International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:8, No:3, 2014

Calculus Logarithmic Function for Image Encryption

Adil AL-Rammahi

***Abstract*—**When we prefer to make the data secure from various attacks and fore integrity of data, we must encrypt the data before it is transmitted or stored. This paper introduces a new effective and lossless image encryption algorithm using a natural logarithmic function. The new algorithm encrypts an image through a three stage process. In the first stage, a reference natural logarithmic function is generated as the foundation for the encryption image. The image numeral matrix is then analyzed to five integer numbers, and then the numbers' positions are transformed to matrices. The advantages of this method is useful for efficiently encrypting a variety of digital images, such as binary images, gray images, and RGB images without any quality loss. The principles of the presented scheme could be applied to provide complexity and then security for a variety of data systems such as image and others.

***Keywords*—**Linear Systems, Image Encryption, Calculus.

I. Introduction

NOW days, computers and communication technology have become widespread in domestic and official demands of our daily lives. Really, we are living in digital age representing in usages of internet, email, remote video conference, Facebook, medical reports, diagnostic of diseases, online student registration, and others. Images have taken common data via online corresponding. In other hand, important and confidential images are stored in digital ways. So, the privacy of these images must be protected from unauthorized access.

Many researches work hard in image encryption, for updating, Dang et al. proposed an approach based on the Discrete Wavelet Transform [1]. Younes and Jantan introduced a block-based transformation encrypted image algorithm [2]. Mao et al introduced chaotic Baker maps image encryption scheme [3]. Wu et al. used Sadouka matrix in encrypted image [4]. Jayant and Roy introduced the method of breaking the correlation among neighboring pixels [5]. Alghamdi and Hanif Ullah used chaotic function for iris encryption image [6]. Jolfaei and Mirghadri Surveyed the Salsa20 scheme for image encryption [7]. Ye and Zhou proposed a chaos-based image encryption scheme [8]. Dey introduced encrypted algorithm mixed the concepts of 8 bit binary numbers and Vernam permutation [9]. Landge et al. introduced encrypted algorithm by using the method of 64-bits blowfish [10]. Al-Husainy introduced algorithm based on Boolean operations and image hiding [11]. Shreef and Hoomod used interpolating functions to encrypt image [12]. Ye introduced chaos-based image encryption scheme with a permutation–diffusion mechanism [13]. Al-Rammahi introduced an algorithm based on multiplying image matrix by special contraction matrix, then a final values deal with modular technique [14]. Nidhal et al used the concepts of singular values decomposition for introducing an algorithm of image encryption [15].

Most of the available encryption algorithms are mainly used for textual data and may not be suitable for multimedia data such as images. Decimal numbers which appeared in logarithmic function are not consisting with the integer numbers of image matrix. This adds a difficult for using logarithmic function in encryption image. So, the encrypted matrix image through this function must be deal in accuracy and in sensitivity before any transformation. In other hand, rounding or punching of decimal numbers causes big errors in the stage of decryption.

In this paper, a concept of natural decimal logarithmic function is used for encryption the digital image. When decimal function operates on integer variable, the output values become decimal. So, the result does not consist with the properties of image values. And then, big errors calculated in decryption stage through exponent function. For exceeding these difficulties, output value must be analyzed with respect to each digit. Here five matrices were constructed. Each matrix is corresponding to each digit. Finally five encrypted images were transmitted for one original plain image. 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.

II. New Main Results

This section was concerned for presenting our proposed method of encryption digital image. In our approach, the decimal logarithmic function is used in encryption stage while decimal exponent function is used in the stage of decryption. The two stages are cleared carefully as follows:

Stage 1: Encryption

1) Input original image a.
2) Compute $c = Log(a)$.
3) Analyze $c = c_0.c_1c_2c_3c_4$.
4) Write encrypted images c_0 , c_1, c_2 , c_3 ,and c_4 .

Stage 2: Decryption

1) Input encrypted images c_0 , c_1 , c_2 , c_3 ,and c_4 .
2) Compute

$$y = c_0 + 0.1 * c_1 + c_2 0.01 * + c_3 0.001 * + 0.0001 * c_4$$

Adil Al-Rammahi is with the Kufa University, Faculty of Mathematics and Computer Science, Department of Mathematics, Njaf, IRQ (phone: +964(0)33219195; B.O. Box 21 Kufa, e-mail: adilm.hasan@ uokufa.edu.iq).

3) Compute $b = \exp(y)$.
4) Write decrypted images b.

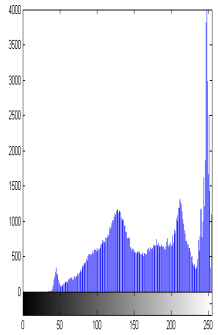
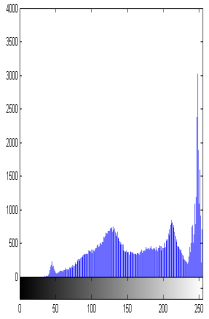
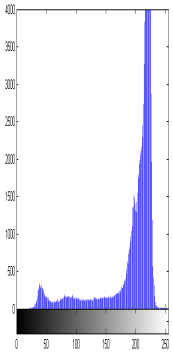
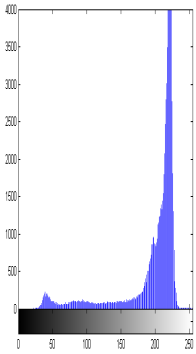
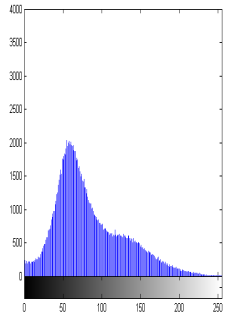
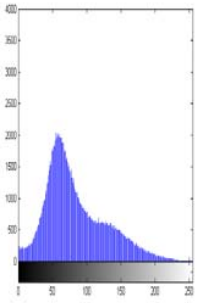
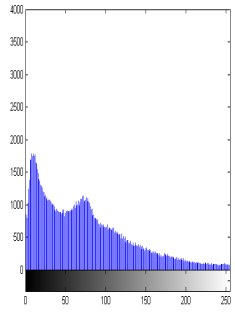
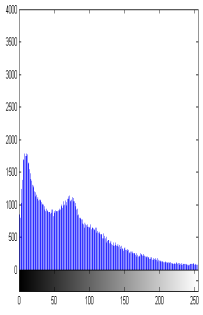
III. Implementations

For explaining the powerful of proposed method many images are tested as appearing in Table I. For explaining the goodness of proposed method, the histogram of each of the original and decrypted image implemented as showing in Table II where ha and hb represents the histograms of original image (a) and decrypted image (b) respectively.

TABLE I
TEST IMAGES

	Image 1	Image 2	Image 3	Image 4
a				
c_0				
c_1				
c_2				
c_3				
c_4				
b				

TABLE II
IMAGE HISTOGRAM

Im./ Hist.	ha	hb
1		
2		
3		
4		

IV. CONCLUSION

In this paper, we proposed a new image encryption scheme using the decimal natural logarithmic function. For testing images as referred in Table I, we have five encrypted images ($c_0, c_1, c_2, c_3,$ and c_4) corresponding to original plain image (a). These five encrypted images add more complexity for attacker and in the same way give more integrity for decryption stage. Indeed the cryptography of image has a property that the decrypted values must belong to integer numbers interval [0,255]. In our proposed algorithm, the allowed interval is transformed to fewer intervals under the action or calculus of logarithmic function. That's good, but this sub interval is containing decimal numbers. Then the encrypted values over and exceed the pliable interval. And then that is considered a problem in image matrix. When we processed these errors by approximations, a deforming is resulted for encrypted image in decryption stage. So we must think in a processing procedure deals with this problem in the integer numbers field. Here we transform each encrypted value (c) to five values ($c_0, c_1, c_2, c_3,$ and c_4). Each of them belongs to integer numbers interval [0,9]. That is leading that all encrypted images component with respect to ($c_0, c_1, c_2, c_3,$ and c_4) appears nearly black. And so, a complexity is adding against attacker, and more integrity occurs to security. The result of this method was promised. The goodness of proposed method deduces from the histogram of each the original and decrypted image as referred in Table II.

ACKNOWLEDGEMENT

This paper was supported by the faculty of mathematics and computer science of university of Kufa, Iraq. The author thanks all reviewers for deep reading on this paper.

REFERENCES

[1] P. P. Dang, and P. M. Chau, "Image encryption for secure Internet multimedia applications, Consumer Electronics", IEEE Transactions on Image Processing, 46(3), 2000, pp. 395-403.
[2] M. A. B. Younes and A. Jantan, "Image Encryption Using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, 35:1, 2003, pp. 1-8.
[3] 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, pp. 3613-3624.
[4] 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.
[5] J. Kushwaha and B. N. Roy, "Secure Image Data by Double encryption", International Journal of Computer Applications, 5(10), 2010, pp. 28-32.
[6] 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.
[7] A. Jolfaei and A. Mirghadri, "Survey: Image Encryption Using Salsa20", International Journal of Computer Science Issues, 7(5), 2010, pp. 213-220.
[8] R. Ye and 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.
[9] 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.
[10] 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.

[11] 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.
[12] 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.
[13] 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.
[14] A. AL-Rammahi, "Encryption Image Using Small Order Linear Systems and Repeated Modular Numbers", To be published at The International Conference of Applied and Engineering Mathematics, World Congress on Engineering, International Association of Engineers, London , 2-4 July 2014.
[15] N. Al-Ebadi, A. AL-Rammahi, and M. Al-Kufi, "Image Encryption Based on Singular Value Decomposition", Journal of Computer Science 10 (7), 2014, pp. 1222-1230.

Adil AL-Rammahi was born on 1963 in Najaf, Iraq. He studied Applied Mathematics at University of Technology, Baghdad, Iraq. From the same university, he obtained his M. Sc in stability. The title of Assistant professor was awarded to him in 2002. He was awarded the degree of PhD in Fractals in 2005. He has supervised several M.Sc. dissertations. He has headed the Mathematics Department for three years from 2008-2011. His area of research is Fractals, Numerical Analysis, Cryptography and Image Processing. He published more than 25 papers and one book. He was selected as an editor, reviewer and a scientific committee member in many journals and conferences.