Stream cipher based on pseudorandom number generation with optical affine transformation

Toru Sasaki, Hiroyuki Togo, Jun Tanida, and Yoshiki Ichioka

We propose a new, to our knowledge, stream cipher technique for two-dimensional (2-D) image data that can be implemented by iterative optical transformation. The stream cipher uses a pseudorandom number generator (PRNG) to generate a pseudorandom bit sequence. The proposed method for the PRNG is composed of the iterative operation of 2-D affine transformation achieved by optical components and by modulo-n addition of the transformed images. We expect efficient execution of the method by optical parallel processing. We verify the performance of the proposed method in terms of security strength and clarify problems on optical implementation by the optical fractal synthesizer.

OCIS codes: 100.1160, 200.3050, 200.4960.

1. Introduction

In recent years various types of information from a simple message in an e-mail system to a personal identification code in electronic commerce have been transmitted over communication networks. Information leakage is a serious problem in such networks, and data encryption is considered a key technique for overcoming the problem. Characteristic of current web technology, massive image data are frequently dealt with on the Internet. For such large amounts of information large keys are required for guaranteeing a high level of security, and the large keys demand lengthy computational time for encryption and decryption.

Optical computing techniques should be useful for encryption of massive information because of parallel optical processing.[1–10] Encryption using encoding masks with random phase distributions has been proposed.[2] This method uses two statistically independent phase masks at the input and the Fourier planes, and the target message is encrypted into stationary white noise. By experimental demonstration, method performance has been studied.[3,4] As an application of the technique an encrypted memory has been studied.[5–7] A method using a stream cipher technique has also been proposed.[8–10] In this method, XOR operations between a random bit sequence and the message are executed in parallel by optical techniques. The random bit sequence, which is used as a key for encryption, is generated by a pseudorandom number generator (PRNG). To generate a random bit sequence, optical parallel processing can be applied effectively.

In this paper we propose what we believe is a new method of pseudorandom number generation, which is based on an optical feedback operation with two-dimensional (2-D) affine transformations. Affine transformation is a kind of linear transformation composed of rotation, scaling, and translation. This transformation can be implemented in parallel by optical components. For example, the series of an imaging lens, a dove prism, and a deflection mirror achieve it efficiently. Although the proposed method also requires modulo-n addition of images, this operation is expected to be achieved in parallel by a spatial light modulator. With a small number of parameters, such as the rotation angle and the scaling factor, we can generate pseudorandom intensity distribution on a 2-D image. We verify the performance of the proposed method in terms of security strength by computer simulations and evaluate randomness of the patterns generated by the proposed PRNG. Finally, the proposed PRNG is implemented by the optical fractal synthesizer[11] to clarify problems in the optical implementation of this method.

Section 2 describes the proposed stream cipher

The authors are with the Department of Material and Life Science, Graduate School of Engineering, Osaka University, 2–1 Yamadaoka, Suita, Osaka 565-0871, Japan. T. Sasaki's e-mail address is sasaki@redeye.ap.eng.osaka-u.ac.jp.

Received 15 June 1999; revised manuscript received 3 January 2000.

0003-6935/00/142340-07$15.00/0

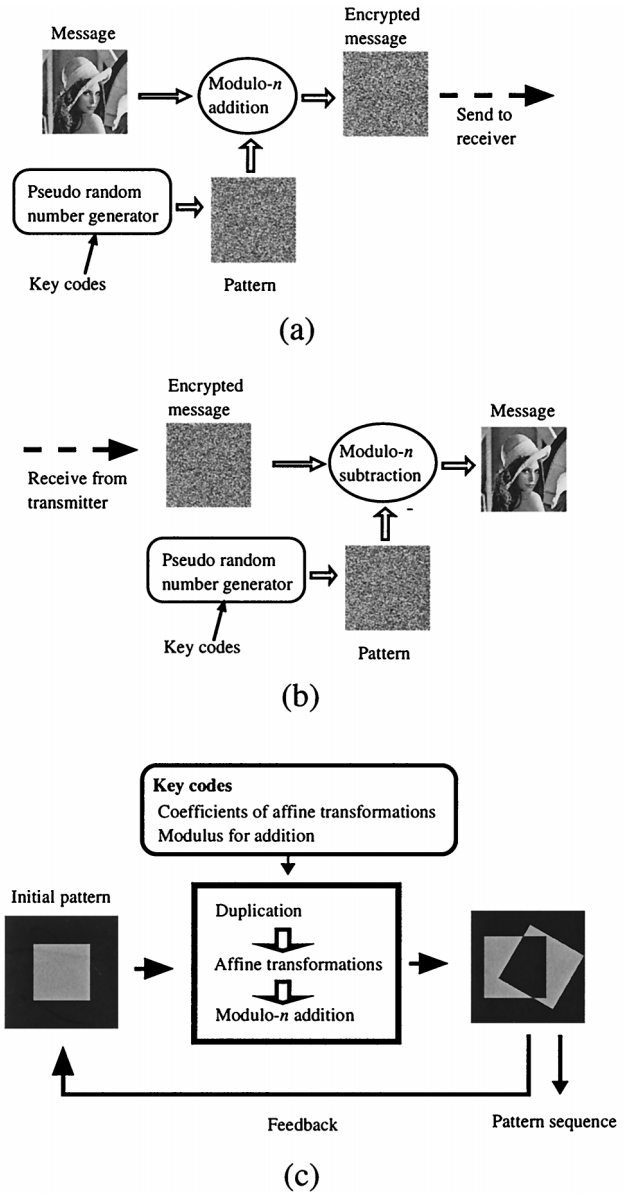

Fig. 1. Schematic diagram of the proposed method: (a) encoding and (b) decoding methods, (c) PRNG.

method. Section 3 explains computer simulations for verification of the proposed method and discusses security performance. In Section 4 we consider the randomness of the generated patterns by means of comparison with a linear feedback shift register[12] and correlation functions of the generated patterns. Section 5 shows optical implementation of the proposed PRNG with the experimental optical fractal synthesizer. In Section 2 below we explain the principle of our method.

2. Stream Cipher with Two-Dimensional Affine Transformation

Figures 1(a) and 1(b) show the schematic diagrams of encryption and decryption, respectively, based on the stream cipher. In these diagrams messages and patterns are 2-D images whose intensity is represented by 256 levels. Although one-dimensional bit sequences are often employed in the stream cipher, we use 2-D bit sequences on an image, because of the suitability for optical implementation. In the encryption a message and a key pattern generated by the PRNG for a set of key codes are added in modulo n. The encrypted message has random intensity distribution, which does not show any structure of the original message. In the decryption the message is retrieved by subtraction of the key pattern from the encrypted message in modulo n. The key pattern is generated by the PRNG by use of the same key codes as the encoding ones.

Figure 1(c) shows the schematic diagram of the proposed PRNG. This method is composed of affine transformations and feedback operations. Affine transformation is expressed by a set of a deformation matrix and a translation vector as follows:

$$\mathbf{x}' = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mathbf{x} + \begin{pmatrix} e \\ f \end{pmatrix}, \tag{1}$$

where $\mathbf{x}$ and $\mathbf{x}'$ are 2-D vectors representing the points on the input and the output planes. Several affine transformations are used for the PRNG. The initial image is multiplied, and each image is transformed by any one of the affine transformations. The transformed images are summed up by addition in modulo n. The resultant image is used as the input of the next step to generate another 2-D bit sequence.

The matrix in Eq. (1) can be rewritten for optical implementation. 2-D rotation and scaling implemented by a dove prism and a lens system are written with the following equations:

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \tag{2}$$

$$S(s) = \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix}, \tag{3}$$

where θ is the rotation angle and s is the scaling factor. In this paper we use a specific affine transformation for the proposed PRNG represented by Eq. (4):

$$\mathbf{x}' = S(s)R(\theta)\mathbf{x} + \mathbf{t}, \tag{4}$$

where $\mathbf{t}$ is the translation vector representing image shift.

In this method the key codes are assigned by the parameters of the affine transformations and the number of iterations. The amount of space required for the decoding key codes, which is expected to be large for high-security strength, is determined by the possible combinatorial number of the parameters and the iteration. Although the space seems to be smaller than other implementations of the PRNG, high sensitivity of the parameter of the affine transformations enables us to increase available values for the parameter. Even if the number is insufficient,

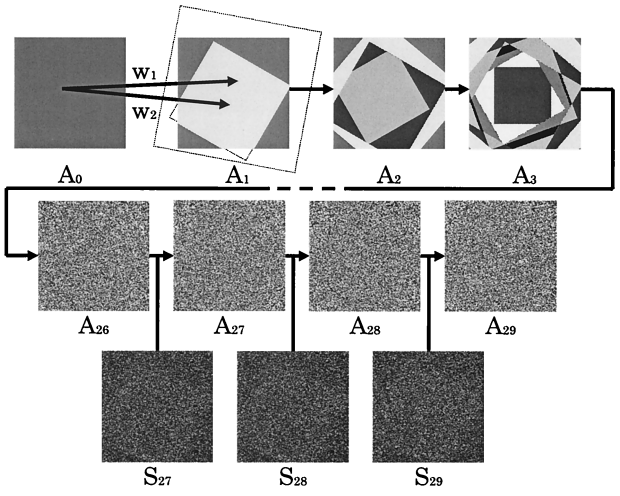

Fig. 2. Image sequence generated by the PRNG.

switching of several sets of affine transforms during iterations can be used to enlarge the key code space.

Figure 2 shows a sequence of 256 × 256 images generated by the PRNG with modulo 256 addition. A_i indicates the pattern generated by i times iteration. After 26 iterations, images with random intensity distribution are obtained. S_i represents the absolute value of intensity difference between A_i and A_{i-1}. These difference images show that the images generated by different iteration numbers have different intensity distribution.

Figures 3(a) and 3(b) show the patterns generated by different sets of the affine transformations. The parameter sets of the affine transformations are

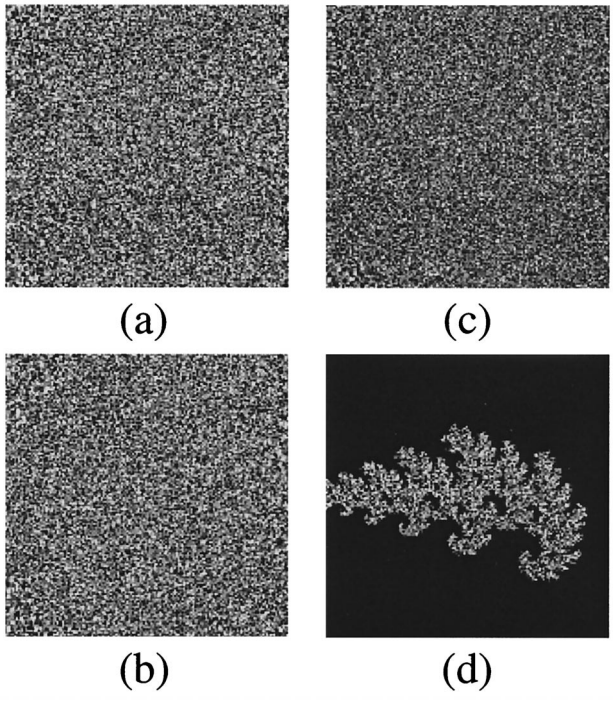

Fig. 3. Patterns generated by different parameter sets of affine transformations.

Table 1. Coefficients of Affine Transformations for Patterns of Figs. 3(a), 3(b), and 3(d)

Pattern	i	s_i	θ_i	$\mathbf{t}_i$
(a)	1	1.3	30	(50, 0)
(a)	2	1.3	0	(−50, 0)
(b)	1	1.3	40	(50, 0)
(b)	2	1.3	0	(−50, 0)
(d)	1	0.7	30	(50, 0)
(d)	2	0.7	0	(−50, 0)

shown in Table 1, where i is the identifier of affine transformation. The iteration number is set as 19. Figure 3(c) shows the absolute value of intensity difference between Figs. 3(a) and 3(b). As seen from Fig. 3(c), it is clear that Figs. 3(a) and 3(b) have different intensity distributions. Figure 3(d) shows a specific case in which random intensity distribution is localized in a fractal area. To use the proposed method for the stream cipher, the affine transformations and the iteration number must be selected to obtain a pattern in which intensity is distributed randomly on the whole image. In this paper, to select the iteration number and the affine transformations, we calculate the autocorrelation function of the pattern for the iteration number and the affine transformations and verify whether the autocorrelation function has only one peak on the center of a plane, such as a delta function, as described in Section 4.

3. Computer Simulation

To verify the effectiveness of the proposed method, we executed a computer simulation of data encryption and decryption. The message (the target image of the cipher) is a 256 × 256 pixel image whose intensity is represented by 256 levels. The modulus for the image addition is 256. Figure 4 indicates (a) the message, (b) the key pattern, (c) the ciphered message, and (d) the decoded image. Coefficients of the affine transformations are shown in Table 2. The iteration number for the key pattern generation is 15. Randomness of the key pattern can be verified by the autocorrelation function as described in Section 4. The ciphered message in Fig. 4(c) has a pseudorandom intensity distribution in which the message content is not visible.

To verify security strength of the proposed method, we try to retrieve the message by slightly different key patterns. The key pattern is generated by the affine transformations whose parameters are modified from that of the encoding key. The encoding key pattern is the same as the pattern in Fig. 4(b). Table 3 indicates the modified parameters. Figures 5(a)–5(c) show the decoded images by the key patterns with different scaling factor, rotation angle, and translation vector, respectively. The correct image cannot be retrieved by these keys. Figure 5(d) shows the decoded image by the key pattern with the iteration number one time larger than that of the encoding key. Even in this case the correct message cannot be obtained. As seen from these results, it is

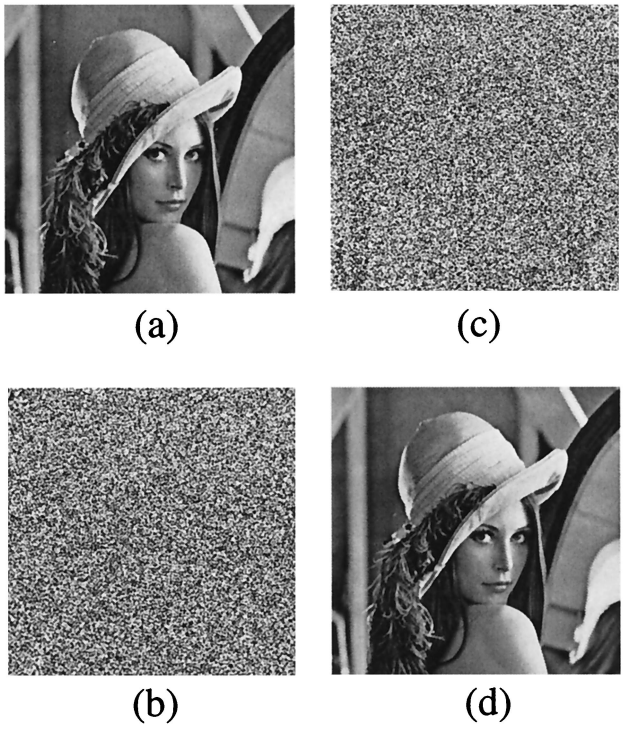

Fig. 4. Verification of the proposed method: (a) message, (b) key pattern, (c) encrypted message, (d) encoded message.

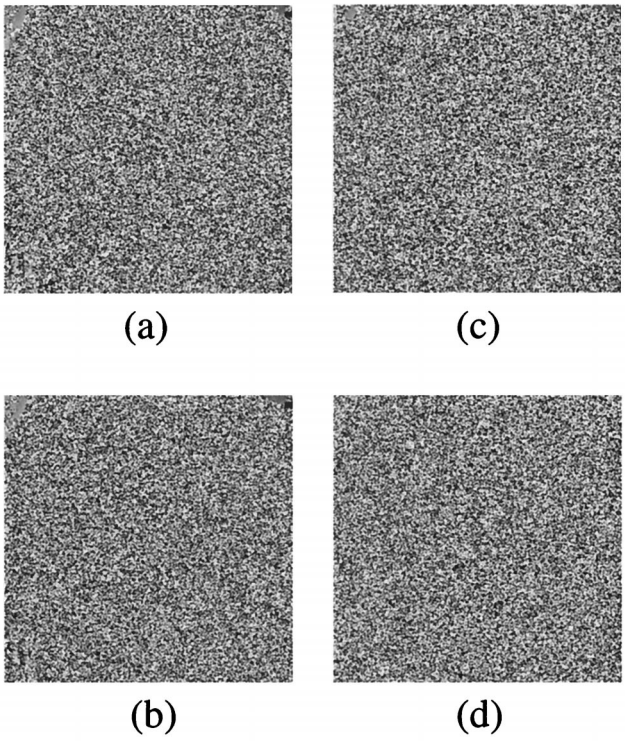

Fig. 5. Decoded images by modified key pattern. Images correspond to information given in Table 3.

difficult to decrypt the message with keys similar to the encoding ones.

4. Randomness of Pseudorandom Pattern Generation

To understand the mechanism of pattern generation by the proposed method, we compare it with a linear feedback shift register (LFSR).[12] Figure 6 shows the schematic diagram of the LFSR. The LFSR is composed of L delay cells and a feedback connection transferring the output signal to the entry of the shift register. The output is obtained by the weighted summation of the cells where modulo-2 addition is

Table 2. Coefficients of Affine Transformations for Key Pattern of Fig. 4(b)

i	s_i	θ_i	$\mathbf{t}_i$
1	0.8	60	(50, −10)
2	0.7	200	(−40, −50)
3	1.1	90	(0, 5)

Table 3. Modified Parameters and Variations of Fig. 5

Example	Parameter	Variation
(a)	s_1	+0.01
(b)	θ_1	+0.1
(c)	$\mathbf{t}_1$	+(1, 0)
(d)	iteration	+1

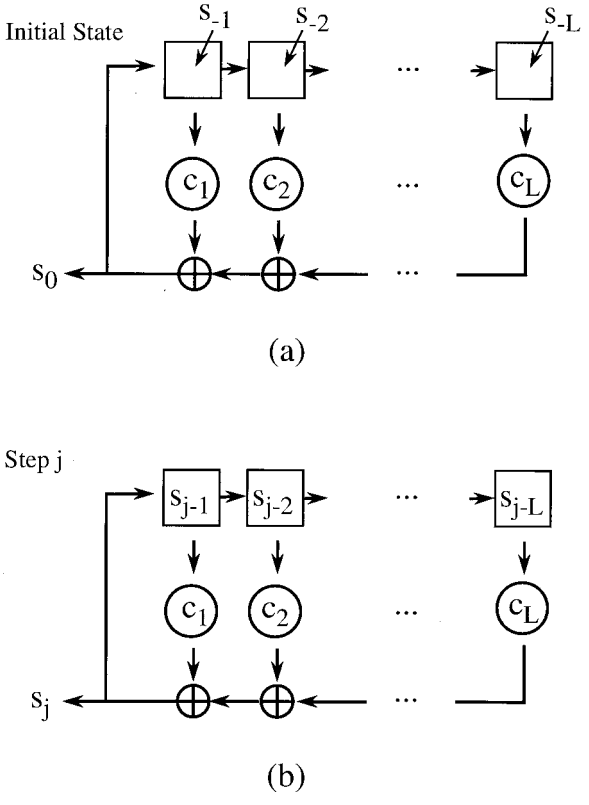

Fig. 6. Schematic diagram of linear feedback shift register.

used for the summation. The procedure is expressed as the following equation,

$$s_j = \sum_{\substack{i=1 \\ (\mathrm{mod}\ 2)}}^{L} c_i s_{j-1}, \tag{5}$$

where i is the cell position, c_i is the weight factor, s_{j-i} is the cell content of the i position at step j, and $\Sigma_{(\mathrm{mod}\ n)}$ represents summation based on the modulo-n number system. j corresponds to the processing step starting from 0. $\{s_{-1}, s_{-2}, \ldots, s_{-L}\}$ are given as the initial parameters. As shown in Fig. 6(b), s_j is the output (a number) at the step j calculated from $\{s_{j-1}, s_{j-2}, \ldots, s_{j-L}\}$. s_j is fed back into the entry of the shift register and used to generate the subsequent number generation. When we repeat the same procedure, a sequence of random numbers are generated. The weight factors $\{c_1, c_2, \ldots, c_L\}$ determine the period of the output sequence.

The feedback process of the proposed method is denoted by the following equation,

$$f_{j+1}(\mathbf{x}) = \sum_{\substack{i=0 \\ (\mathrm{mod}\ n)}}^{N} f_j[\mathcal{A}_i^{-1}(\mathbf{x} - \mathbf{a}_i)], \tag{6}$$

where $\mathbf{x}$ is a 2-D vector representing a pixel on the image, $f_j(\mathbf{x})$ is the pixel intensity of $\mathbf{x}$, and $\mathcal{A}_i$ and $\mathbf{a}_i$ are the deformation matrix and the translation vector, respectively, which correspond to rotation, scaling, and translation in the experimental setup. Parameter i is an identifier of N affine transformations, and j shows the iteration number.

Transition of each pixel intensity obeys the generation rule of the pseudorandom bit sequence similar to the LFSR in the case of modulo-2 addition. In our method the delay cells correspond to the pixels on the 2-D plane. For example, Fig. 7 shows propagation of a single bright pixel by the optical feedback with two affine transformations. In this case, a bright pixel and a dark pixel mean 1 and 0, respectively. A bright pixel is moved to the other pixels, which corresponds to the shift operation of the cell content in the LFSR. Because the 2-D plane is addressed by finite resolution, a close path is formed for the bright pixel movement. In this case the pixel intensity $f_j[\mathcal{A}_i^{-1}(\mathbf{x} - \mathbf{a}_i)]$ in Eq. (6) can be written as $f_{j-k}(\mathbf{x})$ where k is a constant representing delay of iterations. Consequently, Eq. (6) is equivalent to Eq. (5), whose weight factor c_k is 1. In this case the pixel $\mathbf{x}$ is a seed of the pseudorandom bit sequence. Note that in a usual case many bright pixels are located on the image so that more-complicated pattern generation is expected by the same procedure.

Randomness of the intensity distribution is evaluated by statistical methods. In the case of a pattern with random intensity distribution, its autocorrelation function should be a delta function. Figure 8(a) shows the autocorrelation function of the key pattern in Fig. 4(b). It can be found that the autocorrelation function has only one peak on the center of the pattern. As a consequence, the pattern is considered to have random intensity distribution.

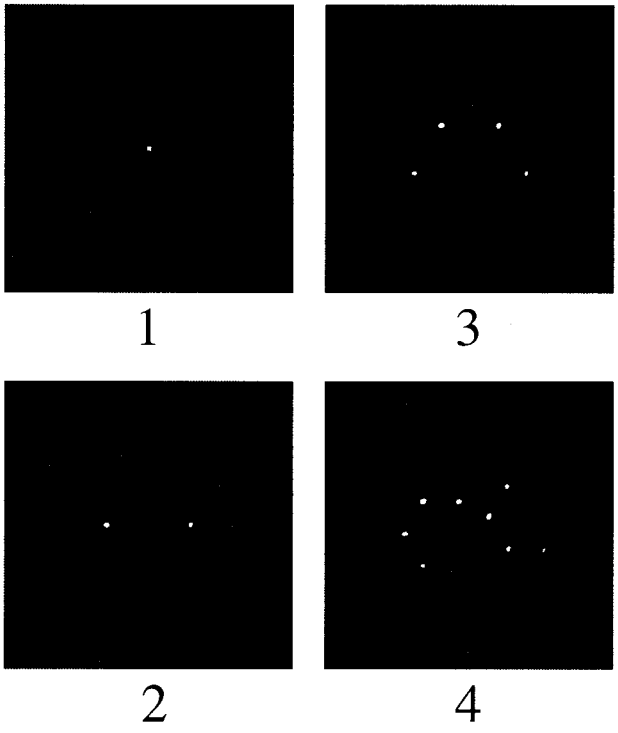

Fig. 7. Trace of a bright pixel during iteration.

As shown in the comparison between the proposed method and the LFSR, each pixel on the image becomes a seed of pseudorandom patterns. For this case it is expected that the patterns generated by different numbers of iterations have no correlation peak, because they have different random distribution. Figure 8(b) shows the correlation function between the patterns obtained by 14 and 15 iterations whose affine transformations are the same as in Fig. 4(b). There is no peak on the correlation function. Therefore we can verify that the patterns generated by the different iteration number, even if the difference is just one, have different random distribution.

5. Optical Implementation

To clarify problems with optical implementation of the proposed method, we constructed the PRNG on the optical fractal synthesizer.[11] Optical setup of the optical fractal synthesizer is shown in Fig. 9. This system can generate a fractal pattern for given system parameters by optical feedback processing. The input image of the optical fractal synthesizer is displayed on the CRT and is duplicated by the beam splitter BS1. Each image is rotated and reflected by the dove prism and translated by the tilted mirror in each optical path. The images passing through the different paths are combined by the second beam splitter BS2. After scaling by the zoom lens, the images are captured by the CCD camera. The captured image is displayed on the CRT again, and the same procedure is repeated. After a large number of

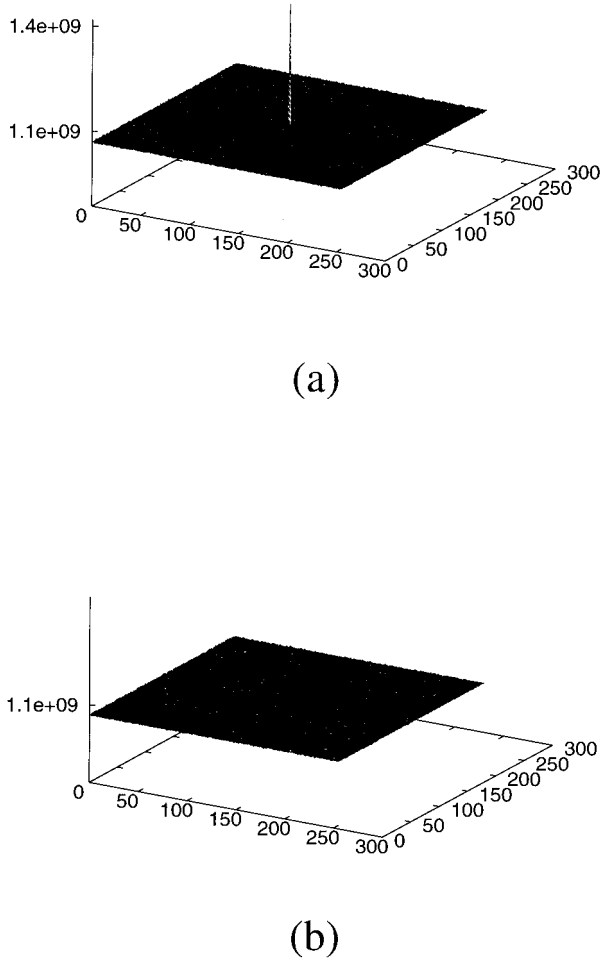

Fig. 8. Autocorrelation function of the generated patterns.

iterations, the initial pattern is transformed into a complicated shape specified according to the system parameters.

To generate images with pseudorandom intensity distribution, the captured images through the different optical paths are added in modulo 2. XOR operation is used as modulo-2 addition, which is suitable for binary images. Figure 10 shows an example of a pattern sequence generated by the optical system. Parameters of the affine transformation are shown in Table 4. Image resolutional is 200 × 200 pixels. The overlapped area of two transformed patterns becomes dark by XOR operation executed by the computer. After 13 iterations bright and dark pixels are spread over the image area.

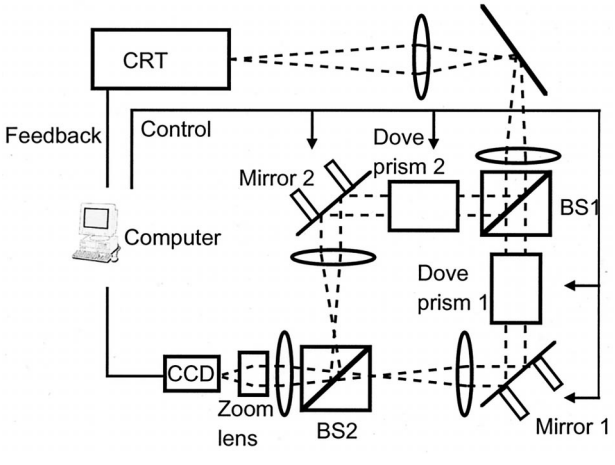

Fig. 9. Optical setup of optical fractal synthesizer. BS, beam splitter.

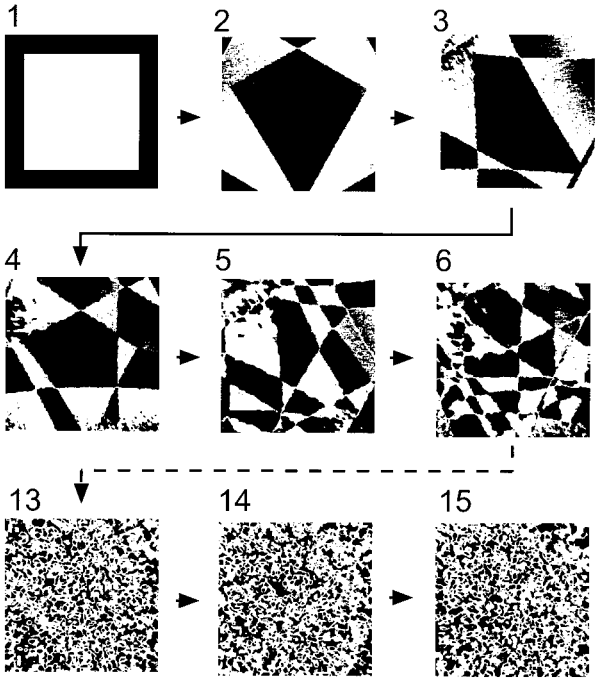

Fig. 10. Random pattern sequence generated by the optical system.

Figures 11(a)–11(c) show results of message encryption and decryption by use of the optical PRNG, where the key pattern is the one obtained by 15 iterations shown in Fig. 10. In this case the message is a binarized image to avoid the effect of nonlinearity of the television feedback system. As seen from Fig. 11(c), the original message [Fig. 11 (a)] cannot be retrieved. In addition, the abstract structure of the message remains in the encrypted image of Fig. 11(b). These results come from instability of the optical PRNG. The difference between the key patterns independently generated by the same parameters is shown in Fig. 11(d). As shown in this figure, the difference is relatively large. To reproduce the key pattern exactly, we should improve precision of the modulo-n addition in the optical system. The proposed method requires quantization of intensity for

Table 4. Parameters of Affine Transformations Used in Optical Implementation

i	s_i	θ_i	$\mathbf{t}_i$
1	1.2	60	(75, 0)
2	1.2	120	(−75, 0)

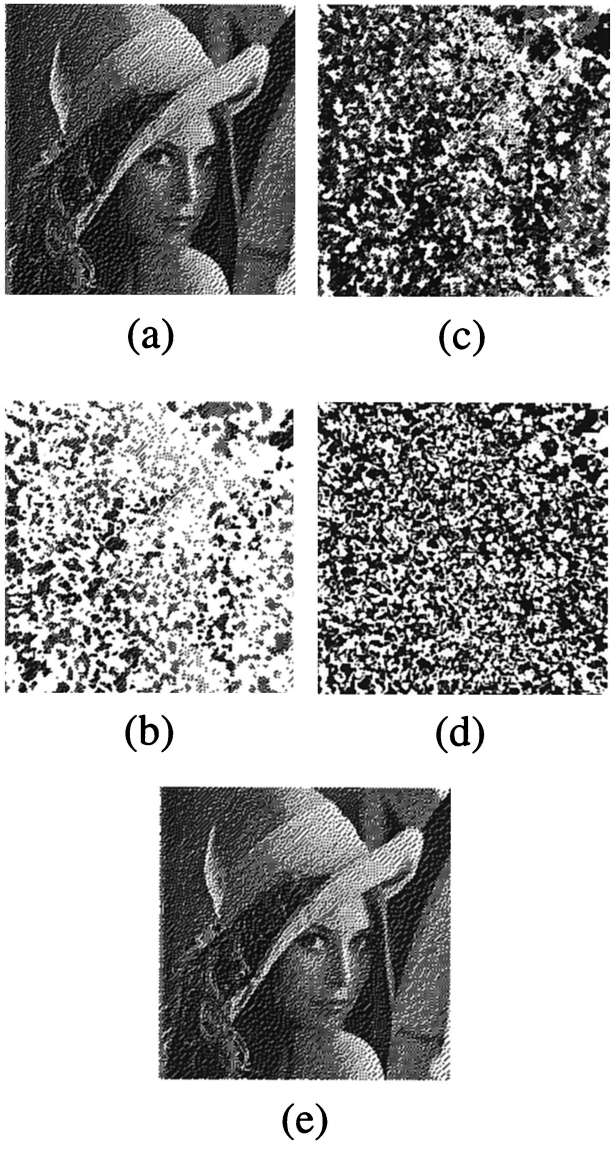

Fig. 11. Result of optical implementation: (a) message, (b) data encrypted by a key generated optically, (c) message decoded by a key pattern generated independently, (d) intensity difference between the keys used for (b) and (c), and (e) message decoded by the key pattern used for (b).

modulo-n addition, but accurate quantization is difficult, because intensity distribution on the CRT of the experimental system fluctuates temporally and because the intensity distribution captured by the CCD is not uniform by aberration of the optical system. If we use the same key pattern as that of the encryption, the correct message is obtained as shown in Fig. 11(e). It is clear that the obtained message is the same as the original.

The slow speed of the optical feedback operation is also an important problem. In the experimental system, the speed of the feedback operation is limited by the transfer frame rate from the CCD camera to the CRT, which is ~30 frames/s. A high-speed optical feedback system based on the smart pixels with parallel optical input–output ports and free-space optics is expected to overcome the problem.

6. Conclusion

We have proposed a stream cipher method based on the PRNG with geometrical transformation, such as image rotation, scaling, and translations. The proposed method is suitable for optical implementation and can generate 2-D pseudorandom intensity distribution by optical parallel affine transformations and optical feedback processing. The security strength of the method has been evaluated by computer simulations. It has been shown that different key pattern cannot retrieve the ciphered image if sufficient numbers of iterations were performed for random pattern generation. We have explained the mechanism of random pattern generation by comparing it with the pseudorandom bit generation by the LFSR. The proposed method was implemented on the optical fractal synthesizer, which suggests that uniformity of intensity distribution on the image plane is important for correct decoding.

References

1. B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," Opt. Eng. **33,** 1752–1756 (1994).
2. P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20,** 767–769 (1995).
3. B. Javidi, G. Zhang, and J. Li, "Experimental demonstration of the random phase encoding technique for image encryption and security verification," Opt. Eng. **35,** 2506–2512 (1996).
4. B. Javidi, A. Sergent, and E. Ahouzi, "Performance of double phase encoding encryption technique using binarized encrypted images," Opt. Eng. **37,** 565–569 (1998).
5. B. Javidi, G. Zhang, and J. Li, "Encrypted optical memory using double-random phase encoding," Appl. Opt. **36,** 1054–1058 (1997).
6. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption system that uses phase conjugation in a photorefractive crystal," Appl. Opt. **37,** 8181–8186 (1998).
7. O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett. **24,** 762–764 (1999).
8. M. Madjarova, M. Kakuta, M.Yamaguchi, and N. Ohyama, "Optical implementation of the stream cipher based on the irreversible cellular automata algorithm," Opt. Lett. **22,** 1624–1626 (1997).
9. M. Kakuta, M. Madjarova, T. Obi, M. Yamaguchi, and N. Ohyama, "Vernam encryption using optical parallel processing," Jpn. J. Opt. **27,** 104–109 (1998).
10. S. Zhang and M. Karim, "High-security optical integrated stream ciphers," Opt. Eng. **38,** 20–24 (1999).
11. J. Tanida, A. Uemoto, and Y. Ichioka, "Optical fractal synthesizer: concept and experimental verification," Appl. Opt. **32,** 653–658 (1993).
12. J. L. Massey, "Shift-register synthesis and BCH decoding," IEEE Trans. Inf. Theory **IT-15,** 122–127 (1969).