Proceeding of the 2004 American Control Conference
Boston, Massachusetts June 30 - July 2, 2004

Secure Communication Using H_∞ Chaotic Synchronization and International Data Encryption Algorithm

Gwo-Ruey Yu
Department of Electrical Engineering
I-Shou University
Kaohsiung County 840, Taiwan
gwoyu@isu.edu.tw

Abstract – **In this paper, the international data encryption algorithm is applied to design the symmetric cryptosystem based on chaotic signals. Ciphertext are masked by means of the tent map. Plaintext could be recovered to the original signals through chaos synchronization. Since the H_∞ controller is robust, it can restrain effects of different initial values and variant system parameters between the transmitter and the receiver. To synchronize the tent map between the transmitter and the receiver, the controller is designed using H_∞ methodology. At last, the tent map cryptosystem are structured by combining the international data encryption algorithm and chaos synchronization and applied to the encryption of voice and picture. Computer simulations demonstrate that the cryptosystem based on cryptography and chaotic masking could promote the performance of information security.**

I. INTRODUCTION

For recent years, great attention has been devoted to the problem of synchronization of chaotic systems and its application to secure communication. Secure communication has been an important issue since the Internet and mobile phone are worldwide. The demands for privacy and security in wireless communication have led to the need for developing robust encryption schemes.

Chaotic systems are situated between deterministic systems and stochastic systems. The chaotic phenomena could be presented in many physical systems, such as hydrodynamics, laser optics, electric circuit and medicine. The characteristics of chaotic systems include broad-banded spectrum and unlimited period. By the way, it is difficult to predict the future response of chaotic systems due to the property of the sensitivity to initial conditions [1]. Therefore, chaotic signals are suitable to enhance the level of security through masking messages that are coded with classical encryption.

Increasing efforts have been made to study the chaos-based secure communication systems. Various methods have been proposed to make sure the data security using chaotic signals, for instance, chaotic switching [2], chaotic modulation [3] and chaotic masking [4]. Pecora and Carrol launched the concept of chaotic synchronization based on Lyapunov exponents [5]. To decrypt the masked signals, two chaotic systems have to be synchronized between the transmitter and the receiver. In [6], a nonlinear observer is utilized to estimate the states of the transmitter.

In this paper, the H_∞ methodology is employed to the problem of synchronization by dynamic compensation the receiver. The H_∞-optimization theory [7] has enlarged the repertoire of the tools available to design robust control. The synchronization schemes could be treated as the "model matching" problem between the transmitter and the receiver. The "model matching" problem is converted to the "standard 2-port H_∞" problem. We have proposed the best possible matching in the sense of the H_∞ norm of the closed loop transfer matrix from exogenous input to regulated output. The exogenous input comprises the nonlinear terms of chaotic dynamics and channel noise. The regulated output involves the synchronization error.

It has been shown that neither the chaotic switching method nor the chaotic masking method is secure [8]. An intruder can retrieve the encoded message from the transmitted chaotic signal by means of many different filtering technologies. The chaotic modulation method has a low level of security because the sensitivity of the secure communication systems is not satisfactory to the modelling error of the transmitter. To overcome the drawbacks, the conventional cryptography has been introduced to the chaos-based secure communication systems. In [9], the encrypter consists of a chaotic system and an encryption function; the plain signal is encrypted first using the n-shift cipher.

In this context, the International Data Encryption Algorithm (IDEA) is used as the encryption function to code the plaintext. The block cipher IDEA was presented by Lai and Massey in 1990 [10]. In this cipher, the plaintext and the ciphertext are processed in blocks of 64 bit, while the key length is 128 bit. The cipher relies on combining operations from three algebraic groups. The IDEA block cipher is one of the most important algorithms for network security, which offers the required confusion and diffusion [11]. Thus the chaotic cryptography systems has been designed by means of combining the IDEA cipher with H_∞ chaotic synchronization to promote the degree of security in this paper. First, the plaintext is encrypted by IDEA cipher. Second, the ciphertext is masked with a chaotic signal generated from the tent map. After the mixed signal transmitted through the public channel, the H_∞-optimization controller is utilized to solve the chaotic synchronization problem in the receiver. Last, the plaintext is recovered through the IDEA decipher.

The organization of this paper is as follows. Section 2 discusses the characteristic of IDEA and tent map. A cryptosystem based on chaos is proposed. Section 3 presents the computer simulations for the picture message

0-7803-8335-4/04/$17.00 ©2004 AACC

and the voice signal. The effectiveness of the design is revealed. Section 5 gives the conclusions.

II. CRYPTOSYSTEMS BASED ON CHAOS

The block diagram of the proposed chaotic cryptosystem is shown in Fig. 1. To enhance the level of security for the communication system, the encrypter consists of an encryption function and a chaotic dynamics in the transmitter. The encryption function and decryption function are defined as follows, respectively

$$c(n) = E(p(t), K(n)) \quad (1)$$

$$\hat{p}(t) = D(\hat{x}(n), KK(n)) \quad (2)$$

where $E(\cdot)$ is the encryption function IDEA, $D(\cdot)$ is the decryption function IDEA, $p(t)$ is the plaintext, $c(n)$ is the signal after encrypting, $\hat{x}(n)$ is the estimated signal, $\hat{p}(t)$ is the recovered text. Both the length of encrypted key $K(n)$ and the decrypted key $KK(n)$ are 128-bit.

The plaintext is first encrypted using the IDEA cipher and then it is masked with a chaotic signal generated from the tent map. The IDEA cipher is a kind of secret-key cryptosystems that is characterized by the symmetry of encryption and decryption processes. The design philosophy of this algorithm is based on the concept of mixing operations from different algebraic groups.

The IDEA is an iterated block cipher consisting of 8 rounds followed by an output transformation. Fig. 2 gives the architecture of one round in the encryption process [12]. The 64-bit plaintext block is partitioned into four 16-bit sub-blocks X_i (i = 1…4). During the ciphering process, three group operations are (1) bit by bit XOR (denoted as $\oplus$), (2) addition of integers modulo 2^{16} (denoted as $\boxplus$), and (3) multiplication of integers modulo $2^{16}+1$ (denoted as $\odot$). Each round produces four 16-bit output sub-blocks using six 16-bit sub-keys K_i (i = 1…6). There are totally 52 sub-keys of 16 bits adopted in the encryption process.

Finally, the remaining four 16-bit sub-keys are used in the output transformation to form the 64-bit ciphertext. The 52 sub-keys are generated from the 128-bit session-key according to a key schedule. The decryption process is similar to the encryption process except that different 16-bit sub-keys are used.

After the plaintext is encrypted through IDEA, the ciphertext is masked with a chaotic signal. The term “chaos” refers to complicated dynamic behavior. The Lyapunov exponent λ could be used to judge whether a system is chaotic or not:

$$\lambda(x_0) \equiv \lim_{n\to\infty} \frac{1}{n} \ln \left| \frac{df^n(x)}{dx} \Big|_{x_0} \right| \quad (3)$$

where f is the function of the system, x_0 is the initial value, n is the times of iteration. It has been be shown that a system is chaotic if $\lambda > 0$ [13].

One-dimensional maps provide a clearer idea of the qualitative behavior of chaotic systems and act as a good representative of higher dimensional and more complicated maps. Therefore, the tent map is chosen here to be an example of one-dimensional maps to illustrate the whole design idea.

The tent map $f_\mu : [0,\ 1] \to [0,\ 1]$ is defined by

$$\begin{aligned} x(n+1) &= f_\mu[x(n),\ \mu(n)] \\ &= \mu(n)(1 - 2\left|x(n) - \frac{1}{2}\right|) \end{aligned} \quad (4)$$

where μ is called the control parameter. An important feature of the tent map is the transition to chaos through a sequence of period doublings. Initially, for $0 < \mu < 0.5$, the attracting set consists of a single point that bifurcates into 2 points at $\mu = 0.5$. Subsequently, these points bifurcate again into four points. From the Lyapunov exponent of equation (3), it is known that the tent map exhibits chaotic phenomena for $\mu > 0.5$. The bifurcation phenomena are shown in Fig. 3.

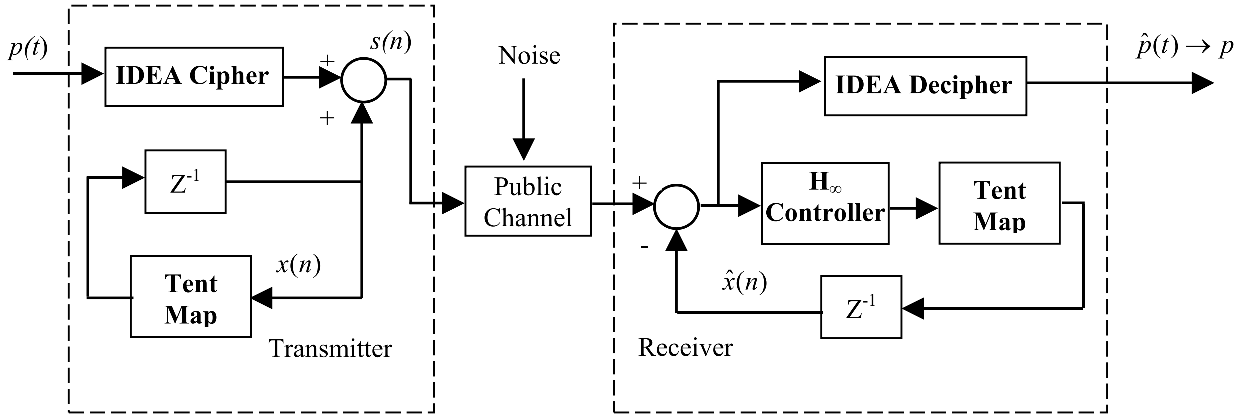

Fig. 1 Block diagram of the chaos-based secure system

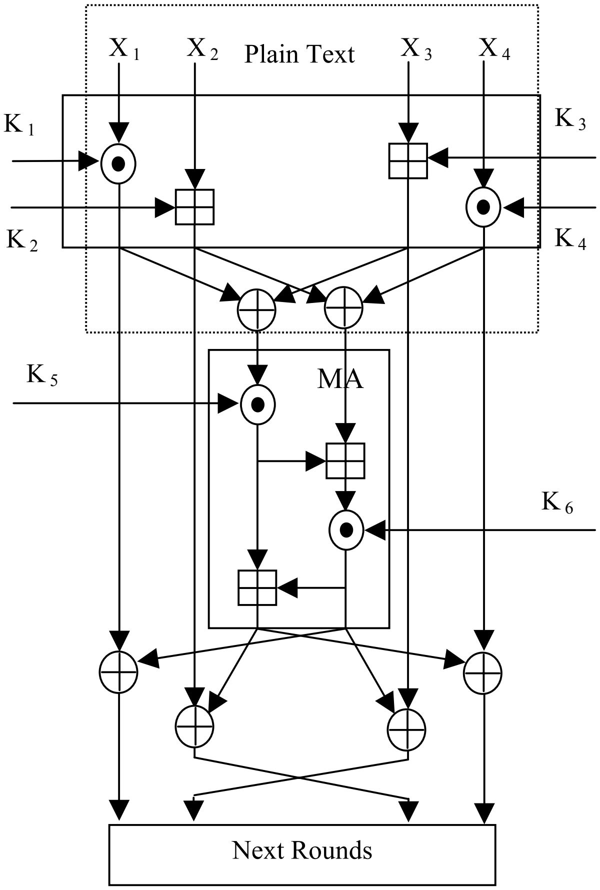

Fig. 2 IDEA architecture

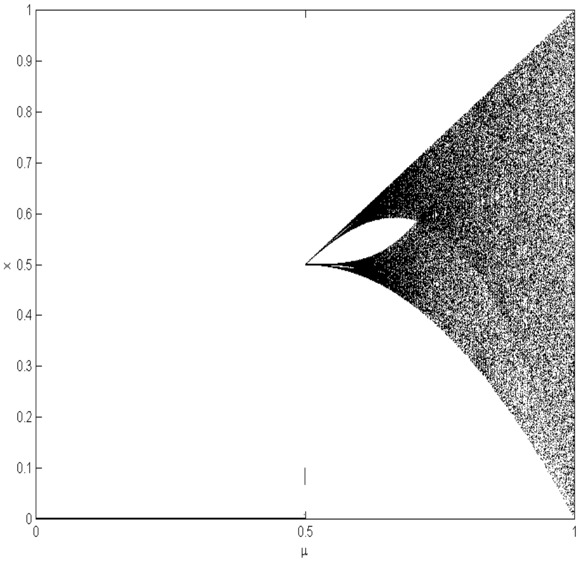

Fig. 3 Bifurcation of the tent map

The transmitted signal in the public channel is obtained by means of masking the ciphertext.

$$s(n) = x(n) + c(n) \tag{5}$$

Accordingly, the dynamic equations in the transmitter are

$$\begin{cases} x(n+1) = Ax(n) + f(x) \\ \quad y(n) = s(n) + N(n) \end{cases} \tag{6}$$

where $f(x)$ is the nonlinear terms of the tent map and $N(n)$ is the noise signal in the public channel. The estimated dynamic equations of the tent map at the receiver are designed as

$$\begin{cases} \hat{x}(n+1) = A\hat{x}(n) + f(\hat{x}) + u(n) \\ \quad \hat{y}(n) = \hat{x}(n) \end{cases} \tag{7}$$

where u is the output signal of the H$_\infty$ controller. The H$_\infty$-optimization theory has enlarged the repertoire of the tools available to design robust control. For example, in the mixed-sensitivity design formulation, both performance and robustness objectives can be incorporated. In this paper, the H$_\infty$ framework will be used to find the best possible matching between the transmitter and the receiver.

The synchronization error is defined as

$$e(n+1) = \hat{x}(n+1) - x(n+1) \tag{8}$$

The system is called synchronization if $e(n) \to 0$.

Substituting (6) and (7) into (9) yields

$$e(n+1) = Ae(n) + u(n) + f(\hat{x}) - f(x) \tag{9}$$

Let the dynamic equations of the synchronization error be augmented as the 2-port system shown in Fig. 4

$$\begin{cases} e(n+1) = Ae(n) + Bu(n) + \delta w(n) \\ \quad Z(n) = Ce(n) + u(n) \\ \quad Y(n) = e(n) \end{cases} \tag{10}$$

where $e(n)$ is the synchronization error, $u(n)$ is the control input, $\delta w(n)$ is the additive perturbation that occurs due to the nonlinear dynamics, $Z(n)$ is the weighted error, $Y(n)$ is the output. Let $T_{Z\delta w}$ be the closed loop transfer function from δw to Z . Let F be the transfer function of the linear controller connecting Y to u . The H$_\infty$ control problem is to choose the weighting function C such that the closed loop is internally stable and $\left\|T_{Z\delta w}\right\|_\infty \le \gamma$, where $\gamma \ge \gamma_{optimal}$.

The control effort that ensures $\left\|T_{Z\delta w}\right\|_\infty \le \gamma$ is given by

$$\begin{aligned} u(n) &= FY(n) \\ &= -B^T P \Lambda^{-1} AY(n) \end{aligned} \tag{11}$$

where

$$\Lambda = I + (BB^T - \gamma^{-2} I)P \tag{12}$$

and P is the positive definite solution to the generalized algebraic Riccati equation

$$C^T C + A^T P \Lambda^{-1} P - P = 0 \tag{13}$$

Once the chaotic synchronization is achieved, the plaintext could be recovered through the IDEA decipher.

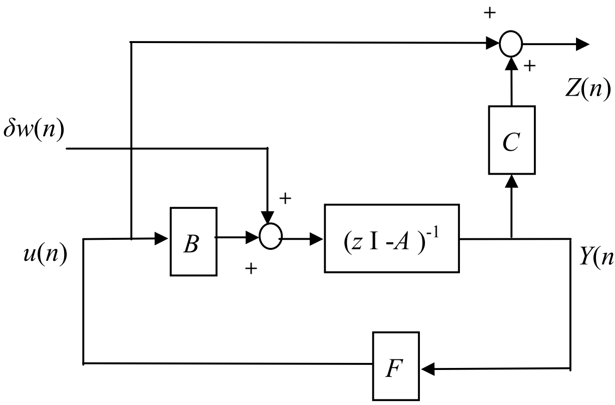

Fig. 4 Block diagram of H∞ controller

III. COMPUTER SIMULATIONS

The plaintext is coded using the IDEA cipher. The 128-bit secret key is divided into eight 16-bit sub-keys. For example, one of the 16-bit sub-keys is chosen as (3, 7, 2, 9, 1, 1, 8, 5, 4, 9, 6, 4, 7, 7, 3, 2). The 128-bit secret key is then rotated left by 25 bits and is divided into eight 16-bit sub-keys again. The procedure is iterated until 52 sub-keys are acquired. The cipher text is masked with a tent map. Let the tent map be selected as

$$x(n+1) = \mu(1 - 2\left|x(n) - \frac{1}{2}\right|) \qquad (14)$$

where $\mu = 0.8$, $x(0) = 0.3$.

After the H∞ chaotic synchronization, the palintext is retrieved through the IDEA decipher. The decryption sub-keys could be calculated from the encryption sub-keys. The encryption sub-keys and decryption sub-keys are listed in Table 1 and Table 2 respectively.

To demonstrate the effectiveness of the design, three examples are given. Figure 5(a) shows the plaintext of a two-dimensional photo. Figure 5(b) is the ciphertext coded through IDEA. Figure 5(c) is the ciphertext masked with the chaotic signal. Figure 5(d) shows the recovered signal. Obviously, the security of the system will be not enough if the signal is encrypted via IDEA only. Figure 5 and Figure 6 illustrate different order of encryption. Figure 6(a) shows the plaintext of Saturn photo. Figure 6(b) is the image masked with the tent map. Figure 6(c) is the ciphered image via IDEA. Figure 6(d) shows the recovered image. To study the robustness of the proposed cryptosystem, noise is given in the public channel of Figure 7. Figure 7(a) shows the plaintext of Handel's opera. Figure 7(b) is the noise signal. Figure 7(c) is the ciphertext masked with the chaotic signal. Figure 7(d) shows the recovered signal. Simulation results reveal that the chaos-based secure systems have the advantages of avoiding detection and intercept.

IV. CONCLUSIONS

In this paper, a cryptosystem based on tent map is presented. The plaintext is first encrypted via the IDEA cipher. The H∞ framework is applied to solve the chaotic synchronization problem between the transmitter and the receiver. The digital image and the sound wave could be recovered to original signals. The proposed scheme promotes the degree of security in communication.

Table 1. IDEA encryption sub-keys

	Encryption sub-keys
1 round	$K_1\ K_2 K_3\ K_4 K_5\ K_6$
2 round	$K_7\ K_8 K_9\ K_{10} K_{11}\ K_{12}$
3 round	$K_{13}\ K_{14} K_{15}\ K_{16} K_{17}\ K_{18}$
4 round	$K_{19}\ K_{20} K_{21}\ K_{22} K_{23}\ K_{24}$
5 round	$K_{25}\ K_{26} K_{27}\ K_{28} K_{29}\ K_{30}$
6 round	$K_{31}\ K_{32} K_{33}\ K_{34} K_{35}\ K_{36}$
7 round	$K_{37}\ K_{38} K_{39}\ K_{40} K_{41}\ K_{42}$
8 round	$K_{43}\ K_{44} K_{45}\ K_{46} K_{47}\ K_{48}$
Transformation	$K_{49}\ K_{50} K_{51}\ K_{52}$

Table 2. IDEA decryption sub-keys

	Decryption sub-keys
1 round	$K_{49}^{-1} - K_{50} - K_{51}\ K_{52}^{-1}\ K_{47}\ K_{48}$
2 round	$K_{43}^{-1} - K_{45} - K_{44}\ K_{46}^{-1}\ K_{41}\ K_{42}$
3 round	$K_{37}^{-1} - K_{39} - K_{38}\ K_{40}^{-1}\ K_{35}\ K_{36}$
4 round	$K_{31}^{-1} - K_{33} - K_{32}\ K_{34}^{-1}\ K_{29}\ K_{30}$
5 round	$K_{25}^{-1} - K_{27} - K_{26}\ K_{28}^{-1}\ K_{23}\ K_{24}$
6 round	$K_{19}^{-1} - K_{21} - K_{20}\ K_{22}^{-1}\ K_{17}\ K_{18}$
7 round	$K_{13}^{-1} - K_{15} - K_{14}\ K_{16}^{-1}\ K_{11}\ K_{12}$
8 round	$K_7^{-1} - K_9 - K_8\ K_{10}^{-1}\ K_5\ K_6$
Transformation	$K_1^{-1} - K_2 - K_3\ K_4^{-1}$

V. ACKNOWLEDGMENTS

This research is sponsored by means of the National Science Council of the Republic of China, under Grant NSC-92-2213-E-214-014.

VI. REFERENCES

[1] S. N. Rasband, *Chaotic Dynamics of Nonlinear Systems*, A Wiley-Interscience Publication, New York, 1989.

[2] T. Yang, "Recovery of Digital Signals from Chaotic Switching", *Int. J. Circuit Theory Appl.*, Vol. 23, No. 6, 1995, pp. 611-615.

[3] H. Leung and J. Lam, "Design of Demodulator for the Chaotic Modulation Communication System", *IEEE Trans. Circuits Syst.*, Vol. 44, Mar. 1997, pp. 262-267.

[4] C. Zhou and T. Chen, "Extracting Information Masked by Chaos and Contaminated with Noise: Some Considerations on the Security of Communication Approaches Using Chaos", *Phys. Lett. A*, Vol. 234, 1997, pp. 429-435.

[5] T. L. Carroll and L. M. Pecora, "Synchronization in Chaotic Systems", *IEEE Trans. Circuits Sys. I*, Vol. 38, 1991, pp. 453-456.

[6] G. Grassi and S. Mascolo, "Nonlinear Observer Design to Synchronize Hyperchaotic Systems via a Scalar Signal", *IEEE Trans. Circuits Syst. I*, Vol. 44, Oct. 1997, pp. 1011-1014.

[7] J. Doyle, K. Glover, P. Khargonekar and B. Francis, "State Space Solutions to Standard H_2 and H_∞ Control Problems", *IEEE Trans. on Automatic Control*, AC-24(8): August l988, pp. 731-747.

[8] M. S. Baptista, "Cryptography with Chaos", *Physical Letters A*, Vol.240, 1998, pp.50-54.

[9] T. Yang, C. W. Wu and L. O. Chua, "Cryptography Based on Chaotic Systems", *IEEE Trans. Circuits Sys.*, Vol.44, 1997, pp.469-472.

[10] X. Lai and J. Massey, "A Proposal for a New Block Encryption Standard", *Advances in Cryptology – EUROCRYPT '90*, 1991, pp.389-404.

[11] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Upper Saddle River, NJ: Prentice-Hall, 1999.

[12] E. Biham, and *A.* Shamir, *Differential Cryptanalysis of the Data Encryption Standard.* New York: Springer-Verlag, 1993.

[13] A. Hammad, E. Johckheere, C. -Y. Cheng, S. Bhajekar and C. -C. Chien, "Stabilization of Chaotic Dynamics: a Modern Control Approach", *International Journal of Control*, Vol. 64, No.4, 1996, pp.663-667.

[14] Gwo-Ruey Yu, "Pole-Placement Control of the Tent Map by Gray Prediction", Proceedings of 2002 *IEEE International Conference on Industrial Technology*, pp. 1122-1127.

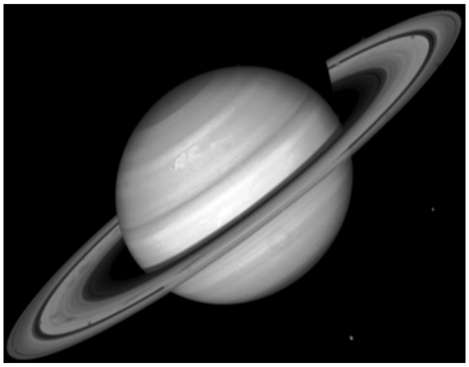

Fig. 5(a) Plaintext

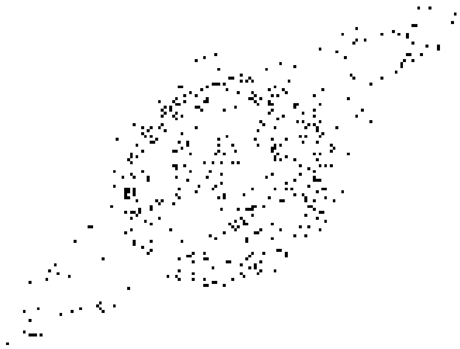

Fig. 5(b) Ciphertext

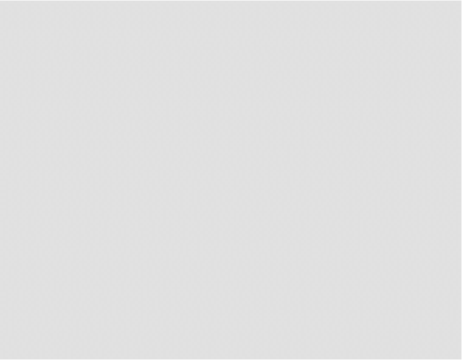

Fig. 5(c) Ciphertext with chaos

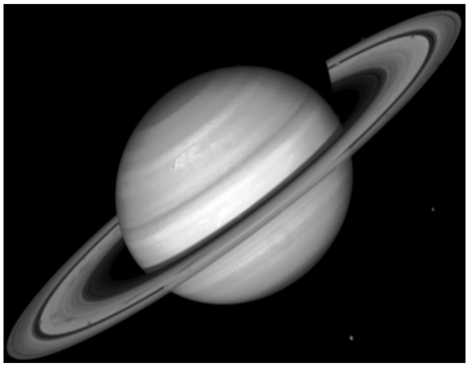

Fig. 5(d) Recovered plaintext

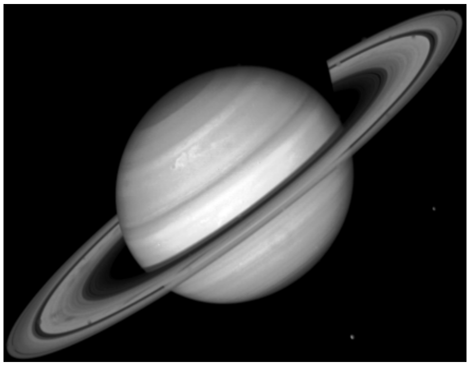

Fig. 6(a) Plaintext

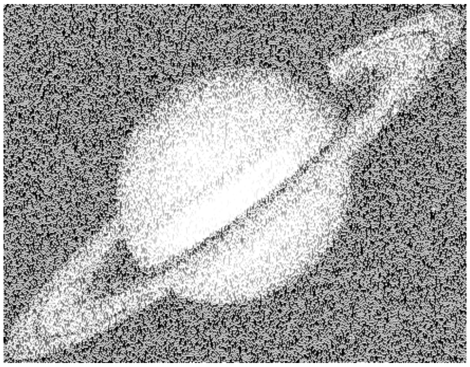

Fig.6(b) Plaintext with chaos

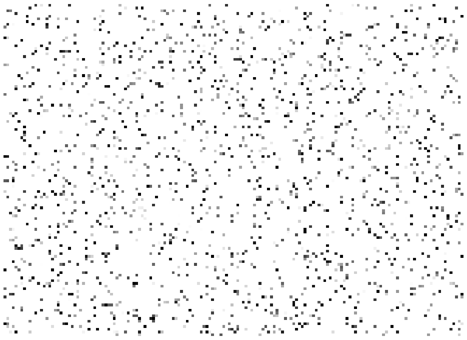

Fig. 6(c) Ciphertext via IDEA

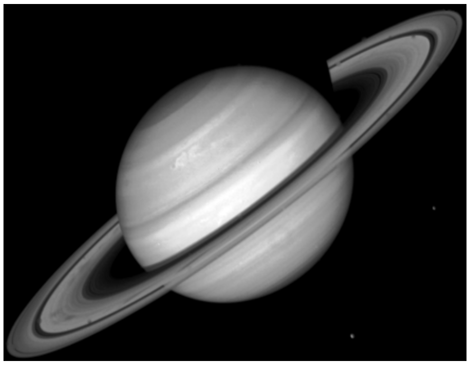

Fig. 6(d) Recovered plaintext

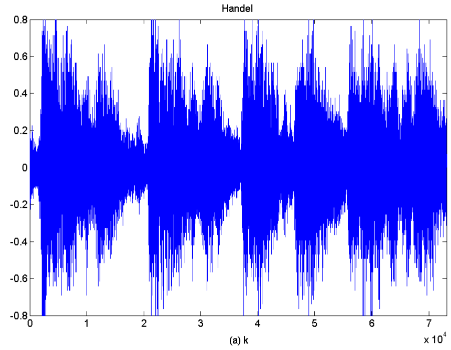

Fig. 7(a) Plaintext

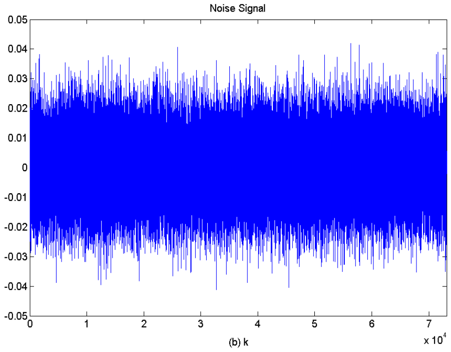

Fig. 7(b) Noise signal

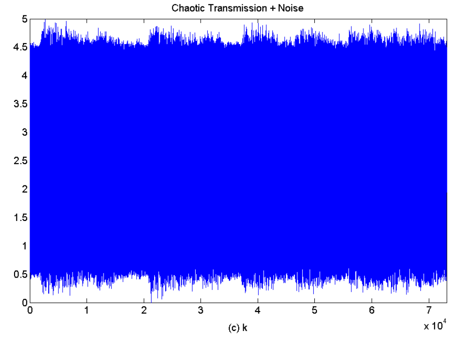

Fig. 7(c) Plaintext with chaos

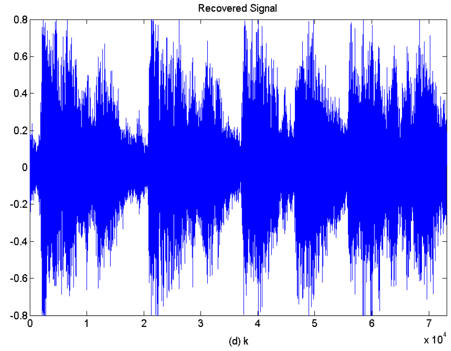

Fig. 7(d) Recovered plaintext