

Dynamic Shuffling for Speed Image Encryption

Hala Bahjat, PhD
University of Technology
Computer Science Department

May A. Salih
Babylon University
Physical education collage

ABSTRACT

Encryption security and encryption speed are two important aspects of image encryption algorithms. Due to their increasingly large size, video images present a great challenge to currently available cryptographic algorithms; the processes of encryption and decryption of images are so computationally intensive that they introduce delays beyond acceptable real-time application limits. [1] In this paper we introduce a new algorithm that uses Dynamic Total Shuffling as both encryption keys and the control stream to verify which key will be used for each block.

The goal is to provide a highly secure encryption algorithm with a wide space for encryption speed.

General Terms

Pattern Recognition, Security, Algorithms, Chaotic

Keywords

Total Shuffling, real time, image encryption

1. INTRODUCTION

We ask that authors follow some simple guidelines. In essence, we ask you to make your paper look exactly like this document. The easiest way to do this is simply to download the template, and replace the content with your own material.

During the development of network and multimedia technology, more and more images transmit over the Internet and through the wireless networks. Digital images have become one of the most important information carriers, which is helpful for people to communicate with each other. However, because of the intrinsic features of images, such as bulk data capacity and high correlation among pixels, it is not suitable for practical image encryption, especially during on-line communications. Therefore, people begin to explore chaotic dynamic shuffling which is more efficient at hiding image information. [2]

Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. Images differ from text in that they are bigger in size and the decrypted image must be equal to the encrypted image. Another significant point to consider in transfer of digital images is their special attributes like bulk data capacity, high redundancy, and high correlation between neighboring pixels [3][4].

2. IMAGE CRYPTOGRAPHY

Cryptography presents the best, and an inevitable, solution to problems in sending images. Cryptography can be defined as the art of creating an unintelligible form from intelligent information [6]. It is done to ensure that if any eavesdropper attempts to deduce the plaintext, then he is unable to discover this confidential data. It is an ancient technology for the secure transfer of messages. Traditional use of cryptography dealt only with textual data and not much focus was laid on

the secure transmission of images or audio/visual data. But today, the situation has changed and now it is capable for handling any type of media or data. Encryption of textual data is relevant mostly to one-dimensional data, which is why techniques best suited for text are inadequate for two-dimensional digital images. Moreover, cryptography has spread gradually from its early use in military and political fields into everyday civilian life. It now plays a crucial role in activities like Internet banking, e-commerce, e-finance, etc.[7].

3. TRADITIONAL ENCRYPTION STANDARDS

The established encryption algorithms like DES, AES, etc. concentrate on changing two-dimensional data into one-dimensional data and then applying encryption on it. [3] But this technique is less efficient to encrypt and decrypt images. Because the most important factor in the encryption process is time of this reason, such a primitive style of encryption it is not preferred for digital images. Recently, Zhang et al. proposed an image encryption method based on a total shuffling scheme [11]. In this method, the secret encryption code stream is not only associated with the key, but also related to the plain image. Because the random number used in the diffusion process is obtained by iterating the skew tent map, and the number of iterations is determined by the previous pixel value of cipher image, which includes the plain image's previous pixel value, the next random number is indirectly related to the previous pixel value of plain image. This plain image encryption method holds up strongly against plaintext attacks [12]. However, the first secret code in [11] is not safe enough to resist the chosen plaintext attack.

4. CHAOTIC SYSTEMS

Some of the inherent characteristics of a chaotic system (the initial value sensitivity, parameter sensitivity, long-term evolution unpredictability) correspond to those of image encryption system. Examples are plaintext sensitivity, key sensitivity, and noise-like cipher-text. In addition, one can obtain a chaotic system using deterministic equations which can generate pseudo-random numbers with excellent features. Therefore, chaotic systems are widely employed in image encryption research [10].

5. THE PROPOSED IMAGE ENCRYPTION ALGORITHM

The proposed schema is based on two types of keys: encryption key and control key. The control key is generated using a controlled ranged randomized stream and the encryption keys are a set of non-fixed variable Dynamic shuffling. Encryption in digital images mostly works at pixel level, which is the lowest level of information in the image. But because of strong correlation between neighboring pixels, one can easily decode data for one pixel if that of a neighboring pixel becomes known. However, an image can

also be interpreted as an ordered arrangement of image blocks instead of pixels. An accurate orientation of these image blocks lets us infer information from the image, where any change causes visual disruption [4]. The skew tent map is used in [11] and formulated as

$$F(x) = \begin{cases} \frac{x}{p} & , \quad x \in [0, p] \\ \frac{1-x}{1-p} & , \quad (p, 1] \end{cases} \quad (1).$$

Assume the plain image is of 8-bit grayscale and size $M \times N$, denoted by $P = \{p_0, p_1, \dots, p_{MN-1}\}$ using top to bottom and then left to right scanning methods. The encryption scheme in [11] consists of two procedures, i.e. permutation and diffusion. The pixel permutation procedure is shown as follows:

Step 1. Iterate (1) to obtain a pseudo-random sequence of size $M \times N$, denoted by $Z = \{z_0, z_1, \dots, z_{MN-1}\}$ excluding the transient states of the first L iterations.

Step 2. Sort Z in ascending order to get $L = \{L_0, L_1, \dots, L_{MN-1}\}$.

Step 3. According to the relationship of Z and L , a scrambling vector $T = \{t_0, t_1, \dots, t_{MN-1}\}$ is obtained such that $z_i = z_{t_i}$, $i = 0, 1, \dots, MN-1$.

Step 4. Permute the plain image P with T to get $P' = \{p_{(0)}, p_{(1)}, \dots, p_{(MN-1)}\}$ such that $p_{(i)} = p_{(t_i)}$, $i = 0, 1, \dots, MN-1$.

Then the diffusion procedure is as follows:

Step 1. Let $i = 0$.

Step 2. Get an 8-bit pseudo-random integer d_i from the current state value x , i.e. $d_i = \text{mod}(\text{floor}(x \times 256), 256)$.

Step 3. Calculate the current pixel value c_i of cipher image according to the current pixel value p_i and the previous pixel value $p_{(t_i)}$ of the plain image as well as d_i , i.e. $c_i = p_i \oplus p_{(t_i)} \oplus d_i$, where \oplus means bitwise XOR operator.

Step 4. Calculate k using c_i , i.e. $k = 1 + \text{mod}(c_i, 2)$. Then continue to iterate (1) for k times to obtain a new state value x .

Step 5. Let $i = i + 1$, and return to Step 2 until i reaches MN . [13]

We modify the original algorithm in [13] to have a variable-sized key that changes with each image size giving a wider key space computed as in the following $(\text{length} \times \text{height} \times \text{pixel range values})^{\text{length} \times \text{height} \times \text{pixel range values}}$ that is $2.0589e + 64$ for an image with 10×10 pixels and only 30 gray level, for example.

6. PERFORMANCE OF THE PROPOSED ALGORITHM

A good image encryption algorithm should be sensitive to the cipher keys, and the key space should be large enough to make brute force attacks infeasible. For the proposed image encryption algorithm, key space analysis and testing have been performed and completed, with results summarized as follows:

Key Space is $1.8388e+118$. The proposed image cipher has $(1.8388 e+118)$ different combinations of possible keys An

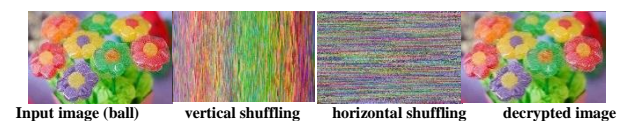
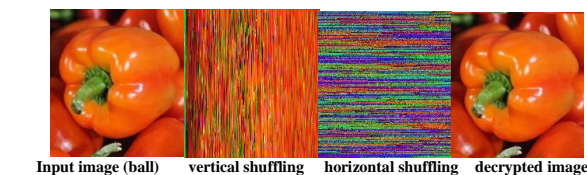
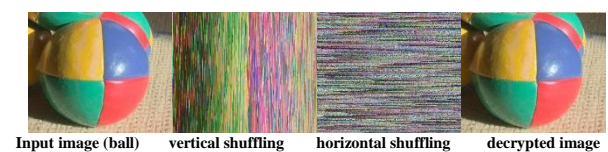
image cipher with such a large combined key space is sufficient for reliable practical use and can resist all kinds of brute force attacks.

7. EXPERIMENTAL RESULTS

This algorithm is designed to encode - decode images fast . Time is a major concern. during the algorithm behavior analysis the following results are noticed

Table (1). Behavior Analysis

Image size (pixels)	Average encryption time	Average decryption time	Average total time
480*480	0.04 sec.	2.5 sec.	2.54 sec.
720*720	2.7 sec.	3.1 sec.	5.8 sec.
960*960	8 sec.	13.3 sec.	21.3 sec.



Table(2) encryption / decryption time

Image	Encryption time	Decryption time
Ball	0.003422 sec.	4.239834 sec
Pepper	0.002073 sec	0.194880 sec
Roses	0.005908 sec	1.982690 sec

8. OBJECTIVE FIDELITY CRITERIA

Table (3)SNR , PNSR and MSE results

image	NSR	PNSR	MSE
Ball	3.0634	6.7695	1.3255e+04
Pepper	4.0483	5.9599	1.6485e+04
Roses	3.4704	7.6080	1.1015e+04

The objective fidelity criteria provide equations that can measure the amount of error in the reconstructed (deciphered) images or to measure the amount of error between pure image and ciphered image. Commonly used objective measures are the Root-Mean-Square- error (RMSE), Signal-to-Noise Ratio (SNR) and the Peak Signal-to-Noise Ratio (PSNR) [Sco98].

8.1 (The Root- Mean- Square Error (RMSE))

The MSE is the average of the square of errors (pixel differences) of the two images, found by taking the square root ("root") of the error squared ("square") divided by the total number of pixels in the image ("mean") [lkh05]:

$$MSE = \frac{1}{H * W} \sum_{y=0}^{H-1} \sum_{x=0}^{W-1} (f(x, y) - f'(x, y))^2$$

The Root Mean Square error (RMSE) is defined as the square root of the MSE:

$$RMSE = \left[\frac{1}{H * W} \sum_{y=0}^{H-1} \sum_{x=0}^{W-1} (f(x, y) - f'(x, y))^2 \right]^{1/2}$$

Hence, the smaller the value of MSE, the better the deciphered image represents the original image and the large value of error. The better the ciphered image, the more pure image information it conceals.

8.2 (Signal to Noise Ratio)

It is fidelity parameter used to measure the distortion level caused by image cryptography. It can be defined as:

$$SNR = \frac{\sum_{y=0}^{H-1} \sum_{x=0}^{W-1} (f(x, y))^2}{\sum_{y=0}^{H-1} \sum_{x=0}^{W-1} (f(x, y) - f'(x, y))^2}$$

8.3 Peak Signal to Noise Ratio (PSNR)

This can be defined as:

$$PSNR = 10 \log_{10} \left(\frac{(255)^2}{MSE} \right)$$

Where MSE is the mean square error.

In image cryptography, a large PSNR value implies a better-deciphered image, and a smaller number implies better image concealment of original image is obtained. Subsequent Pages

For pages other than the first page, start at the top of the page, and continue in double-column format. The two columns on the last page should be as close to equal length as possible.

9. CONCLUSION

9.1 Trade-off between complexity and security

For multimedia content encryption, especially for application in real-time video communication, low processing overhead becomes extremely important. Due to the restriction of real-time, it becomes important to select the most critical unit to shuffle. Syntax compliance makes it easier to locate different types of critical data blocks in the process of bit stream analysis.

9.2 Security Analysis

Due to the good randomness of pseudo-random sequence, the encryption approach presented in this paper amounts to changing the cipher every time. According to the theory of cryptology, it is the most secure encryption approach and is therefore superior to methods using a standard encryption algorithm.

In this paper, we proposed a lookup table method to improve the encryption/decryption speed of the image encryption scheme presented in [10, 11], and employed “addition and modulo” operator instead of “XOR” in the diffusion procedure. We compared our proposal and the methods in [10, 11] regarding encryption/decryption speed, key space, key

sensitivity, information entropy, cipher image statistical properties, and plain image sensitivity analysis. The results fully demonstrate that the speed of our proposed method is about 8 times faster than those of [10, 11] and with stronger, more complex security. Therefore, the proposed method is more feasible for practical communications.

10. REFERENCES

- [1] "Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-Time Video" Las Vegas, Nevada, USA September 20-September 23 ISBN: 0-8186-7180-7
- [2] "A Symmetric Image Encryption Scheme Based on Composite Chaotic Dispersed Dynamics System" Zhenzhen Lv1, Lei Zhang2, and Jiansheng Guo 3, Proceedings of the Second Symposium International Computer Science and Computational Technology (ISCSCCT '09) Huangshan, P. R. China, 26-28, Dec. 2009, pp. 191-194
- [3] Zhang S. and M. A. Karim, pp. 318-322, Vol. 21, No. 5, June 5 1999, Color image encryption using double random phase encoding, Microwave and optical technology letters.
- [4] Maniccam S.S and Bourbakis N.G., pp. 1229-1245, 2001, Lossless image compression and encryption using SCAN, Pattern Recognition.
- [5] Vinod Patidar G. Purohit, K. K. Sud, N. K. Pareek, "Image encryption through a novel permutation substitution scheme based on chaotic standard map," Chaos-Fractal Theory and its Applications, IEEE International Workshop on, 2010, pp. 164-169.
- [6] Quist-Aphetsi Kester, "A cryptographic Image Encryption technique based on the RGB Pixel shuffling," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 2, issue 2, January 2013, pp. 848-854
- [7] The Hacking Tutorial Website. [Online]. Available: <http://www.hacking-tutorial.com/tips-and-trick/hideseecret-file-inside-an-image-steganography/>
- [8] "Sparse Matrix Technology" 2007 by Sergio Pissanetzky and SciControls.com. ISBN 978-0-9762775-3-8 .
- [9] "Gauss Jordan elimination method for computing outer inverses " ,Predrag S. Stanimirovi_c1, Marko D. Petkovi_c2.
- [10] A. A. Adb El-Latif, L. Li, T. Zhang, N. Wang, X. Song, and X. Niu, "Digital image encryption scheme based on multiple chaotic systems," Sensing. Imaging. An Int. J. vol. 13, pp. 67-88, 2012.
- [11] G. Zhang, and Q. Liu, "A novel image encryption method based on total shuffling scheme," Opt. Commun. vol. 284, pp. 2775-2780, 2011.
- [12] Y. Zhang, J. Xia, P. Cai, and B. Chen, "Plaintext related two-level secret key image encryption scheme," TELKOMNIKA. vol. 10, pp. 1254-1262, 2012.
- [13] Yong Zhang "Encryption Speed Improvement on "An Improvement over An Image Encryption Method Based on Total Shuffling" 2013 International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS)