encryption of an image by applying small order linear system and modular numbers analysis. A two by two linear system is imposed for two sequential values of image matrix. Then a rearrangement of production matrix is calculated via modular numbers. For non loss of image values property, a repeated modular technique was implemented. Finally three decrypted images are written, that gives more complexity against attacker. The results of testing images are promised for goodness. Dang

et al used Discrete Wavelet Transform for encrypted images [6]. Younes and Jantan introduced the concept of the block-based transformation encrypted image algorithm [7]. Mao et al used a new scheme of chaotic Baker maps image encryption [8]. Wu et al studied and used the concept of Sadouka matrix in encrypted image [9]. Jayant and Roy proposed the method of break correlation among neighboring pixels [10]. Alghamdi and Hanif Ullah used chaotic function for iris encryption image [11]. Jolfaei and Mirghadri Surveyed and studied the Salsa20 scheme for image encryption [12]. Ye and Zhou proposed the concept of chaos-based image encryption scheme [13]. Dey introduced mixed and Vernam permutation algorithm [14]. Landge et al proposed the method of 64-bits blowfish [15]. Al-Husainy proposed algorithm which mixed boolean operations and image hiding [16]. Shreef and Hoomod used the interpolating functions technique to encrypt image [17]. Ye proposed an algorithm based on chaos and diffusion mechanism with permutation [18]. Al-Rammahi et al introduced an encrypted algorithm based on the analysis of singular value decomposition [19]. Lin and fuh introduced Barcode Image Decoding in two dimensions [20].

II. NEW MAIN RESULTS

Really there is no complexity or difficulty in encryption algorithms of the type of textual data. In other words encrypted algorithms of text may not be suitable for multimedia data such as images. Decimal numbers which appeared in transformed functions such as matrices are not consisting with the integer numeral image matrix type. This adds a difficult for using linear transformation functions in encryption image. So, the encrypted matrix image through this function must be deal in accuracy and in sensitivity before any transformation. In this paper a concept of linear transformation function is used for encryption the digital image. When a matrix function operates on integer variable, the output values become out of allowable interval (0,255). So, the result does not consist with the properties of image values. And then, big errors calculated in decryption stage through inverse function. For exceeding these difficulties, output value must be analyzed with respect to each digit. Here three matrices were constructed using modulo numbers technique. That adds many complexities against attacker and gives more integrity toward decoder. The proposed method is tested on different image files and the results were far more than satisfactory. For more accuracy, a repeated modular numbers is used.

In this section we introduce our proposed algorithm for encryption digital images as follows:

Manuscript received Jan 2, 2014; revised Mar 23, 2014. This work was supported in part by the faculty of mathematics and computer science, Kufa University, Iraq.

Adil AL-Rammahi, Kufa University, Faculty of Mathematics and Computer Science, Department of Mathematics, Njaf, IRQ (phone:+964(0)33219195; P.O. Box 21 Kufa, e-mail: adil.m.hasan@uokufa.edu.iq).

Algorithm 1

Encryption

- 1) Input image a .
- 2) Input secret keys vector x , and integer number m .
- 3) Compute $c = \begin{bmatrix} 1 & a_1 \\ a_2 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$.
- 4) Analyze $c = m.n + r$.
- 5) Analyze $n = m.n_1 + r_1$.
- 6) Write encrypted images r, r_1 , and n_1 .

Decryption

- 1) Input encrypted images r, r_1 , and n_1 .
- 2) Input secret keys vector x , and integer number m .
- 3) Compute $n = m.n_1 + r_1$.
- 4) Compute $c = m.n + r$.
- 5) Compute $b = c^{-1}x$.
- 6) Write decrypted images b .

III. TEST EXAMPLES

This section was concern for testing the efficiency of proposed algorithm. The details are appearing in Table 1 where the symbols r, r_1, n_1 , and b represents the remainder, repeated remainder, repeated frequency, and decrypted image respectively. Also a histogram of each of original image and corresponding encrypted image is worked in Table 2.

IV. CONCLUSION

Form the testing of our algorithm which appearing in Table 1 we have a three encrypted images for each original image. Firstly we have obtained a plain image of an RGB color. Then this analysis by taking two sequential gray level numbers by constructing 2by2 linear system. Finally repeated modular numbers technique is used for production three matrices. Here it is interesting to note that the encrypted image do not has any resemblance with their corresponding original images. This fact ensures security of images in an effective manner. The histogram of each of original image and its decrypted image referee the goodness of this algorithm. The results of these histograms appear in Table 2 where h_a and h_b represent the histogram of original image and decrypted image respectively. The results appearing in Tables 1 and 2 are promised to develop.

ACKNOWLEDGEMENT

I acknowledge support of the faculty of mathematics and computer science, Kura University, Iraq. Thanks all reviewers for valuable reading.



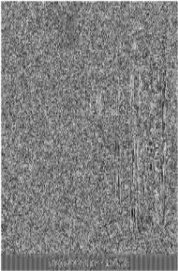

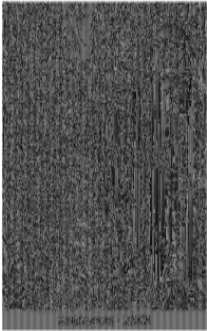
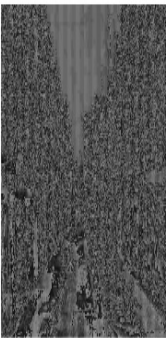




REFERENCES

- [1] Y. Cao, "A New Hybrid Chaotic Map and Its Application on Image Encryption and Hiding", Hindawi Publishing Corporation, Mathematical Problems in Engineering, Volume 2013, pp.1-13.
- [2] C. Samson And Dr. V. Sastry, " Cryptography Of A Gray Level Image And A Color Image Using Modern Advanced Hill Cipher Including A Pair Of Involuntary Matrices As Multiplicands And



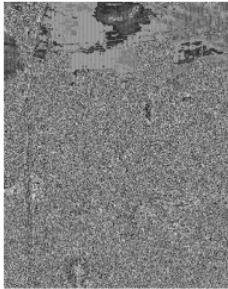
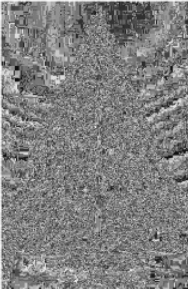

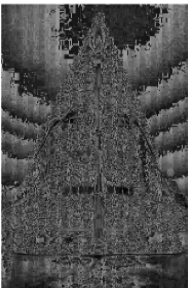




Involving A Set Of Functions", International Journal of Engineering Science and Technology, Vol. 4 No.07 July 2012, pp. 3611- 3619.



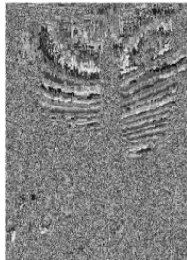
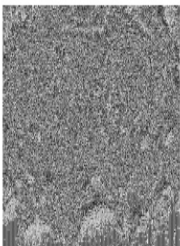
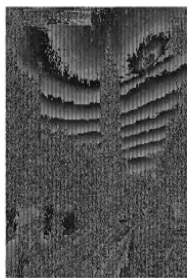
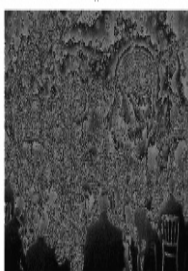




- [3] H. Ogras, M. Turk, " Digital Image Encryption Scheme using Chaotic Sequences with a Nonlinear Function", World Academy of Science, Engineering and Technology, Vol:67 2012-07-21.
- [4] J. LANG, "The Multiple-parameter Weighted Fractional Fourier Transform and its Application to Image Encryption", 4th International Congress on Image and Signal Processing, IEEE, 2011, pp.1779-1783.
- [5] M. Mitra, Y. Rao and S. Prasanna, " A New Image Encryption Approach using Combinational Permutation Techniques", World Academy of Science, Engineering and Technology, Vol:14 2008-02-27.
- [6] P. P. Dang, and P. M. Chau, Image encryption for secure Internet multimedia applications, Consumer Electronics, IEEE Transactions on Image Processing, 46(3), 2000, 395-403.
- [7] M. A. B. Younes and A. Jantan, Image Encryption Using Block-Based Transformation Algorithm ', IAENG International Journal of Computer Science, 2003, 35:1.
- [8] Y. Mao, G. Chen, S. LIAN, A Novel Fast Image Encryption Scheme Based On 3d Chaotic Baker Maps, International Journal of Bifurcation and Chaos, Vol. 14, No. 10, 2004, pp.3613-3624.
- [9] Y. Wu, ,Y. Zhou, J. P. Noonan, K. Panetta, S. Agaian, Image Encryption using the Sudoku Matrix, Mobile Multimedia/Image Processing, Security, and Applications, 2010, pp.1-12.
- [10] J. Kushwaha and B. N. Roy, Secure Image Data by Double encryption, International Journal of Computer Applications, 5(10), 2010, pp.28-32.
- [11] A. S. Alghamdi and Hanif Ullah, A Secure Iris Image Encryption Technique Using Bio-Chaotic Algorithm, International Journal of Computer and Network Security, 2(4), 2010, pp.78-84.
- [12] A. Jolfaei and A. Mirghadri, Survey: Image Encryption Using Salsa20, International Journal of Computer Science Issues, 7(5), 2010, pp.213-220.
- [13] R. Ye, W.Zhou, An Image Encryption Scheme Based on 2D Tent Map and Coupled Map Lattice, International Journal of Information and Communication Technology Research, 1(8),2011, pp. 344-348.
- [14] S. Dey, An Image Encryption Method: SD-Advanced Image Encryption Standard: SD-AIES, International Journal of Cyber-Security and Digital Forensics, 1(2), 2012, pp.82-88.
- [15] I. Landge, B. Contractor, A. Patel, and R. Choudhary, Image encryption and decryption using blowfish algorithm, World Journal of Science and Technology, 2(3), 2012, pp.151-156.
- [16] M. A. F. Al-Husainy, A Novel Encryption Method for Image Security, International Journal of Security and Its Applications, 6(1), 2012, pp.1-8.
- [17] M.A. Shreef and H. K. Hoomod, Image Encryption Using Lagrange-Least Squares Interpolation, International Journal of Advanced Computer Science and Information Technology, 2(4), 2013, pp.35-55.
- [18] R. Ye, A Highly Secure Image Encryption Scheme using Compound Chaotic Maps, Journal of Emerging Trends in Computing and Information Sciences, 4(6), 2013, pp.532-544.
- [19] A. Al-Rammahi, N. Alebadi, M. Alkufi, "Image Encryption Used Singular Values Decomposition", To Be Published in Journal of Computer Science, 2014.
- [20] J. A. Lin And C. S. Fuh, "2d Barcode Image Decoding", Hindawi Publishing Corporation, Mathematical Problems In Engineering, Volume1, pp.1-10, 2013.



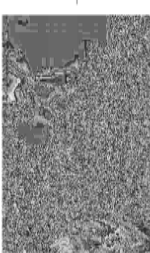
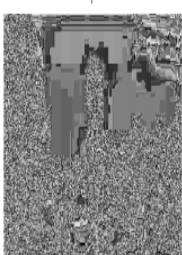
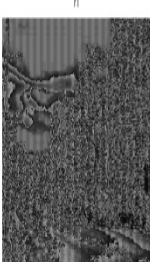





TABLE 1 TEST EXAMPLES

| | 1 | 2 |
|-------|---|---|
| g |  |  |
| r |  |  |
| r_1 |  |  |
| n_1 |  |  |
| b |  |  |



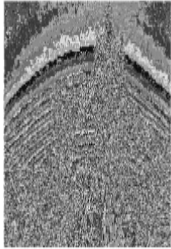

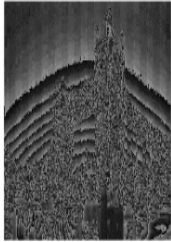
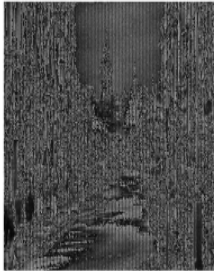




CONTINUED FROM TABLE 1

| | 3 | 4 |
|-------|--|---|
| g |  |  |
| r |  |  |
| r_1 |  |  |
| n_1 |  |  |
| b |  |  |

| CONTINUED FROM TABLE 1 | | |
|------------------------|---|---|
| | 5 | 6 |
| g |  |  |
| r |  |  |
| r_1 |  |  |
| n_1 |  |  |
| b |  |  |

| CONTINUED FROM TABLE 1 | | |
|------------------------|---|---|
| | 7 | 8 |
| g |  |  |
| r |  |  |
| r_1 |  |  |
| n_1 |  |  |
| b |  |  |

CONTINUED FROM TABLE 1

| | 9 | 10 |
|-------|---|---|
| g |  |  |
| r |  |  |
| r_1 |  |  |
| n_1 |  |  |
| b |  |  |

