Proceedings of the Seventh International Conference on Machine Learning and Cybernetics, Kunming, 12-15 July 2008

AN IMAGE SCRAMBLING ALGORITHM USING PARAMETER BASED M-SEQUENCES

YICONG ZHOU[1], KAREN PANETTA[1], SOS AGAIAN[2]

[1]Department of Electrical and Computer Engineering, Tufts University, Medford, MA 02155, USA
[2]Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX 78249, USA
E-MAIL: Yicong.Zhou@tufts.edu, Karen@eecs.tufts.edu, Sos.Agaian@utsa.edu

Abstract:

Image scrambling is a useful approach to secure the image data by transforming the image into an unintelligible format. This paper introduces a new parameter based M-sequence which can be produced by a series of shift registers. In addition, a new image scrambling algorithm based on the parametric M-sequence is presented. The user can change the security keys, *r*, which indicates the number of shift operations to be implemented, or the distance parameter *p*, to generate many different M-sequences. This makes the scrambled images difficult to decode thus providing a high level of security protection for the images. The presented algorithm can encrypt the 2-D or 3-D images in one step. It also shows good performance in the image attacks such as filters (data loss) and noise attacks. The algorithm can be applied in the real-time applications since it is a straightforward process and easily implemented.

Keywords:

Image scrambling algorithm; parametric M-sequence

1. Introduction

With rapid escalation of network community, a large amount of videos and images with private or business information spread in the network. The information security becomes an important and urgent issue not only for individuals but also for business and governments. Security of image and video data is very important in many areas, such as privacy and copyright protection, security communication, and also in military applications. Image scrambling (i.e. encryption) is a good tool to make the scrambled image visually unrecognizable and difficult to decrypt for unauthorized users.

The M-sequence, also called maximum length sequence, is a type of pseudorandom binary recursive sequence which can be generated by maximal linear feedback shift registers [1-3]. Due to its remarkable and useful properties, M-sequence is widely used in digital communication such as spread spectrum communication, pseudo random noise [4-6].

Several applications of M-sequence have been addressed specially focusing on its pseudo random properties. State-of-the-art applications on M-sequence include digital watermarking such as image watermarking [7, 8], video watermarking [9], and audio watermarking [10, 11]. The M-sequence is also used for FRMI experiment in biomedical applications [12].

Since the M-sequence is a periodic binary sequence with autocorrelation characteristics, it can be extended to the new application area of image scrambling. In this paper, we introduce a new parameter based M-sequence and a new image scrambling algorithm using this M-sequence. The scrambled images are difficult to decode since the security keys, the shift parameter r and the distance parameter p, have many options. The new algorithm can be used to scramble the 2-D image such as binary images, grayscale images and 3-component color images as well. The experimental results in section 4 demonstrate that the new scrambling algorithm is a lossless encryption approach and show good performance in common image attacks such as filters (data loss), Gaussian noise and Salt Pepper noise attacks.

2. Parameter based M-sequence and its transforms

2.1. Parameter based M-sequence

The classical M-sequence is a periodical binary sequence which can be generated by a series of shift registers with modulo 2 operations.

Definition 2.1, Classical M-sequence:

The classical M-sequence $\{m_k\}$ is satisfied as the following operation [4, 5]

$$m_k = \sum_{i=1}^{n} a_i m_{k-i} \pmod 2 \qquad (1)$$

where n is the number of the shift registers, $a_i = 0,1$ is the

978-1-4244-2096-4/08/$25.00 ©2008 IEEE

coefficient of the i^{th} shift register, and $m_k = 0,1$. The circuit implementing the operation above is called the M-sequence generator.

The output of the M-sequence generator depends on the coefficient and the initial value of the registers. The output M-sequence is a binary sequence with a maximum length period $T = 2^n - 1$. Suppose the output M-sequence be $\{m_k\} = \{m_1, m_2, ..., m_T\}$, then $m_k = m_{k+T} = m_{k+2T} = ...$

Definition 2.2, Parameter based M-sequence:
Let the binary sequence $\{s_1, s_2, ..., s_n\}$ be the initial value of the n-stage shift registers in the M-sequence generator, and the output M-sequence be $\{b_{r1}, b_{r2}, ..., b_{rT}\}$ after the register is shifted r times. The binary sequence $\{c_{r1}, c_{r2}, ..., c_{rn}\}$ called the parameter based M- sequence is defined as

$$c_{ri} = b_{r(i+p)} \tag{2}$$

$\{c_{r1}, c_{r2}, ..., c_{rn}\}$ is also called the M-sequence representation of $\{s_1, s_2, ..., s_n\}$. Where i, r, p, T are integers, and $1 \le i \le n$, $T = 2^n - 1$, $1 \le r \le T$, $0 \le p \le T - n$.

2.2. M-sequence Transforms

Based on the definition 2.2 above, a decimal number with binary representation of $S = (s_1, s_2, ..., s_n)_2$ can be transformed into its M-sequence representation $C_r = (c_{r1}, c_{r2}, ..., c_{rn})_2$, where C_r is another decimal number. Similarly, a decimal sequence $\{S_1, S_2, S_3, ..., S_N\}$ can also be transformed to its M-sequence representation $\{C_{r1}, C_{r2}, C_{r3}, ..., C_{rN}\}$, which the permutation sequence of $\{S_1, S_2, S_3, ..., S_N\}$. Furthermore, the permutation sequence $\{C_{r1}, C_{r2}, C_{r3}, ..., C_{rN}\}$ will differ when the shift parameter r and the distance parameter p have different values.

This permutation transformation can be applied to image scrambling since it can change the row and column positions of the image pixels. The shift parameter r and the distance parameter p will act as the security keys to generate the different sequences $\{C_1, C_2, C_3, ..., C_N\}$.

For the specific values of r and p, the M-sequence representation of $\{1, 2, 3, ..., N\}$ can be defined by

$$C_r = \{C_{r1}, C_{r2}, C_{r3}, ..., C_{rN}\} \tag{3}$$

The 2-D image data is stored in a 2-D matrix such as grayscale images and binary images. To scramble those 2-D images in one step, the 2-D M-sequence transform is introduced.

Definition 2.3, The 2-D M-sequence transform:
Let D be an $M \times N$ image matrix, T_r be the row coefficient matrix, T_c be the column coefficient matrix. The 2-D M-sequence Transform is defined as [13]:

$$S = T_r D T_c \tag{4}$$

where S is the scrambled image matrix, and

$$T_r(m,n) = \begin{cases} 1 & (m, C_{mi}) \\ 0 & otherwise \end{cases}, \quad T_c(i,j) = \begin{cases} 1 & (C_{rj}, j) \\ 0 & otherwise \end{cases}$$

where $1 \le m, n \le M$, $1 \le i, j \le N$

Definition 2.4, The Inverse 2-D M-sequence transform:
Let S be a scrambled $M \times N$ image matrix, T_r^{-1} and T_c^{-1} be the inverse matrices of the row and column coefficient matrices defined in definition 2.3, the Inverse 2-D M-sequence Transform is defined as [13].

$$R = T_r^{-1} S T_c^{-1} \tag{5}$$

where R is the reconstructed image matrix.

Since the data of the 3-component color image is three 2-D matrices, the 3-D M-sequence transform is introduced to achieve a more efficient way scrambling the color images.

Definition 2.5, The 3-D M-sequence transform:
Let $Q = (Q_i \quad i)$, where $i = 1, 2, 3$ refers to three color planes, Q_i is the original image data matrix of the i[th] color plane. $T_r = (T_{ri} \quad i)$ and $T_c = (T_{ci} \quad i)$, where T_{ri} and T_{ci} are the row and column coefficient matrices of the i[th] color plane defined in definition 2.3. The 3-D M-sequence Transform is defined as [13].

$$E = T_r Q T_c \tag{6}$$

where E is the data matrix of the scrambled color image.

Definition 2.6, The inverse 3-D M-sequence transform:
Let $E = (E_i \quad i)$, where $i = 1, 2, 3$, E_i is the scrambled image data matrix of the i[th] color plane. $T_r^{-1} = (T_{ri}^{-1} \quad i)$ and $T_c^{-1} = (T_{ci}^{-1} \quad i)$, where T_r^{-1} and T_{ci}^{-1} are the inverse row and column coefficient matrices of the i[th] color plane. The Inverse 3-D M-sequence Transform is defined as [13].

$$Z = T_r^{-1} E T_c^{-1} \tag{7}$$

where Z is the reconstructed color image.

3. The image scrambling algorithm using parameter based M-sequence transforms

The data of a 2-D image is a 2-D matrix while the data of a 3-component color image is consisted of three 2-D matrices, one matrix for each of the 3 different color planes of an image. Choosing the 3-D M-sequence transform to scramble the color images is a more efficient way than selecting 2-D M-sequence transform since the 3-D images

can be scrambled in one step by using the 3-D M-sequence transform. Similarly, the 2-D M-sequence transform is more efficient for scrambling the 2-D images in one step such as grayscale images, binary images, medical images, and so on.

The image scrambling algorithm is shown as Figure 1. The 2-D or 3-D transform will be chosen based on the characteristics of the image data. If the image is a 2-D image, the 2-D M-sequence transform will be chosen to scramble the image data. Otherwise, the 3-D transform will be selected. The row and column coefficient matrices should be calculated by choosing the security keys: the shift parameter r and the distance parameter p. The scrambled image can be generated by applying the 2-D/3-D M-sequence transform to the original image at one time.

The authorized users should be provided the security keys to reconstruct the original image in their inverse process. The security keys will be used to calculate the inverse row and column coefficient matrices. The inverse 2-D M-sequence transform will be selected if the image data is a 2-D matrix. On the other hand, the inverse 3-D transform will be used to decode the scrambled image data. The reconstructed images can be obtained by applying the inverse transform to the scrambled image.

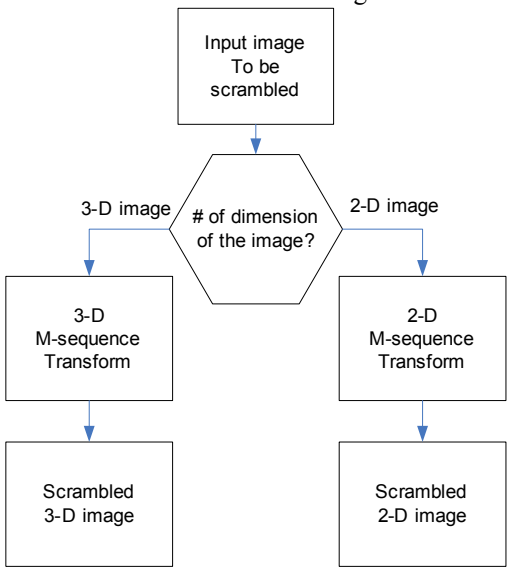

Figure 1. Block diagram of image scrambling algorithm

4. Experimental results

The new algorithm has been implemented in several types of images such as binary images, medical images, grayscale images and also color images. Some examples will be provided in the following to show the performance of the presented algorithm.

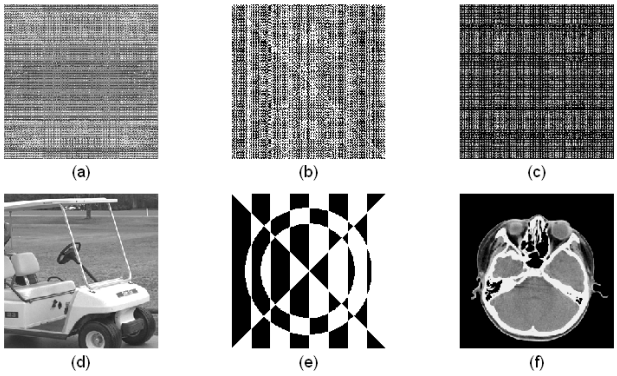

Figure 2. 2-D image scrambling with different security keys (a) Scrambled grayscale image with r=6, p=0; (b) Scrambled binary image with r=9, p=3; (c) Scrambled medical image with r=12, p=5; (d) Reconstructed medical image from (a); (e) Reconstructed medical image from (b); (f) Reconstructed medical image from (c);

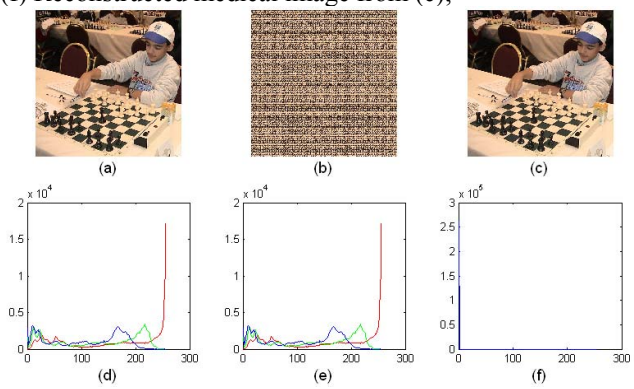

Figure 3. Color image scrambling with r=8, p=2; (a) The original color image; (b) The scrambled color image; (c) The reconstructed color image; (d) Histogram of (a); (e) Histogram of (b); (f) Histogram of difference (a) and (c)

The 2-D images are scrambled with different security keys as shown in Figure 2. The reconstructed images in Figure 2 and reconstructed color image in Figure 3(c) demonstrate that the original images can be perfectly reconstructed without any distortion. This is also verified by the histogram of the difference between the original image and the reconstructed image as shown in Figure 3(f). All of these show that the parametric M-sequence based algorithm is a lossless encryption approach.

Figure 4 demonstrates that the parameter M-sequence based scrambling algorithm also shows good performance for the image attacks such as Gaussian low pass filter (data loss), Gaussian noise and Salt & Pepper noise attacks. The reconstructed images after attacks are visually acceptable

since they contain almost all visual information of the original images.

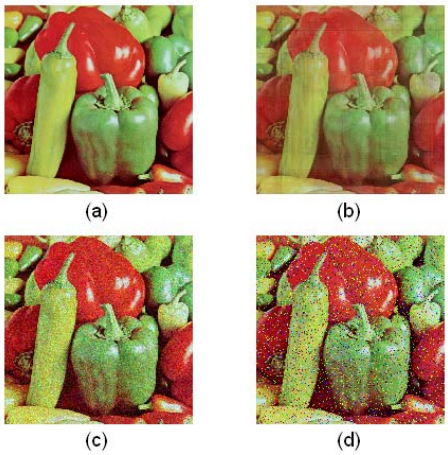

Figure 4. Color image scrambling with attacks, r=7, p=1; (a) The original color image; (b) Reconstructed image after applying Gaussian Lowpass Filter to the scrambled image; (c) Reconstructed image after adding 10% Gaussian noise to the scrambled image; (d) Reconstructed image after adding 10% Salt & Pepper noise to the scrambled image.

5. Conclusions

In this paper, we introduced a new parameter based M-sequence which can be generated by shift registers. We also presented a new image scrambling algorithm based on this M-sequence. The parameter *r*, which is the number of shift operations to be performed on the register, and the distance parameter *p* can be used as the security keys since the many different M-sequences can be derived by changing the *r* and *p* values. The many possible choices of the security keys prevent eavesdroppers from decoding the scrambled images. As a result, the image is protected with high level of security. The experimental results show that the new algorithm is a lossless encryption method since the original images can be completely reconstructed without losing quality. The test results from image attacks demonstrate that the parameter M-sequence based scrambling algorithm can tolerate the common image attacks since the original images can be reconstructed with high quality after an image attack. The scrambling algorithm can be also used in the real-time applications due to its straightforward and efficient process.

References

[1] M. Cohn, and A. Lempel, "On fast M-sequence transforms (Corresp.)," *Information Theory, IEEE Transactions on,* vol. 23, pp. 135-137, 1977.

[2] S. Golomb, *Shift Register Sequences*: Aegean Park Press, 1982.

[3] A. Lempel, and W. L. Eastman, "High Speed Generation of Maximal Length Sequences," *Computers, IEEE Transactions on,* vol. C-20, pp. 227-229, 1971.

[4] R. Pickholtz, D. Schilling, and L. Milstein, "Theory of Spread-Spectrum Communications-A Tutorial," *Communications, IEEE Transactions on,* vol. 30, pp. 855-884, 1982.

[5] D. R. Morgan, "Autocorrelation Function of Sequential M-Bit Words Taken from an N-Bit Shift Register (PN) Sequence," *Transactions on Computers,* vol. C-29, pp. 408-410, 1980.

[6] F. J. MacWilliams, and N. J. A. Sloane, "Pseudo-Random Sequences and Arrays," *Proceedings of the IEEE,* vol. 64, pp. 1715-1729, 1976.

[7] Yanmei Fang, Jiwu Huang, and Y.Q.Shi, "Image watermarking algorithm applying CDMA," in *Circuits and Systems, Proceedings of the 2003 International Symposium on*, Bangkok, Thailand, 2003, pp. 948-951.

[8] A. Z. Tirkel, C. F. Osborne, and R. G. Van Schyndel, "Image watermarking-a spread spectrum application," in *Spread Spectrum Techniques and Applications Proceedings, IEEE 4th International Symposium on*, Electoral Palace, Mainz, Germany, 1996, pp. 785-789.

[9] Fuhao Zou, Zhengding Lu, Hefei Ling and Yanwei Yu, "Real-time video watermarking based on extended m-sequences," in *Multimedia and Expo, 2006 IEEE International Conference on*, Toronto, Canada, 2006, pp. 1561-1564.

[10] Hong Wang, Ling Lu, Dashun Que, and Junbo Huang, "Adaptive audio digital watermark algorithm based on m-sequence modulation," in *Signal Processing, 7th International Conference on*, Beijing, China, 2004, pp. 2401-2404.

[11] N. Cvejic, A. Keskinarkaus, and T. Seppanen, "Audio watermarking using m-sequences and temporal masking," in *Applications of Signal Processing to Audio and Acoustics, 2001 IEEE Workshop on the*, New Paltz, NY, 2001, pp. 227-230.

[12] G. T. Buracas, and G. M. Boynton, "Efficient Design of Event-Related fMRI Experiments Using M-sequences," *NeuroImage,* vol. 16, pp. 801-813, 2002.

[13] Yicong Zhou, Karen Panetta and Sos Agaian, "P-recursive sequence and key-dependent multimedia scrambling," in *Mobile Multimedia/Image Processing for Military and Security Applications, SPIE Defence and Security Symposium 2008*, Orlando, FL USA 2008.