P-recursive Sequence and key-dependent Multimedia Scrambling

Yicong Zhou*[a], Karen Panetta[a], Sos Agaian[b]
[a] Department of Electrical and Computer Engineering, Tufts University, Medford, MA 02155
[b] Department of Electrical and Computer Engineering, The University of Texas at San Antonio, San Antonio, TX 78249

ABSTRACT

Multimedia scrambling technologies ensure that multimedia content is only used by authorized users by transforming multimedia data into an unintelligible format. This paper introduces a new P-recursive sequence and two multimedia scrambling algorithms based on the P-recursive sequence. The P-recursive sequence is a more generalized sequence which can derive many well-known sequences such as the P-Fibonacci sequence, the P-Lucas sequence and P-Gray code. The algorithms can be used to scramble two or three dimensional multimedia data in one step. Electronic signatures, grayscale images and three-color-component images are all examples of 2-D & 3-D multimedia data which can utilize these algorithms. Furthermore, a security key parameter p may be chosen as different or the same values for each dimensional component of the multimedia data. Experiments show that the presented algorithms can scramble multimedia data at different levels of security by partially or fully encrypting multimedia data. They also have been demonstrated in the experiments to show good performance in known-plain text attack and common image attacks such as data loss, Gaussian noise, and Salt Pepper noise. The scrambled multimedia data can be completely reconstructed only by using the correct security keys.

Keywords: multimedia scrambling, P-recursive sequence, P-Fibonacci sequence, P-Lucas sequence, P-Gray Code.

1. INTRODUCTION

Multimedia and digital communication technologies provide many different opportunities and approaches for people all over the world to share, transmit and access the information and data such as network and mobile phone[1]. As a result, security of image and video data becomes a key issue for consumers, companies and governments in many areas, such as video-on-demand, confidential remote video conferencing, security communication, and also in military applications. Multimedia scrambling (i.e., encryption) technologies are very useful tools to ensure that multimedia data is only used by authorized users by transforming the multimedia data into an unrecognizable format.

Several interesting image scrambling approaches have been developed recently. Zou et al. [2]use the classical Fibonacci number to scramble images. Gu et al. [3] present a chaos scrambling method in the wavelet domain. Zou et al. [4] also introduce image scrambling algorithms based on the 3-D Arnold and generalized Gray Code transforms. These developments have their particular contributions for image scrambling. However, much more work needs to be done to improve the security of multimedia data such as copyright violation and distribution of digital media, network security, and secret communications etc.

In our previous work, we developed two image scrambling algorithms based on a P-Fibonacci sequence [5]. In this paper, we introduce a new P-recursive sequence and also two multimedia scrambling algorithms based on this P-recursive sequence. The P-recursive sequence and its transforms will be introduced in the second section. This sequence can generate many familiar sequences under different initial conditions and p values, such as P-Fibonacci sequence, P-Lucas sequence, P-Gray Code, and some classical sequences as well. The multimedia scrambling algorithms based on the P-recursive sequence are to be introduced in the third section. They can scramble 2-D or 3-D multimedia data in one step. In the fourth section, some experimental results will be given to show the algorithms are straightforward processes. This also makes them suitable for real-time applications including speech and video signals. A parameter p, which can be used as one of the security-keys, may be chosen as the same or different values for each dimensional component of the multimedia data.

* Yicong.Zhou@tufts.edu; phone 1 617-627-5183; fax 1 617-627-3220;

Mobile Multimedia/Image Processing, Security, and Applications 2008
edited by Sos S. Agaian, Sabah A. Jassim, Proc. of SPIE Vol. 6982
69820H, (2008) · 0277-786X/08/$18 · doi: 10.1117/12.777744

2. P-recursive sequence and its transforms

A new P-recursive sequence and its transforms are introduced in this section. Under different conditions, it can yield many different sequences such as the P-Fibonacci sequence, the P-Lucas sequence and P-Gray Code and also the classical Fibonacci number, the classical Lucas number and Gray Code. A few transforms are needed to apply the P-recursive sequence to multimedia scrambling.

2.1. P-recursive sequence

Definition 2.1: The P-recursive sequence is defined as,

$$R(n)=\begin{cases}0 & n\le 0\\ B(n) & 0<n\le p+1\\ R(n-1)*R(n-p-1) & n>p+1\end{cases} \tag{1}$$

where p is a nonnegative integer, and

$$*=\begin{cases}+ & \text{B(n) is integer}\\ \oplus & \text{B(n) is binary}\end{cases}$$

From the definition above, the P-recursive sequences differ based on the different B(n) and p values.

If B(n) is integer, the "*" is the arithmetic addition operation.

(1) If $B(1)=1$ and $B(n)=1$ for $1<n\le p+1$, the P-recursive sequence is P-Fibonacci sequence[5-7].

$$R(n)=\begin{cases}0 & n\le 0\\ 1 & n=1\\ 1 & 1<n\le p+1\\ R(n-1)*R(n-p-1) & n>p+1\end{cases} \tag{2}$$

(2) If $B(1)=2$ and $B(n)=1$ for $1<n\le p+1$, the P-recursive sequence is P-Lucas sequence[5].

$$R(n)=\begin{cases}0 & n\le 0\\ 2 & n=1\\ 1 & 1<n\le p+1\\ R(n-1)*R(n-p-1) & n>p+1\end{cases} \tag{3}$$

If B(n) is binary, the "$\oplus$" is the mod 2 operation (XOR).

(3) If $B(n)$ is a binary sequence, the P-recursive sequence $R(n)$ is P-Gray Code representation of the binary sequence $B(n)$.

$$R(n)=\begin{cases}0 & n\le 0\\ B(n) & 0<n\le p+1\\ B(n-1)\oplus B(n-p-1) & n>p+1\end{cases} \tag{4}$$

Furthermore, many of the classical sequences can be derived from the functions (2), (3) and (4) based on different p values. For example, the binary sequence and the classical Fibonacci number can be derived from the function (2), P-Fibonacci number, when p=1 [5].

2.2. P-recursive Transforms

Definition 2.2 Let $R(n)$ and $R(n+1)$ be two consecutive P-recursive elements. The following transformation is called **the P-recursive Transform** [5].

$$T(k) = k[R(n) + i] \bmod R(n+1) \tag{5}$$

Where $k = 0,1,...,N$, $R(n)+i < R(n+1)$, $N = R(n+1)-1$ and i is an integer.

For a certain B(n) and p value in the definition above, the output sequence $\{T(1),T(2),T(3),...,T(N)\}$ of the P-recursive transform should be the permutation of an input sequence $k = \{0,1,...,N\}$.

In order to scramble an $M \times N$ multimedia data in one step, the row coefficient matrix of the multimedia data is generated as

$$T_r(i,j) = \begin{cases} 1 & (i,T(i)) \\ 0 & else \end{cases} \tag{6}$$

Where $1 \le i, j \le M$

Similarly, the column coefficient matrix of the multimedia data is also generated as

$$T_c(x,y) = \begin{cases} 1 & (T(y),y) \\ 0 & else \end{cases} \tag{7}$$

Where $1 \le x, y \le N$

Definition 2.3: Let A be a 2-D multimedia data matrix, T_r be the row coefficient matrix defined by function (6), and T_c be the column coefficient matrix defined by function (7). The following transformation is called the **2-D P-recursive Transform** [5]:

$$S = T_r A T_c \tag{8}$$

Where S is the scrambled image matrix and

Definition 2.4: Let S be the scrambled 2-D multimedia data matrix, T_r^{-1} be the inverse row coefficient matrix defined by function (6), and T_c^{-1} be the inverse column coefficient matrix defined by function (7). The following transformation is called the **2-D Inverse P-recursive Transform** [5]:

$$R = T_r^{-1} S T_c^{-1} \tag{9}$$

where R is the reconstructed image matrix.

Definition 2.5: Let $D = (D_i \quad i)$ be a 3-D multimedia data matrix, where D_i is the 2-D data matrix of the i[th] multimedia component. $T_r = (T_{ri} \quad i)$, where T_{ri} is the row coefficient matrix for the i[th] multimedia component defined by function (6). $T_c = (T_{ci} \quad i)$, where T_{ci} is the column coefficient matrix of the i[th] multimedia component defined by function (7). The following transformation is called the **3-D P-recursive Transform**.

$$E = T_r D T_c \tag{10}$$

Where E is the matrix of the scrambled 3-D multimedia data, and $i = 1,2,3$.

Definition 2.6: Let $E = (E_i \quad i)$ be a scrambled 3-D multimedia data matrix, where E_i is the scrambled 2-D data matrix of the i[th] multimedia component. $T_r^{-1} = (T_{ri}^{-1} \quad i)$, where T_{ri}^{-1} is the inverse row coefficient matrix of the i[th] multimedia

component. $T_c^{-1} = (T_{ci}^{-1} \quad i)$, where T_{ci}^{-1} is the inverse column coefficient matrix of the i[th] multimedia component. The following transformation is called the **Inverse 3-D P-recursive Transform**.

$$R = T_r^{-1} E T_c^{-1} \tag{11}$$

Where R is the reconstructed 3-D multimedia data, and $i = 1, 2, 3$.

3. Multimedia scrambling algorithms

In order to scramble multimedia data in one step, two scrambling algorithms are introduced in this section. One is based on the 2-D P-recursive Transform; the other uses the 3-D P-recursive Transform. Their corresponding unscrambling algorithms are also presented. The presented algorithms are lossless encryption approaches since they change the physical positions of multimedia data instead of changing multimedia content. The 1-D P-recursive Transform can be used to scramble one dimension multimedia data such as string, text, password and speech signals. Due to space limitation, we will not discuss the applications of the 1-D P-recursive transform in this paper.

3.1. Multimedia scrambling algorithm based on the 2-D P-recursive Transform

The 2-D P-recursive Transform can be used to scramble the multimedia data with a 2-D data matrix such as electronic signatures, binary images and grayscale images. The scrambling algorithm is shown in Figure 1. Based on the definition of 2-D P-recursive transform (definition 2.3), the 2-D multimedia data can be scrambled only in one step by applying the row and column coefficient matrices at the same time. This algorithm can also be applied to the monochrome image and black video.

To scramble the 2-D multimedia data, the B(n) and p security keys should be determined. Certain B(n) and p values determine which kind of sequence, such as P-Fibonacci sequence, P-Lucas sequence, or P-Gray Code, will be used to scramble the 2-D multimedia data. The row and column coefficient matrices can be calculated by using equation (5), (6) and (7). The scrambled 2-D multimedia data can be generated by applying the two coefficient matrices to the 2-D multimedia data based on the definition 2.3.

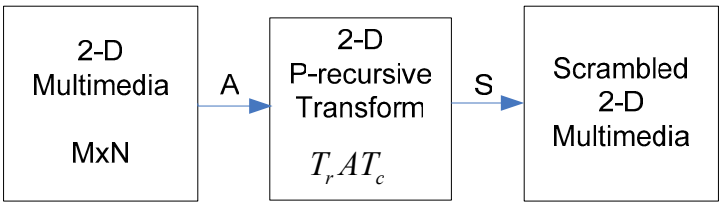

Fig. 1: Block diagram of the Multimedia scrambling algorithm based on the 2-D P-recursive Transform.

3.2. Multimedia unscrambling algorithm based on the Inverse 2-D P-recursive Transform

The 2-D Multimedia unscrambling is also a straightforward one step process as shown in Figure 2. The security keys should be provided to the authorized users to reconstruct the original 2-D multimedia data. The inverse row and column coefficient matrices can be generated by using the security keys: B(n) and p value according to the equation (5), (6) and (7). The original 2-D multimedia data can be reconstructed by applying the inverse P-recursive Transform to the scrambled 2-D multimedia data.

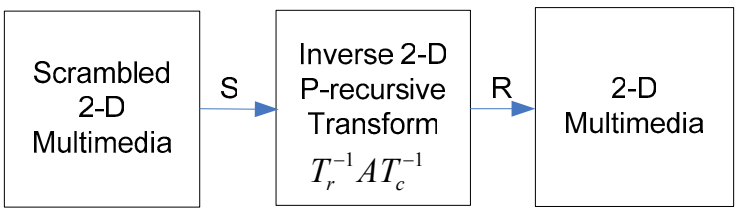

Fig. 2: Block diagram of the Multimedia unscrambling algorithm based on the Inverse 2-D P-recursive Transform.

3.3. Multimedia scrambling algorithm based on the 3-D P-recursive Transform

The 3-D multimedia data is widely used in many areas such as internet and television. Color images, for example, have 3-D data matrices for the three color planes. Each color plane is a 2-D data matrix. The 3-D P-recursive Transform can be used to scramble such 3-D multimedia data in one step (as shown in Figure 3).

The B(n) and p value as the security keys should be chosen to determine which sequence will be used to scramble the 3-D multimedia data. The same sequences are chosen for all three components of the 3-D multimedia data. Of course, the users can choose the different sequences for the three different components of the 3-D multimedia data. The row and column coefficient matrices can be calculated based on the chosen security keys.

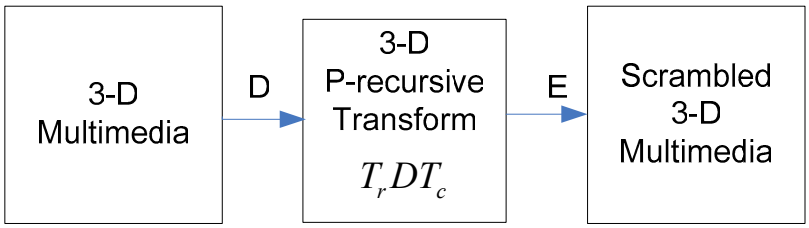

Fig. 3: Block diagram of the image scrambling algorithm based on 3-D P-recursive Transform.

3.4. Multimedia unscrambling algorithm based on the Inverse 3-D P-recursive Transform

For the authorized user to reconstruct the original 3-D multimedia data, the security keys are used to calculate the inverse row and column coefficient matrices. The inverse 3-D P-recursive Transform is applied to the scrambled 3-D multimedia data to recover the original 3-D multimedia data (as shown in Figure 4).

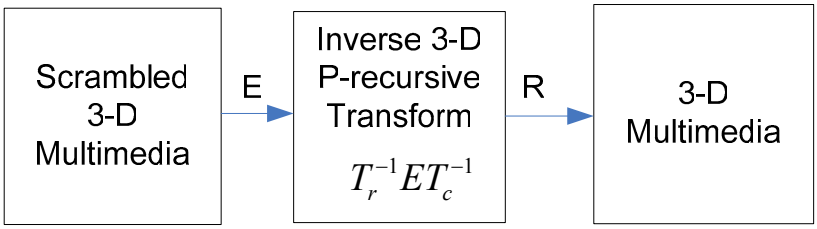

Fig. 4: Block diagram of the image unscrambling algorithm based on the Inverse 3-D P-recursive Transform.

4. Experimental results and security analysis

The presented algorithms have been implemented on many sample multimedia data such as electronic signatures, medical images, binary images, grayscale images, and color images. To show their performance in scrambling 2-D and 3-D multimedia data, some scrambled results are provided as examples in this section.

4.1. Experimental results for 2-D multimedia scrambling

The 2-D scrambling algorithm is very suitable for scrambling 2-D multimedia data since both of them are 2-D matrices. The certain sequence can be determined by security keys. The scrambled and reconstructed results of the binary image, electronic signatures and grayscale images are shown in Figure 5, 6 and 7 separately. These 2-D multimedia data are perfectly reconstructed from the scrambled multimedia data. This demonstrates that the algorithm is a lossless encryption method. The multimedia data can be fully encrypted when the P-Fibonacci sequence or P-Lucas sequence is selected by security keys. Furthermore, they can also be partially encrypted when P-Gray Code is chosen. The higher p value is the less part of the multimedia data encrypted. This can be demonstrated from the scrambled results in Figure 8. The scrambled images differ based on different p values or different sequences.

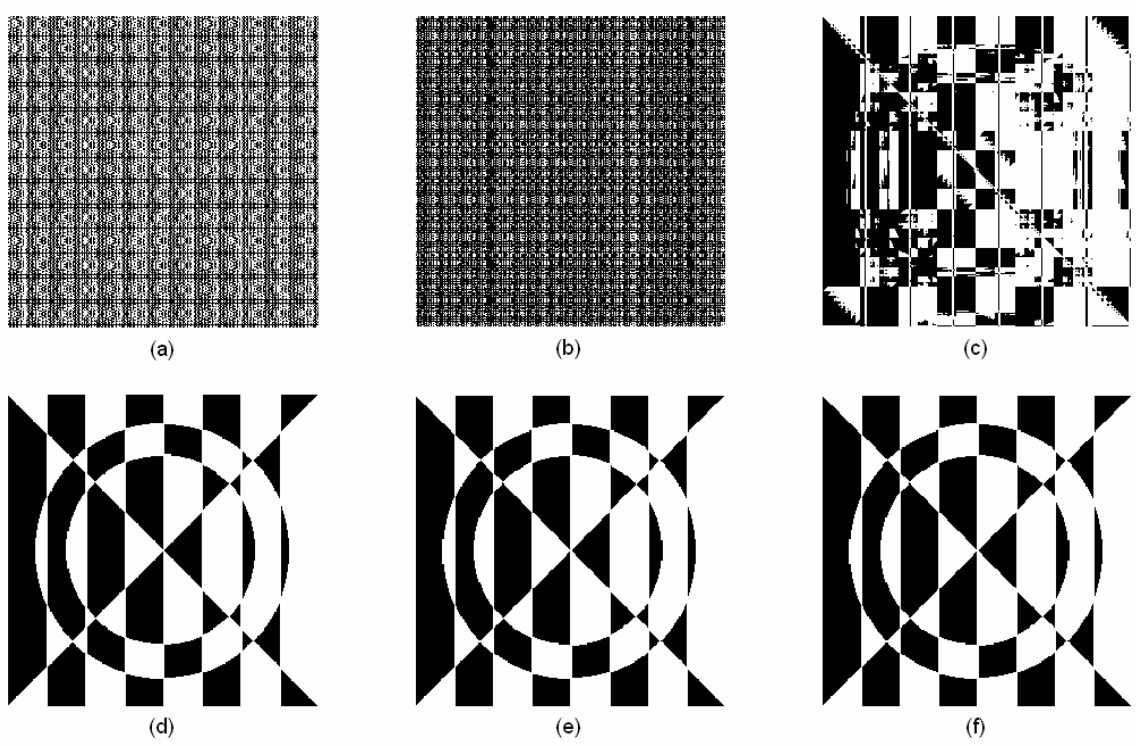

Fig. 5: Scrambled and reconstructed **binary images** based on different sequences, p=2. (a) Scrambled binary image using P-Fibonacci sequence; (b) Scrambled binary image using P-Lucas sequence; (c) Scrambled binary image using P-Gray Code; (d) reconstructed image from (a); (e) reconstructed image from (b); (f) reconstructed image from (c).

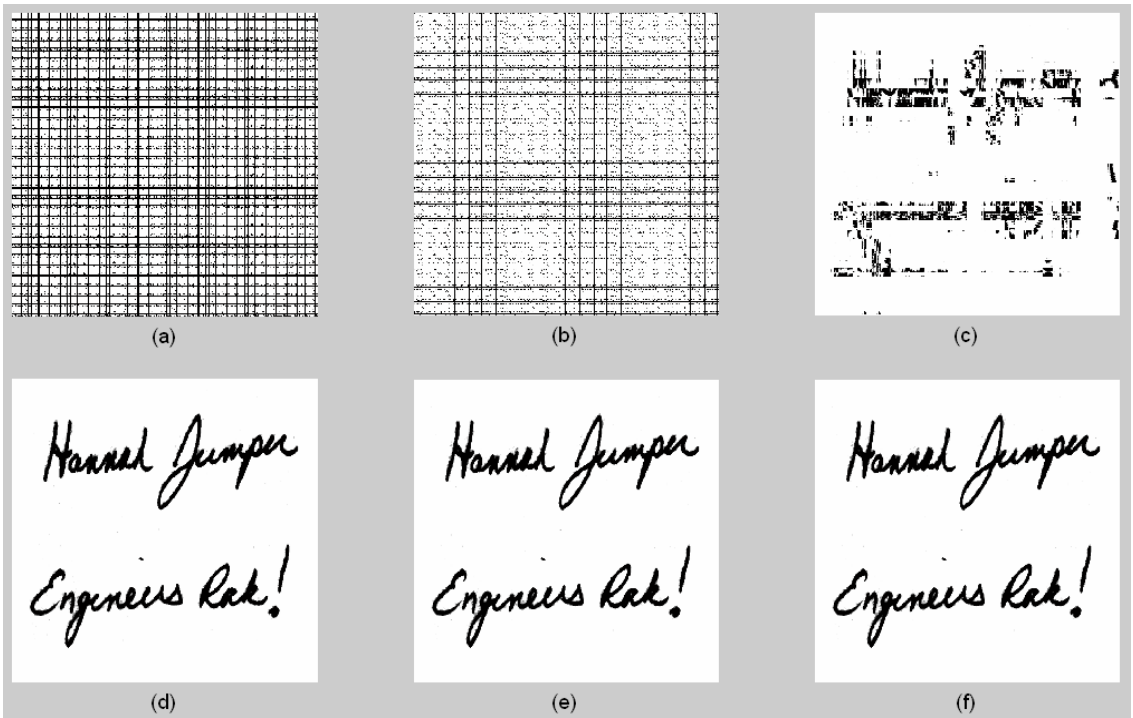

Fig. 6: Scrambled and reconstructed **electronic signatures** based on different sequences, p=2. (a) Scrambled signature using P-Fibonacci sequence; (b) Scrambled signature using P-Lucas sequence; (c) Scrambled signature using P-Gray Code; (d) reconstructed signature from (a); (e) reconstructed signature from (b); (f) reconstructed signature from (c)

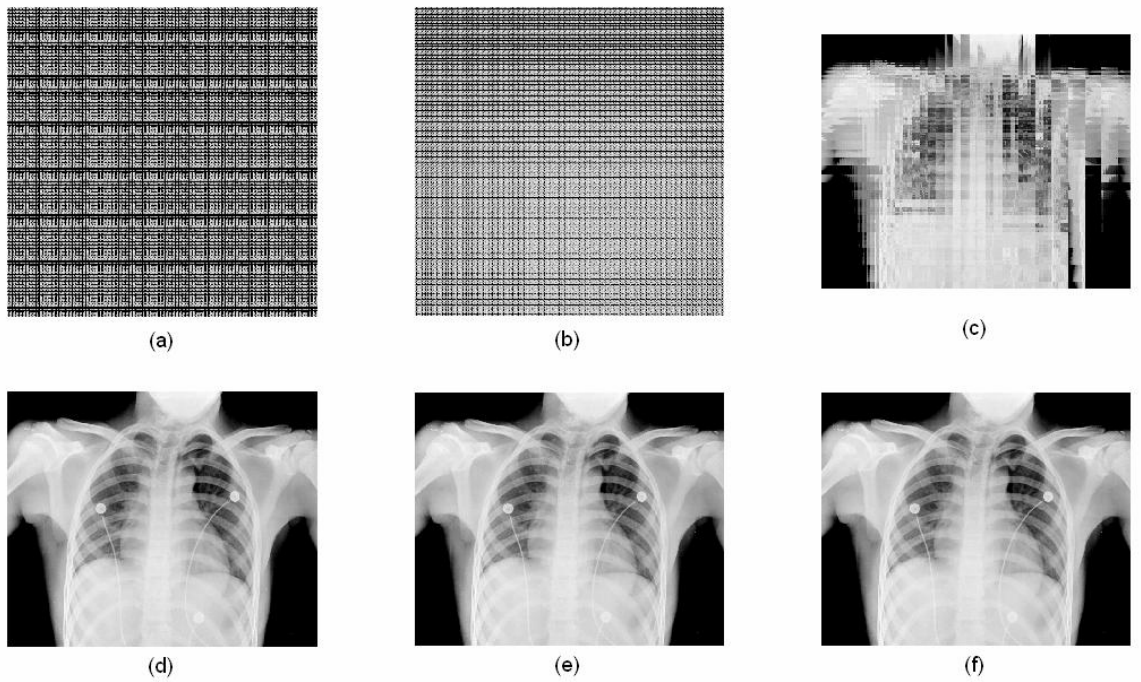

Fig. 7: Scrambled and reconstructed **medical images** based on different sequences, p=2. (a) Scrambled medical image using P-Fibonacci sequence; (b) Scrambled medical image using P-Lucas sequence; (c) Scrambled medical image using P-Gray Code; (d) reconstructed image from (a); (e) reconstructed image form (b); (f) reconstructed image form (c)

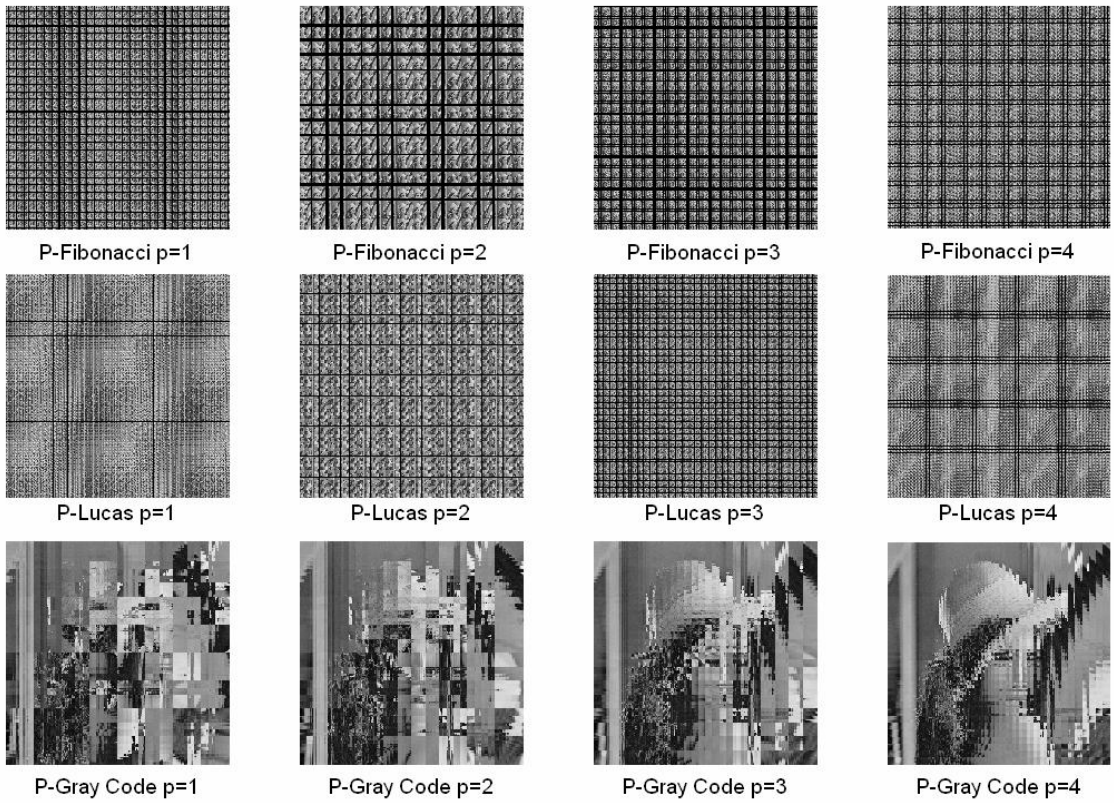

Fig. 8: Scrambled grayscale Lena images based on different sequences and p values.

4.2. Experiment results for 3-D multimedia scrambling

The color image as an example of 3-D multimedia was scrambled by different sequences and p values. The original images can be completely reconstructed from the scrambled images without any distortion, as shown in Figure 9 (d), (e), (f). This further proves that the 3-D scrambling algorithm is also a lossless approach. The scrambled images look like nature images as shown in Figure 10. When the sequences and p values are different, the images are visually different.

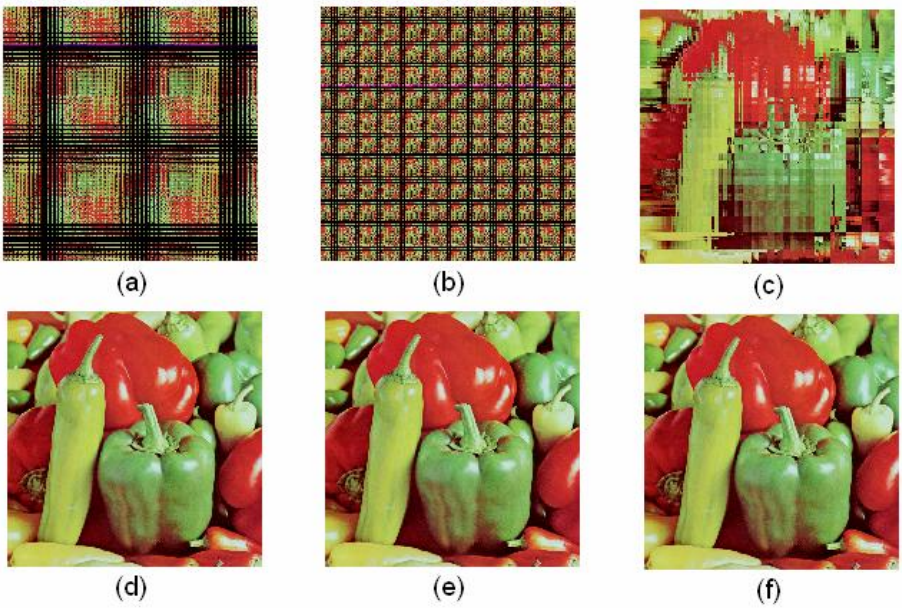

Fig. 9: Scrambled and reconstructed **color images** based on different sequences, p=3. (a) Scrambled color image using P-Fibonacci sequence; (b) Scrambled color image using P-Lucas sequence; (c) Scrambled color image using P-Gray Code; (d) reconstructed image from (a); (e) reconstructed image from (b); (f) reconstructed image from (c)

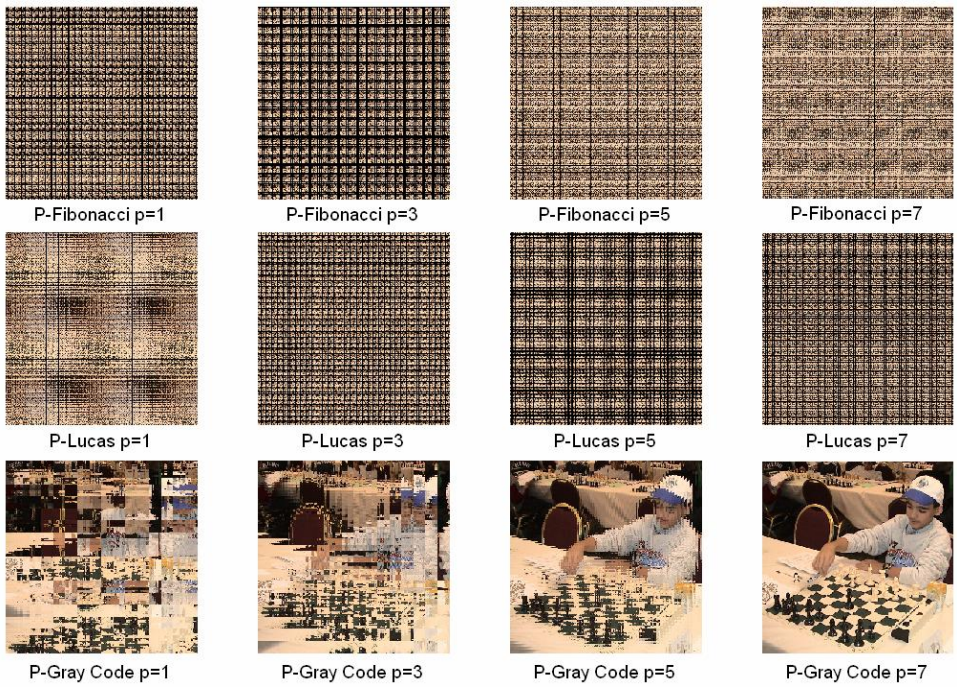

Fig. 10: Scrambled color image with different sequences and p values.

4.3. Security analysis

To show the presented algorithms can tolerate the common attacks, we apply a cutting (data loss) attack, Gaussian noise and Salt Pepper noise to the scrambled color images, and then reconstruct the original images which are shown in Figure 11, 12, and 13. The results demonstrate that the algorithms have good performance for common attacks. The reconstructed images show almost all visual information of the original images even if there are some distortions in the images due to the attacks.

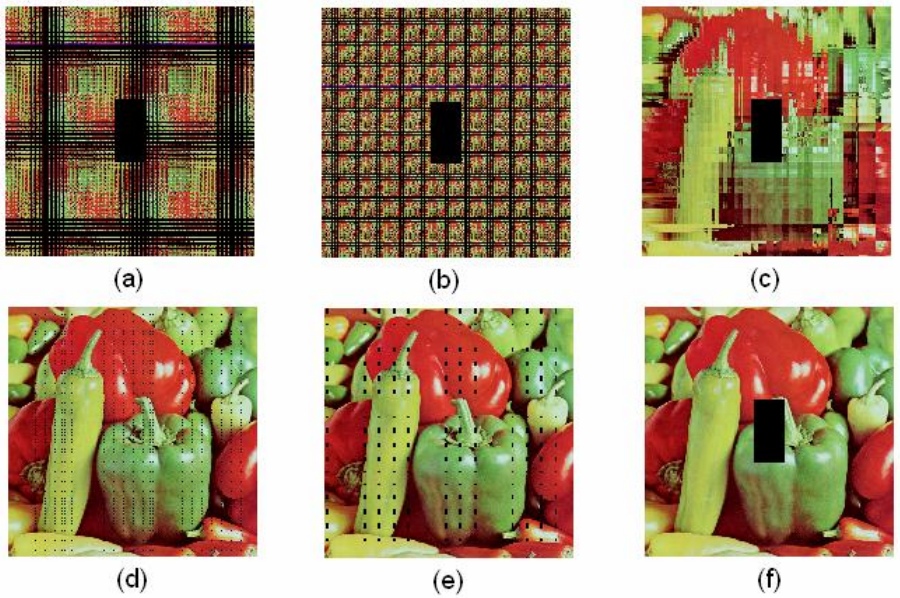

Fig. 11: Scrambled and reconstructed **color images** based on different sequences with a **128x64 cutting attack**, p=3. (a) Scrambled color image using P-Fibonacci sequence with a cutting attack; (b) Scrambled color image using P-Lucas sequence with a cutting attack; (c) Scrambled color image using P-Gray Code with a cutting attack; (d) reconstructed color image from (a); (e) reconstructed color image from (b); (f) reconstructed color image from (c).

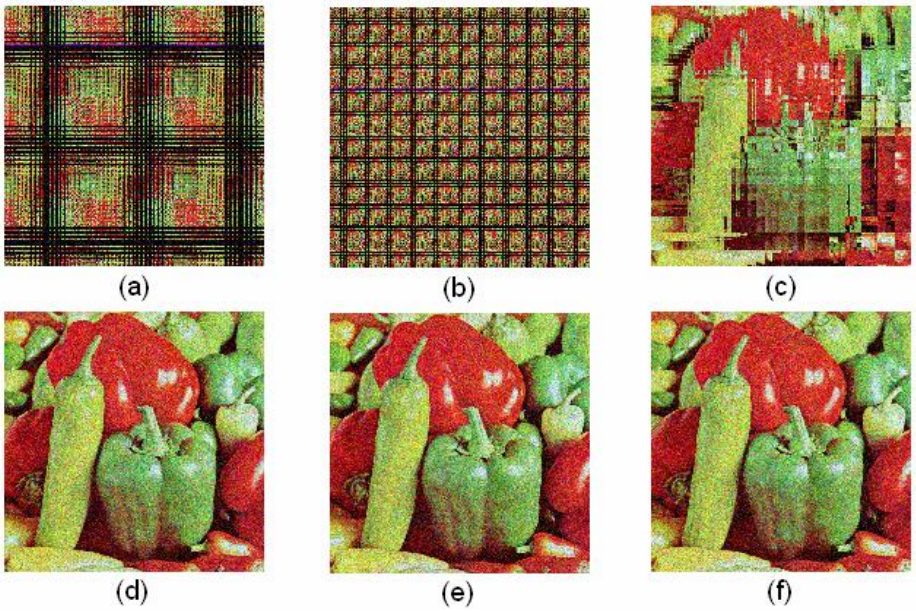

Fig. 12: Scrambled and reconstructed **color images** based on different sequences **with 12.5% Gaussian noise attack**, p=3. (a) Scrambled color image using P-Fibonacci sequence with Gaussian noise; (b) Scrambled color image using P-Lucas sequence with Gaussian noise; (c) Scrambled color image using P-Gray Code with Gaussian noise; (d) reconstructed color image from (a); (e) reconstructed color image from (b); (f) reconstructed color image from (c).

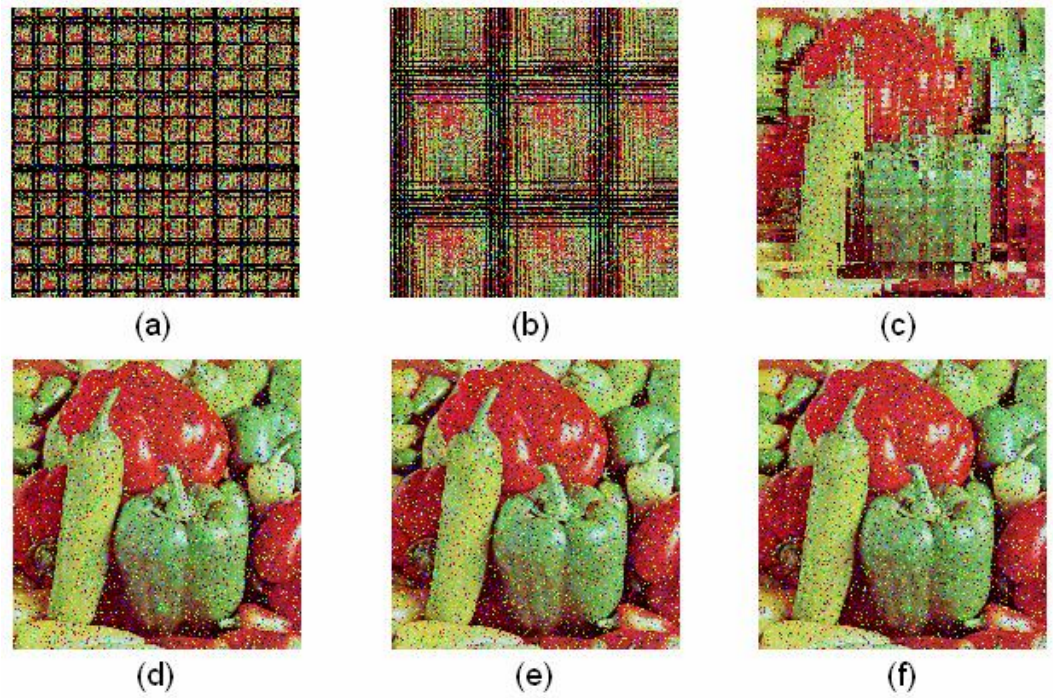

Fig. 13: Scrambled and reconstructed **color images** based on different sequences **with 10% Salt Pepper noise attack,** p=3. (a) Scrambled color image using P-Fibonacci sequence with Salt Pepper noise; (b) Scrambled color image using P-Lucas sequence with Salt Pepper noise; (c) Scrambled color image using P-Gray Code with Salt Pepper noise; (d) reconstructed color image from (a); (e) reconstructed color image from (b); (f) reconstructed color image from (c).

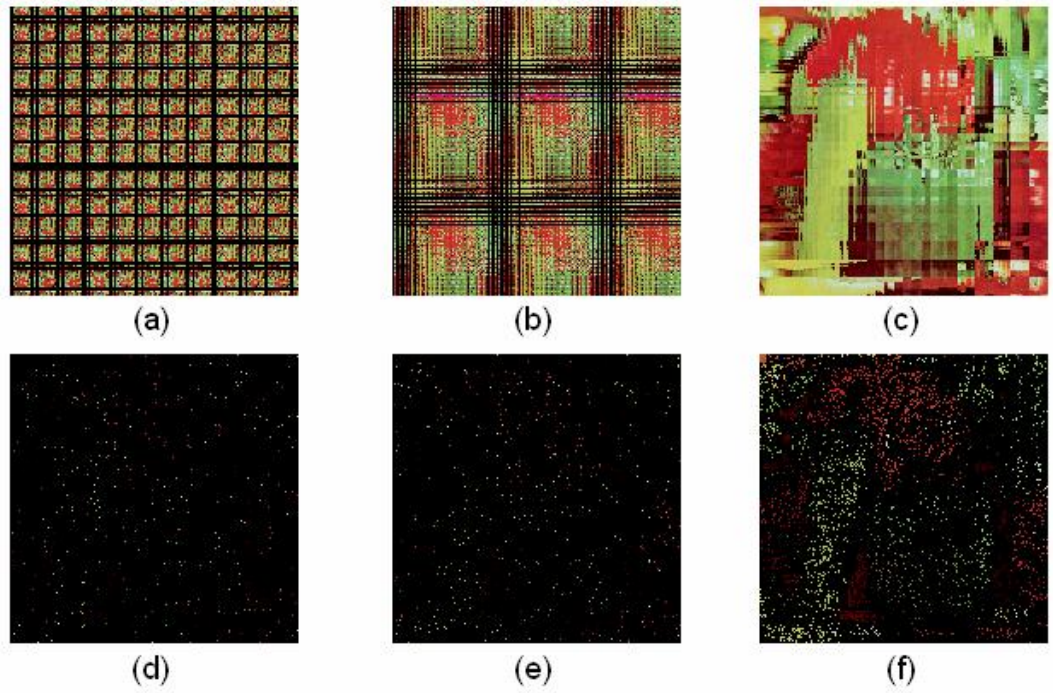

Fig. 14: Scrambled color images based on different sequences, p=3, and reconstructed **color images with Known-plain Text attack**. (a) Scrambled color image using P-Fibonacci sequence; (b) Scrambled color image using P-Lucas sequence; (c) Scrambled color image using P-Gray Code; (d) reconstructed color image from (a); (e) reconstructed color image from (b); (f) reconstructed color image from (c).

Li et al. developed a cryptanalysis approach for permutation-only multimedia encryption based on the known-plain text attack [8]. We decoded the scrambled images by applying their algorithm. The experimental results as shown in Figure 14 demonstrate that the original image cannot be recovered. Furthermore, we reconstruct the scrambled images by using different security keys as shown in Figure 15. The experimental results show that the scrambled images can be completely reconstructed only by using the right security keys. This verifies the presented algorithms can encrypt multimedia with high security level since the encrypted multimedia data is extremely difficult to decode for unauthorized users.

Fig. 15: The scrambled color images with p=1 and **the reconstructed color images using the same sequence but different p values** (1) Scrambled color image using P-Fibonacci sequence with p=1; (2) The reconstructed color image of (1) using P-Fibonacci sequence with p=1; (3) The reconstructed color image of (1) using P-Fibonacci sequence with p=2; (4) The reconstructed color image of (1) using P-Fibonacci sequence with p=3; (5) Scrambled color image using P-Lucas sequence with p=1; (6) The reconstructed color image of (5) using P-Lucas sequence with p=1; (7) The reconstructed color image of (5) using P-Lucas sequence with p=2; (8) The reconstructed color image of (5) using P-Lucas sequence with p=3; (9) Scrambled color image using P-Gray Code with p=1; (10) The reconstructed color image of (9) using P-Gray Code with p=1; (11) The reconstructed color image of (9) using P-Gray Code with p=2; (12) The reconstructed color image of (9) using P-Gray Code with p=3.

5. Conclusion

We introduce a new P-recursive sequence that can generate multiple classical sequences such as P-Fibonacci sequence, P-Lucas sequence, P-Gray code, and classical Fibonacci number, Lucas number, Gray code as well. We also introduce two multimedia scrambling algorithms that are capable of choosing different sequence to encode multimedia data with different security levels. The multimedia data can be protected via either partial encryption or full encryption to meet different applications with special security requirements. The straightforward one step process required for scrambling or unscrambling is an attractive feature. The algorithms can allow different sequences with different security keys to be used on any multimedia component, which demonstrates the algorithms' flexibility. The experimental results show the algorithms have good performance in known-plain text attack and the common media attacks such as cutting (data loss),

Gaussian noise and Salt Pepper noise. The scrambled multimedia data can be only decoded by using the right security keys. Since the algorithms have low complexity, they are suitable for real-time applications such as those utilizing speech and video signals.

REFERENCES

[1] Yinian Mao and Min Wu, "A Joint Signal Processing and Cryptographic Approach to Multimedia Encryption," *IEEE Transactions on Image Processing,* vol. 15, p. 15, July 2006.

[2] Jiancheng Zou, Rabab K. Ward and Dongxu Qi, "A new digital image scrambling method based on Fibonacci numbers," in *ISCAS 2004*, 2004, pp. III-965.

[3] Guosheng Gu and Guoqiang Han, "The application of chaos and DWT in image scrambling," in *Proceedings of the 5th International conference on Machine Learning and Cybernetics*, Dalian, 2006, pp. 3729-3733.

[4] Jiancheng Zou and Rabab K. Ward, "Introducing two new image scrambling methods," in *Proc. IEEE PacRim Conf. Comm. , Comp., and Sig. Proc.*, 2003, pp. 708-711.

[5] Yicong Zhou, Sos Agaian, Valencia Joyner and Karen Panetta, "Two Fibonacci P-code Based Image Scrambling Algorithms " in *SPIE Electronic Imaging 2008* San Jose, 2008.

[6] S. Agaian, J. Astola, K. Egiazarian and P. Kuosmanen, "Decompositional methods for stack filtering using Fibonacci p-codes," *Signal Processing,* vol. 41, p. 10, 1995.

[7] David Z. Gevorkian, Karen O. Egiazarian and S. Agaian, "Parallel Algorithms and VLSI Architectures for Stack Filtering Using Fibonacci p-Codes," *IEEE Transactions on Signal Processing,* vol. 43, pp. 286-295, 1995.

[8] Shujun Li, Chengqing Li, Guanrong Chen, Nikolaos G. Bourbakis and Kwok-Tung Lo, "A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Processing: Image Communication* vol. 23, 2008.