Comparison of Recursive Sequence Based Image Scrambling Algorithms

Yicong Zhou, Karen Panetta, *Fellow, IEEE*
Department of Electrical and Computer Engineering
Tufts University
Medford, MA 02155, USA
Yicong.Zhou@tufts.edu, Karen@eecs.tufts.edu

Sos Agaian, *Senior Member, IEEE*
Department of Electrical and Computer Engineering
University of Texas at San Antonio
San Antonio, TX 78249, USA
Sos.Agaian@utsa.edu

***Abstract*— Image scrambling is an effective method for providing image security. This paper compares and discusses the effectiveness of some image scrambling algorithms based on recursive sequences such as the Fibonacci number, Generalized Fibonacci number, Gray Code, Generalized Gray Code, Generalized P-Gray Code, P-Fibonacci, P-Lucas, P-recursive sequences, and parametric M-sequences for image scrambling. The comparison of these methods for image security is based on three basic types of attacks: data loss attacks, noise attacks and plaintext attacks. The experimental results demonstrate that the scrambling algorithms based on both P-Fibonacci and P-Lucas sequences show better performance when subjected to attacks and also in terms of algorithm execution analysis which shows implementation efficiency and low computational requirements. This makes them suitable for real-time applications.**

***Keywords*— Image scrambling, Fibonacci number, P-Fibonacci, P-Lucas, P-Gray Code, M-sequence**

I. INTRODUCTION

With the advancement of network technology and digital multimedia services, the transmission of the image, video and multimedia with private or business information is more ubiquitous. Providing security for these types of media data becomes an urgent issue for individuals, companies and also governments. Protection and security of the image and video data are important in many areas such as privacy and copyright protection, security communication, video monitoring for homeland security purposes and also in military applications. Image scrambling (i.e., encryption) is an effective approach to protect images by transforming the images into an unintelligible format.

There are many different image scrambling approaches used to protect the images and information. Image scrambling algorithms based on recursive sequences are state-of-the-art approaches that have been discussed frequently [1-8].

Security is important not only for the encrypted objectives but also for the encryption algorithms themselves. There are many types of attacks used to test the security abilities of encryption algorithms. In cryptanalysis, the plaintext is the original information to be encrypted. The ciphertext is the encrypted plaintext generated by an encryption algorithm. The known-plaintext attack and chosen-plaintext attack are two types of plaintext attacks frequently used in cryptanalysis [9].

The permutation based image encryption algorithms such as image scrambling algorithms was shown to be vulnerable by the plaintext attacks [10].

TABLE I. DEFINITION OF THE SEQUENCES

Sequence	Definition	Reference
Parameter based M-sequence	$c_{ri} = b_{r(i+p)}$	[8]
Fibonacci number	$F(n)=\begin{cases}0 & n<1\\ 1 & n=1\\ F(n-1)+F(n-2) & n>1\end{cases}$	[1, 11]
Generalized Fibonacci number	$F(n)=\begin{cases}0 & n<1\\ a & n=1\\ b & n=2\\ F(n-1)+F(n-2) & n>2\end{cases}$	[2]
P-Fibonacci sequence	$F_p(n)=\begin{cases}0 & n<1\\ 1 & n=1\\ F(n-1)+F(n-p-1) & n>1\end{cases}$	[5]
P-Lucas sequence	$L_p(n)=\begin{cases}0 & n<1\\ 2 & n=1\\ 1 & n=2\\ L(n-1)+L(n-p-1) & n>2\end{cases}$	[5]
Gray Code	$g_i=\begin{cases}a_k & i=k\\ (a_i+a_{i+1}) \bmod 2 & 1\le i<k\end{cases}$	[3]
Generalized Gray Code	$g_i=\begin{cases}a_k & i=k\\ (a_i+a_{i+1}) \bmod q & 1\le i<k\end{cases}$	[4]
Generlized P-Gray Code	$g_i=\begin{cases}a_k & i=k\\ (a_i+a_{i+p+1}) \bmod n & 0\le i\le k-p-1\\ a_i & i>k-p-1\end{cases}$	[6]
P-recursive sequence	$R(n)=\begin{cases}0 & n\le 0\\ B(n) & 0<n\le p+1\\ R(n-1)*R(n-p-1) & n>p+1\end{cases}$	[7]

In this paper, we discuss and compare the security issue and execution time of the image scrambling algorithms based on the recursive sequences. The discussion focuses on the comparison of the ability to tolerate image attacks and the space of security keys which addresses the security level of image encryption algorithms. The larger the key space the algorithm has, the more difficulty an unauthorized user will

face to decode the encrypted images. As a result, a higher level of security for encrypted images will be achieved.

The mathematic definition of these recursive sequences is given in the second section. In the third section, we discuss the security issue of these sequence based algorithms such as security keys, data loss attacks, noise attacks and plaintext attacks. The execution time of these algorithms is compared in the fourth section. The experimental results are given as well. The fifth section will draw a conclusion of this paper.

II. Recursive Sequences

In this section, we review the definitions of nine recursive sequences as shown in Table I. These recursive sequences were successfully applied to image scrambling using the corresponding transforms.

From the definition in Table I, some recursive sequences show more comprehensive properties since other sequences can be derived under different conditions. For example, the Fibonacci number and Lucas number are special cases of the Generalized Fibonacci number [2]. Furthermore, the Fibonacci number can be derived from the P-Fibonacci sequence [5]. The Gray Code and Generalized Gray Code can be obtained from the Generalized P-Gray Code [6]. The P-recursive sequence can produce the P-Fibonacci sequence, P-Lucas sequence and the P-Gray Code as well [7].

III. Securtiy Analysis

To utilize these recursive sequences in image scrambling, several sequence transforms were developed [1-7]. The images can be fully encrypted by using the scrambling algorithms based on the Fibonacci number, Generalized Fibonacci number, P-Fibonacci, P-Lucas, and P-recursive sequences, and parametric M-sequence as well. The images can also be partially encrypted by implementing the scrambling algorithms based on the Gray Code, Generalized Gray Code and the Generalized P-Gray Code.

A. The Space of Security Keys

The space of security keys is an important specification of the image scrambling algorithm. The scrambled images are easy to decode if there is no security key in the scrambling algorithm. If the algorithm has a larger key space, namely a larger number of security keys, it will be more difficult for an unauthorized user to decrypt the scrambled images even if the individual knows the scrambling algorithm. Therefore, higher security levels of the scrambled objectives can be obtained.

The experimental results in Fig. 1 show the importance of the security keys in image scrambling. The original image can be perfectly reconstructed only by using the correct security keys. The reconstructed image in Fig. 1(c) and the histogram (Fig. 1(e)) of the difference between the original image (Fig. 1(a)) and the reconstructed image (Fig. 1(c)) verify this perfect reconstruction. However, the original image cannot be recovered even if we use the same sequence but the wrong security key. This can be proved by the reconstructed image in Fig. 1(d) and the histogram (Fig. 1(f)) of the difference between the original image (Fig. 1(a)) and the reconstructed image (Fig. 1(d)). This demonstrates that the recursive sequence based scrambling algorithms are lossless encryption approaches.

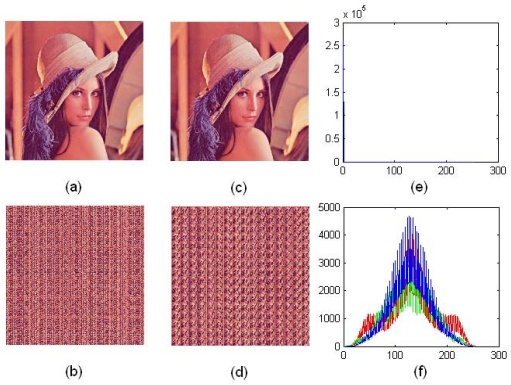

Figure 1. Demonstrating perfect reconstruction using the parametric M-sequence (a) the original image; (b) the scrambled image, r = 8, p=2; (c) the reconstructed image, r = 8, p=2; (d) the reconstructed image, r = 5, p = 3; (e) the image histogram of (c)-(a); (f) the image histogram of (d)-(a).

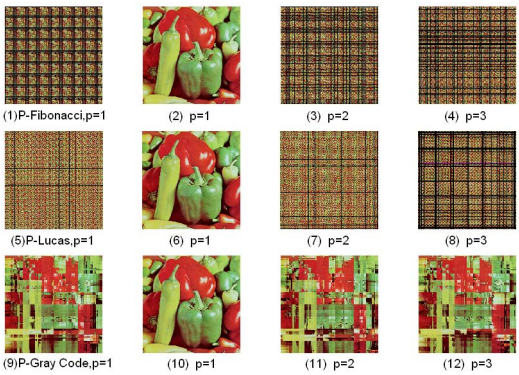

Figure 2. Shows the importance of the security keys by reconstructing images using the same sequence but different p values (1) Scrambled image using P-Fibonacci sequence; (2-4) Reconstructed images of (1) using P-Fibonacci sequence with differeny p values; (5) Scrambled image using P-Lucas sequence; (6-8) Reconstructed images of (5) using P-Lucas sequence with different p values; (9) Scrambled image using P-Gray Code; (10-12) Reconstructed images of (9) using P-Gray Code with different p values.

Fig. 2 depicts the experimental results using the scrambling algorithms based on P-Fibonacci sequence, P-Lucas sequence and P-Gray Code. We tried to use the same sequence but different security keys to decrypt the scrambled images. The results show that the images can be completely recovered only when the correct security keys are being used (shown as Fig. 2 (2), (6), (10)). Otherwise, the original image cannot be recovered even using the scrambling algorithms based on the same sequence.

Furthermore, the larger the number of possible choices for the security keys that exists, i.e., the larger the security key space, the higher the level of security that can be achieved in the scrambled images. A 256x256 grayscale image was used as an example to calculate the possible choices of the security

key(s) as shown in Table II. The results show how the security issue is considered in each scrambling algorithm.

TABLE II. SECURITY KEYS OF THE ALGORITHMS

Scrambling Algorithms Based on	Security Key(s)	Possible choices of the Security Key(s)
Parameter based M-sequence	Shifting times r, the distance parameter p	62985
Fibonacci number	none	none
Generalized Fibonacci number	Initial value a and b, the parameter in transform r	Less than 315
P-Fibonacci sequence	The distance parameter p and the parameter in transform i	Ideally infinite
P-Lucas sequence	The distance parameter p and the parameter in transform i	Ideally infinite
Gray Code	none	none
generalized Gray code	The base q	Less than 16
Generlized P-Gray Code	Base n, the distance parameter p	272
P-recursive sequence	B(n), the distance parameter p	Ideally infinite

The calculation is based on a 256x256 grayscale image

The image scrambling algorithms using Fibonacci number in [1] and Gray Code in [3] don't consider the security issue since they don't have any security key. The parameter q can act as a security key for the algorithm based on generalized Gray Code. However, the security level of this algorithm is still quite low due to the limited number of choices for its security key.

The security issue has been carefully taken into account in the scrambling algorithms based on the P-Fibonacci, P-Lucas, P-recursive sequences and parameter based M-sequence as well. Higher security levels of the scrambled images can be achieved since these algorithms have at lease two security keys and all the security keys have many possible choices.

B. Data Loss Attacks

Data loss attacks are common image attacks. These attacks are to verify the ability of the scrambled images for tolerating the distortions in the public media transmission channels. Consequently, the image scrambling algorithms show great advantages in data loss attacks

Fig. 3 gives an example of cutting attack. A 512x512 Lena image was scrambled by using P-Fibonacci sequence, P-Lucas sequence, P-Gray Code and parameter based M-sequence separately. A 64x64 center cutting attack was applied to these scrambled images. The reconstructed images shown in Fig. 3 are derived from these scrambled images with a cutting attack. These reconstructed images are visually acceptable since they include almost all visual information of the original image.

Fig. 4 shows another example of low pass filter attacks. The Lena image was also scrambled by using the same sequences as those used in Fig.3. These scrambled images were filtered by a 3x3 digital low pass filter, namely the Gaussian low pass filter. The images shown in Fig. 4 were reconstructed from these filtered images. These reconstructed images are obviously recognizable.

The scrambling algorithms based on other sequences also have the similar results as these shown in Fig. 3 and Fig. 4. These experimental results demonstrate that these recursive sequence based image scrambling algorithms show excellent performance in data loss attacks.

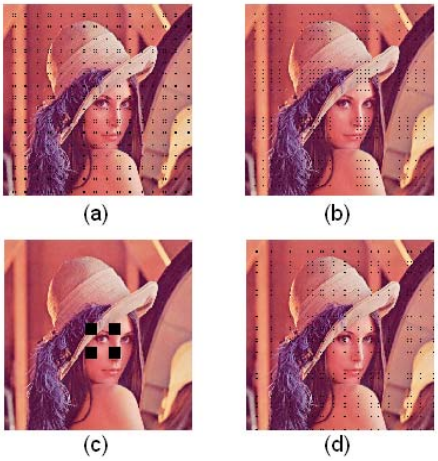

Figure 3. Reconstructed images based on different sequences after a 64x64 center cutting attack, p=2. (a) Reconstructed image based on P-Fibonacci sequence; (b) Reconstructed image based on P-Lucas sequence; (c) Reconstructed image based on P-Gray Code; (d) Reconstructed image based on parameter based M-sequence.

Figure 4. Reconstructed images based on different sequences after a 3x3 Gaussian low pass filter, p=2. (a) Reconstructed image based on P-Fibonacci sequence; (b) Reconstructed image based on P-Lucas sequence; (c) Reconstructed image based on P-Gray Code; (d) Reconstructed image based on parameter based M-sequence.

C. Noise Attacks

There are many different noises in the public media transmission channels such as networks. Noise attacks show the ability of the scrambled images for enduring the noise attacks. This shows another advantage of the image scrambling algorithms.

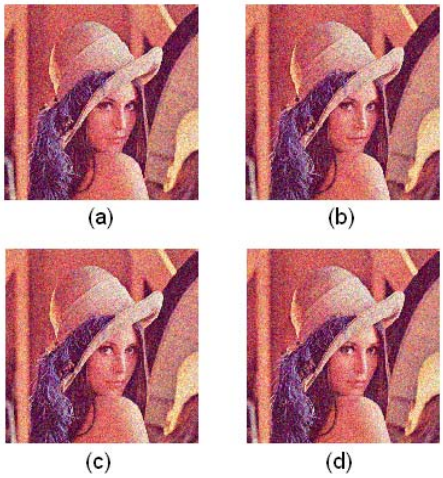

Figure 5. Reconstructed images based on different sequences with 10% Gaussian noise attack, p=2. (a) Reconstructed image based on P-Fibonacci sequence; (b) Reconstructed image based on P-Lucas sequence; (c) Reconstructed image based on P-Gray Code; (d) Reconstructed image based on parameter based M-sequence.

Figure 6. Reconstructed images based on different sequences with 10% Salt Pepper noise attack, p=2. (a) Reconstructed image based on P-Fibonacci sequence; (b) Reconstructed image based on P-Lucas sequence; (c) Reconstructed image based on P-Gray Code; (d) Reconstructed image based on parameter based M-sequence.

The experimental results in Fig. 5 and Fig. 6 show the performance of the scrambling algorithms in noise attacks. A Lena image was scrambled by using the sequences as the same as these used in Fig. 3 and Fig. 4. The scrambled images have an additional 10% Gaussian noise included. The images were recovered from these scrambled images with noise. The recovered images are shown in Fig. 5. The reconstructed images shown in Fig. 6 were obtained from the scrambled images with 10% Salt & Pepper noise.

These reconstructed images contain all the visual information of the original image even though they contain noises. These experimental results demonstrate that the scrambling algorithms also show good performance in the presence of noise attacks. The scrambled images can be reconstructed when subjected to noisy environments.

D. Plaintext Attacks

Theoretically, the scrambled images could be partially or fully decoded by using the plaintext attacks without knowing the security keys or scrambling algorithms. However, this could be accomplished only if the following conditions are satisfied:

1) The attacker can access the encoder which is used to encrypt images, or he/she can obtain enough ciphertexts and the corresponding plaintexts.

2) Security keys of the encoder should not change during the time when the attacker decodes the encrypted images.

3) The number of image pixels with the same value in a plaintext is minimized.

4) The size of all plaintexts and their ciphertexts are identical.

Here is an example of the chosen-plaintext attack. In order to break a 256×256 image encrypted by a certain scrambling algorithm, we introduce a matrix (1) as a plaintext which can show position changes of all image pixels after it is scrambled by the algorithm.

$$X = \{x(i, j) = i + \tfrac{j}{1000} \text{ for } 1 \le i, j \le 256\}$$

Or

$$X = \begin{bmatrix} 1.001 & 1.002 & \dots & 1.256 \\ 2.001 & 2.002 & \dots & 2.256 \\ \dots & \dots & \dots & \dots \\ 256.001 & 256.002 & \dots & 256.256 \end{bmatrix} \quad (1)$$

For the equations above, we can see that each pixel value is unique and corresponds to its location. For example, pixel value 3.002 refers to the third row and the second column. After the plaintext X is scrambled into a new matrix Y, which is used as the index matrix for attacks, all pixel positions in X are changed to new positions in Y. The encrypted images can be broken by searching the locations of all pixel value in the matrix Y. For example, find the new location of 1.001 in Y, pick the pixel value with the same location from the encrypted image, and put it in the first row and the first column in the new matrix named the broken image, on so on. In this manner, the broken image will be the same as the original image after all 256×256 pixels are found. As a result, the encrypted image is completely broken without any security key or knowing the scrambling algorithm.

All conditions above are extremely important for the plaintext attacks. No scrambled image could be decrypted by plaintext attacks without the first condition. The attacker should try all possible cases of the security keys if the second

condition were not satisfied. The quality of the images decrypted by using plaintext attacks depends on the third and fourth conditions if the first condition could be satisfied. However, it is much difficult to make all these requirements satisfied simultaneously.

IV. Execution Time Analysis

The execution time can show how efficiently the algorithms scramble images. This property is to evaluate the scrambling algorithm's suitability for real-time applications.

TABLE III. Execution Time of the Algorithms

The Scrambling Algorithms Based on	Scrambling Time (second)	Unscrambling Time (second)
Parameter based M-sequence	7.4808	7.6158
Fibonacci number	0.0173	0.0246
Generalized Fibonacci number	0.0207	0.025
Gray Code	2.4121	2.4131
generalized Gray code	2.2769	2.2765
P-Fibonacci sequence	0.1665	0.3624
P-Lucas sequence	0.125	0.2701
Generlized P-Gray Code	2.5522	2.6841
P-recursive sequence	0.9479	1.1055

The measurement is based on a 512x512 grayscale image

Table III shows the execution time using the scrambling algorithms based on the different sequences. The results were measured in a computer working Windows XP operation system with 3GB memory and CPU using Intel Core Duo E6550 (2.60GHz, 4MB L2 cache, 1066 MHz FSB).

The scrambling time was measured when a 512x512 grayscale image was scrambled by applying the different sequences one time separately. The unscrambling time was also measured by applying a one-time unscrambling process to the scrambled images using the same sequences.

From the measure results in Table III, the scrambling algorithm based on Fibonacci number has the shortest execution time in both the scrambling process and the unscrambling process. The algorithms based on Generalized Fibonacci, P-Fibonacci and P-Lucas can also scramble images more efficiently. The scrambling algorithm using parameter based M-sequence takes the longest time to performance one scrambling/unscrambling process. This is because it takes most of the process time for the serial shift registers to generate the M-sequence. This can be improved by using parallel shift registers to generate M-sequence instead of the serial shift registers.

V. Conclusion

We analyzed and compared the security issue and execution time of the image scrambling algorithms based on several recursive sequences. They include the Fibonacci number, Generalized Fibonacci number, Gray Code, P-Gray Code, P-Fibonacci, P-Lucas, and P-recursive sequences, and the parameter based M-sequence as well. The security issue contains the space of security keys, data loss attacks, noise attacks and plaintext attacks. A chosen-plaintext matrix has been introduced as an example for the plaintext attacks.

The experimental results show that the scrambling algorithms based on both the P-Fibonacci and P-Lucas sequences have better performance in overall analysis. They can scramble images more efficiently and they can also protect images with higher security levels due to their larger space of security keys. These also demonstrate that they are well suitable for the real-time applications.

References

[1] J. Zou, R. K. Ward, and D. Qi, "A new digital image scrambling method based on Fibonacci numbers," in *2004 IEEE International Symposium on Circuits and Systems*, 2004, pp. III-965.

[2] J. Zou, R. K. Ward, and D. Qi, "The Generalized Fibonacci Transformations and Application to Image Scrambling," in *2004 IEEE International Conference on Acoustics, Speech, and Signal Processing* 2004, pp. 385-388.

[3] W. Ding, W. Yan, and D. Qi, "Digital Image Scrambling," *Progress in Natural Science,* vol. 11, p. 7, 2000.

[4] J. Zou, and R. K. Ward, "Introducing two new image scrambling methods," in *2003 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing* 2003, pp. 708-711.

[5] Y. Zhou, S. Agaian, V. Joyner and K. Panetta, "Two Fibonacci P-code Based Image Scrambling Algorithms " in *2008 SPIE Electronic Imaging*, San Jose, CA, 2008, p. 681215.

[6] Y. Zhou, K. Panetta, and S. Agaian, "Partial Multimedia Encryption with Different Security Levels," in *2008 IEEE Conference on Technologies for Homeland Security*, Waltham, MA, 2008.

[7] Y. Zhou, K. Panetta and S. Agaian, "P-recursive sequence and key-dependent multimedia scrambling," in *2008 SPIE Defense and Security Symposium on Mobile Multimedia/Image Processing for Military and Security Applications*, Orlando, FL USA 2008, p. 69820H.

[8] Y. Zhou, K. Panetta, and S. Agaian, "An Image Scrambling Algorithm Using Parameter Based M-sequence," in *2008 International Conference on Machine Learning and Cybernetics*, Chunming, China, 2008.

[9] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone *Handbook of Applied Cryptography*. New York: CRC Press, Inc., 1997.

[10] S. Li, C. Li, G. Chen, N. G. Bourbakis and K.T. Lo, "A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Processing: Image Communication* vol. 23, pp. 212-223, 2008.

[11] T. Koshy, "Fibonacci and Lucas Numbers with Applications," Wiley-Interscience, 2001.