Novel optical password security technique based on optical fractal synthesizer

Kenan Wu
Jiasheng Hu, MEMBER SPIE
Dalian University of Technology
School of Electronic and Information Engineering
1 Linggong Road
Dalian Liaoning 116024
China
E-mail: jshu@dlut.edu.cn

Xu Wu
Dalian Maritime University
College of Information Technology
1 Linggong Road
Dalian Liaoning 116026
China

Abstract. A novel optical security technique for safeguarding user passwords based on an optical fractal synthesizer is proposed. A validating experiment has been carried out. In the proposed technique, a user password is protected by being converted to a fractal image. When a user sets up a new password, the password is transformed into a fractal pattern, and the fractal pattern is stored in authority. If the user is online-validated, his or her password is converted to a fractal pattern again to compare with the previous stored fractal pattern. The converting process is called the *fractal encoding procedure*, which consists of two steps. First, the password is nonlinearly transformed to get the parameters for the optical fractal synthesizer. Then the optical fractal synthesizer is operated to generate the output fractal image. The experimental result proves the validity of our method. The proposed technique bridges the gap between digital security systems and optical security systems and has many advantages, such as high security level, convenience, flexibility, hyper extensibility, etc. This provides an interesting optical security technique for the protection of digital passwords. [DOI: 10.1117/1.3156052]

Subject terms: optical security; verification; fractal encoding procedure; optical fractal synthesizer.

Paper 080982R received Dec. 18, 2008; revised manuscript received Apr. 12, 2009; accepted for publication Apr. 27, 2009; published online Jun. 26, 2009.

1 Introduction

Optical verification systems have received enormous attention due to their high security level and parallel processing capacity. Early explorations of these systems date back to the 1970s, when some sensitive devices were put forward.[1,2] Within the past decade, research of optical verification systems has been getting more and more successful. Representative achievements include the double random phase encoding technique,[3] a security system based on a joint transform correlator,[4–7] a verification system based on an iterative algorithm,[8,9] a pure phase coding technique,[10,11] and a polarization encoding technique.[12] Despite the diversity of their optical principles and forms of realization, most of these verification techniques share something in common. Often, these verification techniques consist of two procedures, i.e., the encoding procedure and the decoding procedure. In the encoding procedure, an original image is chosen for each user and converted to an encoded image, either by means of optical processing or by electronic computing approaches like digital encoding or iterative algorithms. The obtained encoded image is subsequently distributed to the user. The decoding procedure is to verify the authenticity of the users and is often carried out by optical devices for fast processing. The user being checked is asked to present the encoded image given to him or her. The encoded image is used to reconstruct the original image by the authority. Only the correct reconstruction of the original image means that the provided encoded image is from a valid user. Validation systems like this are always used in situations like certificate verifications or fingerprint identifications. But so far, optical security systems for the protection of user passwords have rarely been reported.

Fractals have already been used in some security areas. A fractal can be determined by a set of parameters. Tebaldi et al. proposed the use of fractal-structured diffractive masks as keys in secure storage-readout systems[13] and pointed out that if a fractal is used as the encrypting key, there is no need to send the key mask itself to the receiver, but a simple set of parameters. This prevents the loss of key information in transmission, reduces the risk of the key mask being intercepted, and makes implementation easy. Fractals can be generated by optical means. The optical fractal synthesizer[14] (OFS) is a parallel optical processor for generating fractals. Sasaki et al. used OFS to generate pseudorandom patterns as the key for stream ciphers.[15,16] One can easily see that until now, fractals and OFS are used only as accessories for other security applications.

In this paper, we present a novel optical password security technique based on OFS. This technique can be used for banks, password locks, or customhouses. It protects the user password by converting the password to a fractal image. The process that converts the user password to a fractal image is called the *fractal encoding procedure* (FEP) and consists of two steps. First, the password is nonlinearly transformed to get the parameters for the OFS; second, the OFS is operated to generate the output fractal image.

The is paper is organized as follows. In Sec. 2, the prin-

0091-3286/2009/$25.00

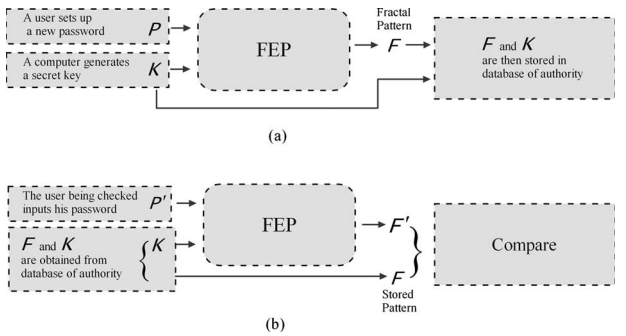


Fig. 1 The flowchart of the optical password security technique when (a) a user sets up a new password and (b) a user is online validated.

ciple of our proposed technique is demonstrated in detail. In Sec. 3, experimental results and discussions are given. Last, a conclusion is given in Sec. 4.

2 Optical Password Security Technique Based on Optical Fractal Synthesizer

2.1 *Working Process of the Optical Password Security Technique*

This optical password security technique utilizes OFS to secure user passwords and can be used in verification sites like banks or customhouses. The kernel of this technique is the fractal encoding procedure (FEP) that converts a user password to a fractal pattern. Figure 1 is a flowchart of the working process of this security technique. As is shown in Fig. 1(a), when a user sets up a new private password P, a secret key K is randomly generated in the same time. A fractal pattern F is obtained from P and K through FEP. F and K are then stored in the database of authority. And in Fig. 1(b), while on-site validation of the user-input password P' takes place, the stored key K is picked up in the database, and another fractal pattern F' will be generated through FEP using P' and K. Subsequently, F' is compared with the stored pattern F. If F' is the same as the stored pattern F, the input password is a legal one; otherwise, it is invalid.

2.2 *Details of the FEP*

The FEP consists of two steps. First, a nonlinear transform is applied to the password to generate the parameters for the OFS. Second, the OFS is operated to generate the output fractal image. Details of the FEP are described as follows.

Suppose that the user password P is composed of 8 integral numbers valued between 0 and 9:

$$P=[p_1 \quad p_2 \quad p_3 \quad p_4 \quad p_5 \quad p_6 \quad p_7 \quad p_8] \times (p_i \in \{0,1,\ldots,9\}, \quad i=1,2,\ldots,8). \tag{1}$$

A secret key K is gotten, either generated by a computer as in Fig. 1(a), or picked up from the database in Fig. 1(b). K is composed of 11 integral numbers, as described in Eq. (2), where k_1 to k_8 range from 0 to 9, and k_9 to k_{11} range from 50 to 150:

$$K=[k_1 \quad k_2 \quad k_3 \quad k_4 \quad k_5 \quad k_6 \quad k_7 \quad k_8 \quad k_9 \quad k_{10} \quad k_{11}] \times (k_i \in \{0,1,\ldots,9\}, \quad i=1,2,\ldots,8, \quad k_j \in \{50,51,\ldots,150\}, \quad j=9,10,11). \tag{2}$$

A linear transform is performed to generate parameters of the OFS:

$$r_n=(p_n+3)^{k_n+3} \bmod k_9 \quad (n=1,2,\ldots,8), \tag{3}$$

$$s_1=r_1/k_9, \tag{4}$$

$$\theta_1=-\arccos(r_2/k_9), \tag{5}$$

$$j_1=(-1)^{k_{10}}, \tag{6}$$

$$\mathbf{t}_1=-[r_3+50,r_4], \tag{7}$$

$$s_2=r_5/k_9, \tag{8}$$

$$\theta_2=\arccos(r_6/k_9), \tag{9}$$

$$j_2=(-1)^{k_{11}}, \tag{10}$$

$$\mathbf{t}_2=[r_7+50,r_8]. \tag{11}$$

Then the OFS is operated to produce the fractal pattern F. The OFS generates fractals based on an iterated function system (IFS). An IFS (Ref. 17) consists of a finite set of affine transformations. In our technique, the $n+1$'th iteration of the IFS can be expressed as:

$$A_{n+1}=W(A_n)=\bigcup_{i=1}^{2}\omega_i(A_n), \quad A_n \in R^2, \tag{12}$$

where A_n indicates a set of points in a two-dimensional (2-D) real number space R^2, corresponding to a pattern on a 2-D plane. And $\omega_i(A_n)$ is a contractive affine transformation expressed as:

$$\omega_i(A_n)=\{\mathbf{x}';\mathbf{x}=S(s_i)R(\theta_i)M(j_i)\mathbf{x}+\mathbf{t}_i,\mathbf{x} \in A_n\} \quad (i=1,2), \tag{13}$$

where

$$S(s_i)=\begin{bmatrix} s_i & 0 \\ 0 & s_i \end{bmatrix}, \quad R(\theta_i)=\begin{bmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{bmatrix}, \quad \text{and} \quad M(j_i)=\begin{bmatrix} j_i & 0 \\ 0 & 1 \end{bmatrix} j \in \{1,-1\},$$

is the transform matrix corresponding to the contraction, rotation, and reflection transformation, respectively.

When an IFS with a certain parameter set $\{s_i,\theta_i,j_i,\mathbf{t}_i\}$ is applied to an arbitrary image iteratively, it will finally converge to a fractal called the *attractor*. The shape of the fractal is determined by the parameter set $\{s_i,\theta_i,j_i,\mathbf{t}_i\}$.[17] The parameter set is decided according to Eq. (4) to Eq.

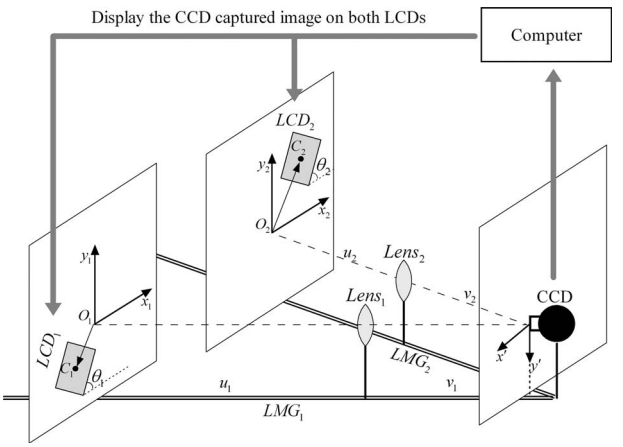


Fig. 2 The OFS used in our experiment.

(11) before the iteration process starts and remains unchanged in all iterations until convergence.

An OFS realizes the previous IFS by optical means. Examples of OFS have been given in the previous literature.[18] Here, we present a new setup of OFS requiring fewer optical elements, as shown in Fig. 2. Two linear motion guides (LMGs) are placed on an experiment table. Each LMG carries a liquid crystal display (LCD) and a convex lens. The CCD is placed upside down for receiving the inverted image of two LCDs. Both the LCDs and the CCD are controlled by a computer, making the CCD-captured image display back on the two LCDs.

To realize the IFS with parameter set $\{s_i, \theta_i, j_i, \mathbf{t}_i\}$, elements in the OFS should be positioned properly before the iterations start. As shown in Fig. 2, the object distance u_i and the image distance v_i are decided by $v_i/u_i \cdot L_{LCD}/L_{CCD}=s_i$ and the thin lens formula $1/u_i+1/v_i=1/f$, where L_{LCD}, L_{CCD} means the width of the LCD screen and the width of the CCD screen, respectively, and f is the focal length of the lens. Suppose that the pixel number of the CCD is $M_{CCD}\times N_{CCD}$. The LCD_i is rotated with angle θ_i. And its center C_i is shifted to $\vec{O_iC_i}=\mathbf{t}_i(L_{CCD}/M_{CCD})(u_i/v_i)$ in the x_iy_i plane. Such a shift makes the image of the LCD_i have a shift of $\mathbf{t}_i(L_{CCD}/M_{CCD})$, i.e., a shift of $\mathbf{t}_i$ pixels in the CCD plane ($x'y'$ plane). If $j_i=1$, the CCD-captured image is displayed on the LCD_i directly, and if $j_i=-1$, the image displayed on the LCD_i is in retroflexion horizontally, realizing the reflection transformation.

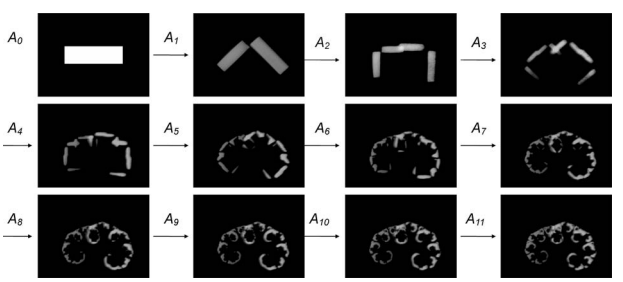


Fig. 3 The CCD-captured image of different iterations in the OFS.

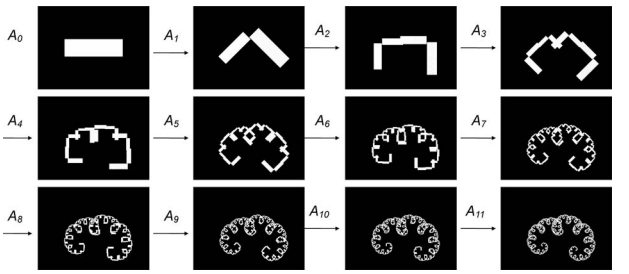


Fig. 4 Computer simulation results of the CCD-captured image of different iterations in the OFS.

This positioning of elements is done by motorized precision rotary and translation stages before the iterative process starts.

For the first iteration, an arbitrary initial pattern A_0 is displayed on both LCDs. In the $n+1$'th iteration, the CCD-captured pattern A_n (obtained from the previous iteration) is displayed back on both LCDs and imaged by the lenses. Each image is contracted by the lens, and at the same time, the images are translated and rotated because the LCD is shifted and rotated. The two images are captured synchronously by the CCD, and the merged pattern A_{n+1} will be used in the next iteration. When the iterative process of the OFS converges, a fractal image F is obtained from the CCD, and the FEP is finished.

The FEP process is used either when a user sets a new password or when a password is validated online, as described in Fig. 1. The nonlinear transformation, corresponding to Eq. (3) to Eq. (11), has low computing expense and therefore can be executed by notebook PC or digital signal processing (DSP). The subsequent fractal generation process is carried out by an OFS system.

3 Experimental Results and Discussion

Experiments were carried out to verify the proposed password security technique. The LCDs in the OFS system are Samsung SyncMaster 713 MB, which is an incoherent light source. The screen size is $L_{LCD}\times H_{LCD}=340\text{mm}\times 270$ mm. The resolution used in our experiment is 1024×768. The CCD camera is a Mintron MTV. 1881EX. The size of the frame is $L_{CCD}\times H_{CCD}=6.36\times 4.77$ mm. The

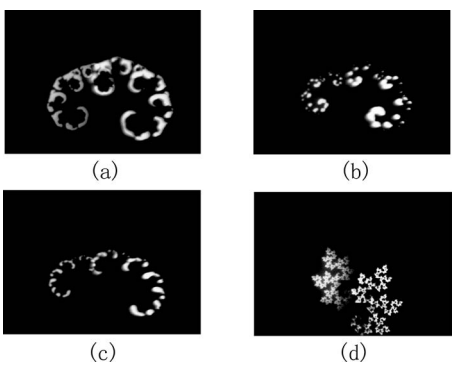


Fig. 5 Generated fractal results from different user-input passwords: (a) P'_1, (b) P'_2, (c) P'_3, (d) P'_4.

Table 1 IFS parameters related to password P_2', P_3', and P_4'.

Password	s_1	s_2	θ_1	θ_2	j_1	j_2	$\mathbf{t}_1$	$\mathbf{t}_2$
P_2'	0.4725	0.7363	$-\pi/4$	$\pi/4$	−1	1	[−101,−1]	[140,1]
P_3'	0.4725	0.7363	-0.18π	0.165π	−1	1	[−101,−1]	[140,1]
P_4'	0.6154	0.7363	$-\pi/4$	$\pi/4$	−1	1	[−101,−1]	[140,90]

pixel number is $M_{CCD}\times N_{CCD}=795\times 596$. The size of each pixel is 8 μm$\times$8 μm. The focal length of the convex lenses is $f=20$ mm.

Suppose that a user sets a new password $P=[4\ 2\ 2\ 5\ 8\ 5\ 7\ 6]$. According to the preceding description of the FEP, a random key $K=[7\ 3\ 7\ 1\ 4\ 7\ 0\ 6\ 91\ 109\ 80]$ is generated by a computer. The parameters of the IFS are obtained by Eq. (4) to Eq. (11). They are $s_1=0.615$, $\theta_1=-\pi/4$, $j_1=-1$, $\mathbf{t}_1=[-101\ -1]$, $s_2=0.736$, $\theta_2=\pi/4$, $j_2=1$, $\mathbf{t}_2=[140\ 1]$, respectively. Before the iterative process of the OFS is running, element positions are configured as follows: $u_1=1757$ mm, $v_1=20.2$ mm, $u_2=1472$ mm, $v_2=20.3$ mm, $\vec{O_1C_1}=[-70.2\text{ mm},-0.7\text{ mm}]$, $\vec{O_2C_2}=[81.3\text{ mm},0.6\text{ mm}]$. Figure 3 exhibits the images captured by the CCD after different iterations. It can be seen that after several iterations, the captured images are stabilized and converged to the attractor—a fractal image F. K and F are then stored in the database of authority. Computer simulation results according to Eq. (12) and Eq. (13) are also given in Fig. 4 to prove the correctness of the OFS operating process.

In the verification process, the user being checked is asked to input his or her password. Suppose that the user input a correct password $P_1'=[4\ 2\ 2\ 5\ 8\ 5\ 7\ 6]$. The previous $K=[7\ 3\ 7\ 1\ 4\ 7\ 0\ 6\ 91\ 109\ 80]$ is picked up from the database. Apparently, the parameter set of the IFS and element positions of the OFS are the same as the case when P is input. The FEP is conducted again to generate another fractal image F_1', which is exhibited in Fig. 5(a). Obviously, F_1' is similar to the stored fractal image F. To further evaluate the similarity between these two images, the mean square error (MSE) is used. The MSE between images $F'(x,y)$ and $F(x,y)$ is defined as:

$$\mathrm{MSE}=\frac{\Sigma_{x,y}|F'(x,y)-F(x,y)|^2}{\Sigma_{x,y}|F(x,y)|^2}. \tag{14}$$

The MSE between F_1' and F is 0.057, very near to zero, which means that the two images are very similar and indicates that the input password P_1' is legal.

Suppose that the user inputs some wrong password—for example, $P_2'=[3\ 2\ 2\ 5\ 8\ 5\ 7\ 6]$, $P_3'=[3\ 4\ 2\ 5\ 8\ 9\ 7\ 6]$, and $P_4'=[4\ 2\ 2\ 5\ 8\ 5\ 7\ 7]$. Related IFS parameters are shown in Table 1. Element positions of the OFS are shown in Table 2. Fractal images F_2', F_3', and F_4' are obtained, respectively, as shown in Figs. 5(b)–5(d). The MSEs between them and F are 1.365, 1.183, and 1.600, respectively. Therefore, they are quite different from F. This indicates that P_2', P_3', and P_4' are invalid passwords. Practically, when MSE is more than 0.2, we consider the input passwords invalid.

The preceding experiment proves the validity of the proposed technique. In our experiment, the speed of the whole system is mainly limited by the transfer frame rate of the CCD-LCD system, which is about 25 frames/s. Often, it takes less than 12 iteration cycles to produce a fractal—that is, $<$0.5 s. This is acceptable in many verification applications. Further improvement of speed is expected if an all-optical setup of OFS is applied.

The FEP has a good stability in producing the fractal pattern F. This is ensured by the character of IFS. The IFS in our technique is a hyperbolic IFS; the attractor of the IFS F is determined uniquely by its parameter set.[19] So if there is turbulence in one iteration cycle, causing the image taken by the CCD to be disturbed, the following iterations will still converge to the same attractor F. Furthermore, the attractor depends continuously on the parameters.[17] So even if there are element position errors in the OFS, the obtained fractal will still be similar to F. Therefore, this system is robust to turbulences and element position errors in the OFS system.

Different from most of the previous research, by utilizing a novel procedure named FEP, this technique has some unique features. First, the result of the FEP process, the

Table 2 Element positions of the OFS.

Password	u_1 (mm)	v_1 (mm)	u_2 (mm)	v_2 (mm)	$\vec{O_1C_1}$ (mm)	$\vec{O_2C_2}$ (mm)
P_2'	2283	20.2	1472	20.3	[−91.4,−0.9]	[81.3,0.6]
P_3'	2283	20.2	1472	20.3	[−91.4,−0.9]	[81.3,0.6]
P_4'	1757	20.2	1472	20.3	[−70.2,−0.7]	[81.3,52.3]

fractal pattern F, has very delicate microstructures; it is therefore impossible to duplicate it exactly. Often, a hacker would derive a user's password from the stored information F. So, theoretically, if the precision and resolution of OFS are improved, and if the produced fractal image is kept in optical storage, it will be very difficult for the cracker to get an accurate copy of the stored information F. Hence, this system could have a very high security level. Second, unlike other optical security methods, this technique converts digital passwords to patterns, so it bridges the gap between digital security systems and optical security systems. This feature can be utilized in many coded methods. For example, if it associates with the double random phase system, it could produce random phase key patterns for the double random phase system from digital passwords. Then users needs to remember only the password rather than always inconveniently keeping a portable key pattern on hand. So our technique can make some traditional optical security systems more convenient for users. Third, the sort and form of the nonlinear transformation and setup of the OFS can be chosen practically according to specific applications. So this technique is very flexible and extensible.

4 Conclusion

A novel optical password security technique based on OFS is presented in this paper. It is used for securing user-input passwords in situations like banks and customhouses. Unlike most previous studies in this area, this technique utilizes the FEP to convert the user input password to a fractal pattern. Experiments have proven the validity of our proposed technique.

Our proposed technique has many unique advantages, such as high security level, convenience, flexibility, and extensibility. It is robust to turbulences and element position errors in the OFS system. It is also viable to be used in association with other existing optical encryption and verification techniques, to produce new forms of optical or optical-electrical security systems.

Acknowledgments

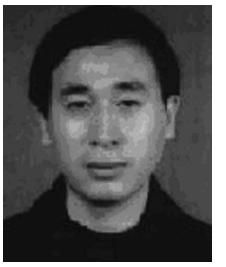
This work was supported in part by the National Natural Science Foundation of China (Grant No. 60707004), and in part by the Dalian Science and Technology Research Project of China (Grant No. 2006A14GX044).

References

1. J. A. Dobrowolski, K. M. Baird, P. D. Carman, and A. Waldorf, "Optical interference coatings for inhibiting of counterfeiting," *Opt. Acta* **20**, 925–937 (1973).
2. R. E. Reinnagel, "Method of forming copy resistant documents by forming an orderly array [P]," U. S. Patent No. 4,025,673 (1977).
3. G. Unnikrishnan and K. Singh, "Double random fractional Fourier-domain encoding for optical security," *Opt. Eng.* **39**, 2853–2859 (2000).
4. D. Abookasis, O. Arazi, and J. Rosen, "Security optical systems based on a joint transform correlator with significant output images," *Opt. Eng.* **40**, 1584–1589 (2001).
5. H. T. Chang, W. C. Lu, and C. J. Kuo, "Multiple-phase retrieval for optical security systems by use of random-phase encoding," *Appl. Opt.* **41**, 4825–4834 (2002).
6. H. T. Chang and C. T. Chen, "Asymmetric-image verification for security optical systems based on joint transform correlator architecture," *Opt. Commun.* **239**, 43–54 (2004).
7. B. Javidi and J. Horner, "Optical pattern recognition for validation and security verification," *Opt. Eng.* **33**, 1752–1756 (1994).
8. R. K. Wang, I. A. Watson, and C. Chatwin, "Random phase encoding for optical security," *Opt. Eng.* **25**, 2464–2469 (1996).
9. M. Yamazaki and J. Ohtsubo, "Optimization of encrypted holograms in optical security systems," *Opt. Eng.* **40**, 132–137 (2001).
10. N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," *J. Opt. Soc. Am. A* **16**, 1915–1927 (1999).
11. J. Ohtsubo and A. Fujimoto, "Practical image encryption and decryption by phase-coding techinique for optical security systems," *Appl. Opt.* **41**, 4848–4855 (2002).
12. K. Wu, J. Hu, and X. Wu, "Hybrid certificate validation technique based on Fresnel encoding," *Opt. Eng.* **47**, 098201 (2008).
13. M. Tebaldi, W. D. Furlan, R. Torroba, and N. Bolognini, "Optical-data storage-readout technique based on fractal encrypting masks," *Opt. Lett.* **34**, 316–318 (2009).
14. J. Tanida, A. Uemoto, and Y. Ichioka, "Optical fractal synthesizer: concept and experimental verification," *Appl. Opt.* **32**, 653–658 (1993).
15. T. Sasaki, H. Togo, J. Tanida, and Y. Ichioka, "Stream cipher based on pseudorandom number generation with optical affine transformation," *Appl. Opt.* **39**, 2340–2346 (2000).
16. J. Tanida and T. Sasaki, "Stream cipher using optical affine transformation," Chap. 12 in *Optical and Digital Techniques for Information Security*, B. Javidi, Ed., pp. 221–240, Springer, New York (2005).
17. M. F. Barnsley, *Fractals Everywhere*, Academic Press, Boston (1993).
18. T. Sasaki, J. Tanida, and Y. Ichioka, "Direct control of fractal pattern generation on an optical fractal systhesizer," *Appl. Opt.* **39**, 2959–2964 (2000).
19. J. Hutchinson, "Fractals and self-similarity," *Indiana Univ. Math. J.* **30**, 713–747 (1981).

Kenan Wu is a PhD student in the School of Electronic and Information Engineering, Dalian University of Technology. He got his BS and MS degrees from Dalian University of Technology. He is currently majoring in optical engineering.

Jiasheng Hu received his MS degree in applied optics in 1966 from Changchun Institute of Optics and Fine Mechanics, Academia Sinica, and became a professor in 1988. He was a visiting scholar and a visiting professor at the University of California, Santa Barbara, from 1980 to 1982 and in 1993, and he is currently a professor at the Dalian University of Technology. Hu has received various awards from the administration of China and the Academia Sinica, including the first prize for research and design of an optical processor for synthetic aperture radar and two second prizes for a laser scanning microscope and a multispectral imaging microscope. He was also named an Excellent Scientist in 1992 and 1997. Hu's main interests are novel imaging techniques, image processing, pattern recognition, and optical system design, and he has published more than 100 papers in these areas. He is a member of SPIE.



Xu Wu received his doctoral degree in optical engineering in 2006 from the School of Electronic and Information Engineering at the Dalian University of Technology, China. He is currently an assistant professor at the Dalian Maritime University. His research interests include optical security and counterfeit deterrence technique, image encryption, chaos theory, and optical/digital image processing. He has published nearly 20 papers in these areas.