CRYPTOGRAPHY BASED ON CHUA'S CIRCUITS

by

Tao Yang, Chai Wah Wu, and Leon O. Chua

Memorandum No. UCB/ERL M97/6

17 January 1997

CRYPTOGRAPHY BASED ON CHUA'S CIRCUITS

by

Tao Yang, Chai Wah Wu, and Leon O. Chua

Memorandum No. UCB/ERL M97/6

17 January 1997

ELECTRONICS RESEARCH LABORATORY

College of Engineering
University of California, Berkeley
94720

Cryptography Based on Chua's Circuits

Tao Yang[*], *Chai Wah Wu* and *Leon O. Chua*
Electronics Research Laboratory and
Department of Electrical Engineering and Computer Sciences,
University of California at Berkeley,
Berkeley, CA 94720, U.S.A.

Abstract

In this letter, a new chaos-based secure communication scheme is proposed in an attempt to thwart the attacks proposed recently[2,8]. Instead of encoding the message signal in a chaotic system directly, we use two chaotic signals in our scheme. One of the chaotic signals is used to synchronize the chaotic encrypter and the chaotic decrypter. The other is used to encrypt the plain signal by using a multi-shift cipher scheme. Thus the transmitted signal is not used to encrypt the message and a more complicated method of encryption is used.

1 Introduction

Recently, there has been much interest in the use of two synchronized chaotic systems for the purpose of secure communication. A chaotic signal is spread-spectrum and can hide a small message signal in spectral domain[6]. However, in the time domain, a chaotic system can be easily identified by using one of its state variables[1-5].

The authors of [2] and [7] found that the additive masking method and the chaotic switching method are not secure. Also, the parameter methods (either using message signal to modulate a parameter or change a state-variable) have a low security[8,9].

All the attacks proposed in [2] and [7-9] are based on the fact that the chaos-based secure communication systems are not sensitive enough to the modeling error of the transmitter. So, an intruder can recover the message signal by using an approximate model with some errors which can be easily removed by standard filtering methods. To defense itself against these attacks, a chaos-based cryptosystem is proposed in this letter. Our method is much more sensitive to the recovering errors and the modeling errors, so the level of security is enhanced. Furthermore, state variables other than the transmitted variable is used in the encrypter (as was done in [13]), thwarting attacks which reconstructs only the transmitted variable[2],[8].

[*]Visiting scholar on leave from the Department of Automatic Control Engineering, Shanghai University of Technology, 149 Yan Chang Road, Shanghai 200072, P.R.China

2 Chaotic cryptosystem

A chaotic cryptosystem is shown in Fig.1. In Fig.1, the encrypter consists of a chaotic system and an encryption function e(). The key signal $k(t)$ is one of the state variables of the chaotic system. Another state variable $s(t)$ is the transmitted signal, which is transmitted through a public channel to the decrypter and used to synchronize the decrypter. $y(t)$ is the encrypted signal which is fed back into the chaotic system.

The decrypter consists of a chaotic system and a decryption function $d()$. The decrypter can find the key signal when the decrypter and the encrypter are synchronized. The encrypted signal is also recovered via synchronization. Then, $d()$ is used to decrypt the encrypted signal.

It should be noted that in the scheme shown in Fig.1, both the key signal $k(t)$ and the encrypted signal $y(t)$ are not transmitted to the decrypter. It is different from the traditional discrete cryptosystem where both the key and the encrypted signal should be transmitted to the decrypter[12].

We use Chua's circuits, which exhibits double scroll chaotic attractors, to implement one such chaotic cryptosystem as shown in Fig.2. $v_R(t)$ is the transmitted signal. $v_2(t)$ is the key signal. $p(t)$ denotes the plain text signal (the message signal). The state equations of this cryptosystem are:

Encrypter:

$$\begin{cases} \frac{dv_1}{dt} = \frac{1}{C_1}[G(v_2 - v_1) - f(v_R)] \\ \frac{dv_2}{dt} = \frac{1}{C_2}[G(v_1 - v_2) + i_3] \\ \frac{di_3}{dt} = \frac{1}{L}[-v_2] \end{cases} \tag{1}$$

where $f()$ is the nonlinear characteristics of Chua's diode in Chua's circuit given by:

$$f(v_1) = G_b v_1 + \frac{1}{2}(G_a - G_b)(|v_1 + E| - |v_1 - E|) \tag{2}$$

and E is the breakpoint voltage of Chua's diode. The voltage v_R is given by:

$$v_R = v_1 - e(p(t)) \tag{3}$$

where $e(p(t))$ is the encrypted signal.

Decrypter:

$$\begin{cases} \frac{d\tilde{v}_1}{dt} = \frac{1}{C_1}[G(\tilde{v}_2 - \tilde{v}_1) - f(v_R)] \\ \frac{d\tilde{v}_2}{dt} = \frac{1}{C_2}[G(\tilde{v}_1 - \tilde{v}_2) + \tilde{i}_3] \\ \frac{d\tilde{i}_3}{dt} = \frac{1}{L}[-\tilde{v}_2] \end{cases} \tag{4}$$

$$\tilde{e}(p(t)) = \tilde{v}_1 - v_R \tag{5}$$

where $\tilde{e}(p(t))$ is the recovered encrypted signal. A sufficient condition of synchronizing systems (1) and (4) are $C_1 > 0, C_2 > 0, G > 0, L > 0$[10]. Since this synchronization configuration of two Chua's

circuits is error-free, we have $\tilde{e}(p(t)) \longrightarrow e(p(t))$ when the synchronization is achieved.

We use an n-shift cipher to encrypt the plain signal. The n-shift cipher is given by:

$$e(p(t)) = \underbrace{f_1\Big(...f_1\Big(f_1}_{n}\Big(p(t), \underbrace{v_2(t)\Big), v_2(t)\Big), ..., v_2(t)\Big)}_{n} = y(t) \tag{6}$$

where h is chosen such that $p(t)$ and $v_2(t)$ lie within $(-h, h)$. And $f_1(*,*)$ is the following nonlinear function:

$$f_1(x,k) = \begin{cases} (x+k) + 2h, & -2h \leq (x+k) \leq -h \\ (x+k), & -h < (x+k) < h \\ (x+k) - 2h, & h \leq (x+k) \leq 2h \end{cases} \tag{7}$$

This function is shown in Fig.3.

The corresponding decryption rule is the same as the encryption rule

$$p(t) = d(y(t)) = e(y(t)) = \underbrace{f_1\Big(...f_1\Big(f_1}_{n}\Big(y(t), \underbrace{-\tilde{v}_2(t)\Big), -\tilde{v}_2(t)\Big), ..., -\tilde{v}_2(t)\Big)}_{n} \tag{8}$$

where $\tilde{v}_2(t)$ is recovered in the receiver circuit and should approximate $v_2(t)$.

In the n-shift cipher, the key signal $v_2(t)$ is used for n times to encrypt the plain signal. Since the encrypted signal is a function of $v_2(t)$ and $p(t)$, and since the encrypted signal is used to drive the Chua's circuit, it hides both the dynamical and the statistical characteristics of both $v_2(t)$ and $p(t)$.

3 Simulation results

In this section, we study the performance of the attack proposed in [8] to the chaotic cryptosystem. In all of the following simulations, the following parameters are used: $C_1 = 5.56nF$, $C_2 = 50nF$, $G = 0.7mS$,$L = 7.14mH$, $G_a = -0.8mS$, $G_b = -0.5mS$, $E = 1V$. The initial conditions are ($v_1(0)$, $v_2(0)$, $i_3(0)$) = ($-0.2V$, $-0.02V$, $0.1mA$) and ($\tilde{v}_1(0)$, $\tilde{v}_2(0)$, $\tilde{i}_3(0)$) = ($0.02V$, $-0.12V$, $-0.1mA$), respectively. So, the encrypter and the decrypter are initial desynchronized. $h = 0.4V$. A 30-shift cipher is used (n=30).

First, we show the performance of our cryptosystem. Fig.4 shows the results when a sinusoidal signal is encrypted. Fig.4(a) shows the transmitted signal $v_R(t)$. Fig.4(b) shows the recovered and then decrypted signal. One can see that the plain signal is decrypted perfectly except for the first $8ms$, which is needed to synchronize both Chua's circuits.

Suppose that an intruder can successfully reconstruct the dynamics of the transmitted signal. By repeating the method proposed in [8], we find the best recovered message signal has a $SNR \approx 20dB$. This SNR is high enough for an intruder to find the sinusoidal signal from the recovered result when the chaotic secure communication scheme proposed in [10] is used. But the following simulation shows

that this SNR is too low to decrypt the recovered encrypted signal when the scheme shown in Fig.2 is used. Fig.4(c) shows the recovered encrypted signal using method in [8]. Since the encrypted signal is a very good pseudo-random signal, which almost distributes uniformly in the full frequency range, no standard filtering method can be used to enhance the SNR of the encrypted signal. Next suppose that the intruder can successfully reconstruct $v_2(t)$ with a $SNR = 20dB$. Then the decrypted signal is shown in Fig.4(d), from which one can see that the intruder can't find the plain signal.

We then study the effects of parameter mismatch. We first consider the mismatch of parameter h. Fig.5(a) shows the decrypted signal when h in the decrypter has a $0.01V$ mismatch. One can see that the plain signal is hard to be recovered from this decrypted result. However, when h has a mismatch smaller than $5mV$, the plain signal can be easily recovered from the decrypted signal. We then study the cases when G is mismatched. Fig.5(b) shows the decrypted signal when G has a 1% mismatch, one can see that the plain signal is hard to be recovered from this result. When G has a mismatch smaller than 0.05%, the plain signal can be recovered from the decrypted signal by using low-passed filter. If G has a mismatch between $0.05\% - 0.1\%$, the plain signal can also be recovered by using some spectral analysis methods. When mismatch is above 1%, it is hard to recover the plain signal.

4 Conclusions

We present here a secure communication system which thwarts attack schemes presented in the literatures. In particular, we use an encryption rule which is very sensitive to the accuracy in the recovered signal. Furthermore, we use state variables other than the transmitted state variables for encryption. Using the current method, the intruder can only recover the encrypted signal with an accuracy which is too low to decrypt the recovered encrypted signal. Furthermore, the intruder also need to reconstruct the key signal which is different from the transmitted signal by using some reconstruction methods which have not been reported so far.

References

[1]U.Parlitz, R.Zoller, J.Holzfuss and W.Lauterborn, "Reconstructing physical variables and parameters from dynamical systems," *International Journal Bifurcation and Chaos*, vol.4, no.6, pp.1715-1719, 1994.

[2]]K.Short, "Steps toward unmasking secure communications," *International Journal Bifurcation and Chaos*, vol.4, no.4, pp.959-977, 1994.

[3]L.Aguirre and S.Billings, "Retrieving dynamical invariants from chaotic data using NARMAX models," *International Journal Bifurcation and Chaos*, vol.5, no.2, pp.449-474, 1995.

[4]S.Haykin and X.Li, "Detecting of signals in chaos," *Proceedings of the IEEE*, vol.83, no.1, pp.95-122, Jan.1995.

[5]J.Stark and B.Arumugam, "Extracting slowly varying signals for a chaotic background," *International Journal Bifurcation and Chaos*, vol.2, no.2, pp.413-419, 1992.

[6]K.Halle, C.W.Wu M.Itoh and L.O.Chua, "Spread spectrum communication through modulation of chaos," *International Journal Bifurcation and Chaos*, vol.3, no.2, pp.469-477, 1992.

[7]T.Yang, "Recovery of digital signals from chaotic switching," *International Journal of Circuit Theory and Applications*, vol.23, no.6, pp.611-615, Nov.-Dec. 1995.

[8]K.Short, "Unmasking a modulated chaotic communications scheme," *International Journal Bifurcation and Chaos*, vol.6, no.2, pp.367-375, 1996.

[9]C.W.Wu, T.Yang and L.O.Chua, "On adaptive synchronization and control of nonlinear dynamical systems," *International Journal Bifurcation and Chaos*, vol.6, no.3, pp.455-471, 1996.

[10]C.W.Wu and L.O.Chua, "A simple way to synchronize chaotic system with applications to secure communication systems," *International Journal Bifurcation and Chaos*, vol.3, no.6, pp.1619-1627, 1993.

[11]L.O.Chua, "Chua's circuit— An overview ten years later," *Journal of Circuit, Systems, and Computers*, vol.4, no.2, pp.117-159, Jan.1994.

[12]D.Stinson, *Cryptography: Theory and Practice*, CRC Press, Baca Raton: 1995.

[13]C.W.Wu and L.O.Chua, "A unified framework for synchronization and control of dynamical systems," *International Journal Bifurcation and Chaos*, vol.4, no.4, pp.979-998, 1994.

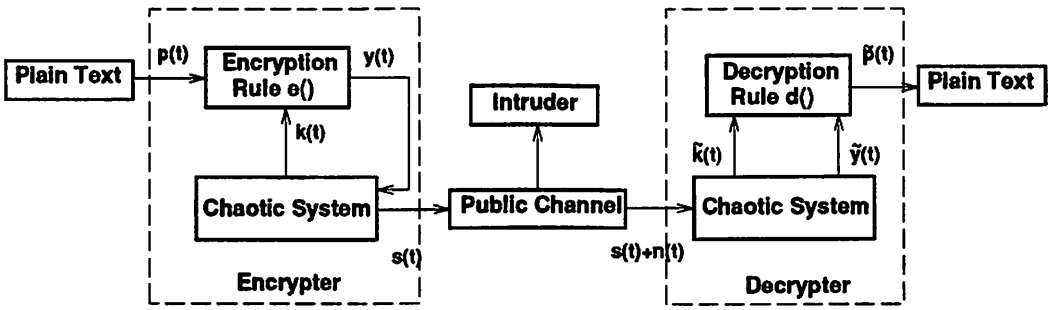


Figure 1: Block diagram of the chaotic cryptosystem.

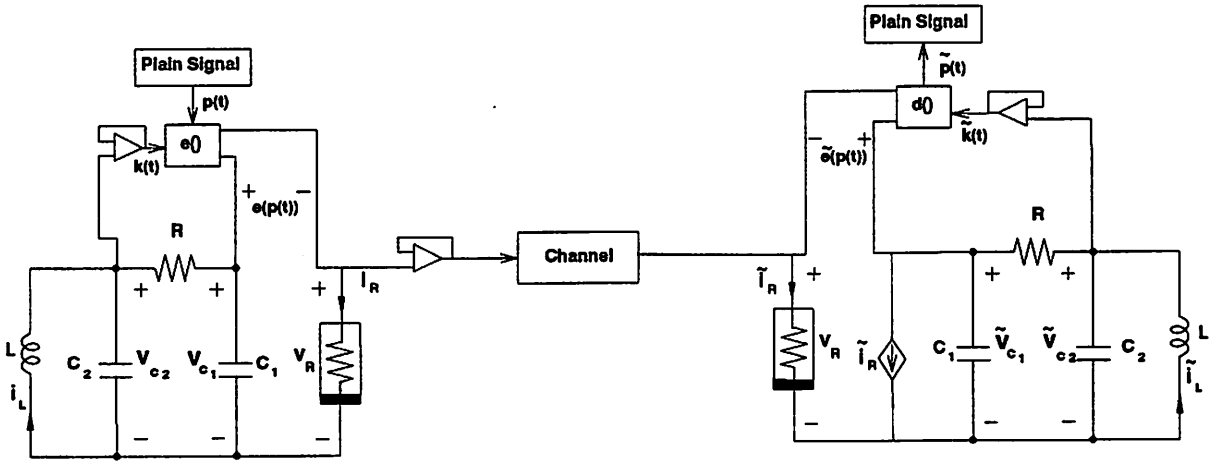


Figure 2 Block diagram of the Chua's circuits based cryptosystem.

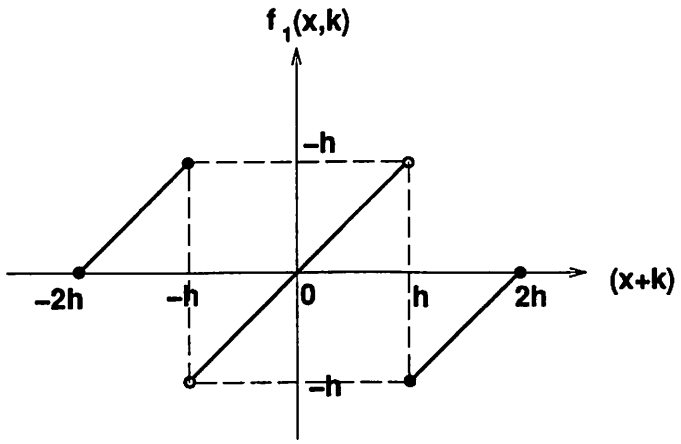
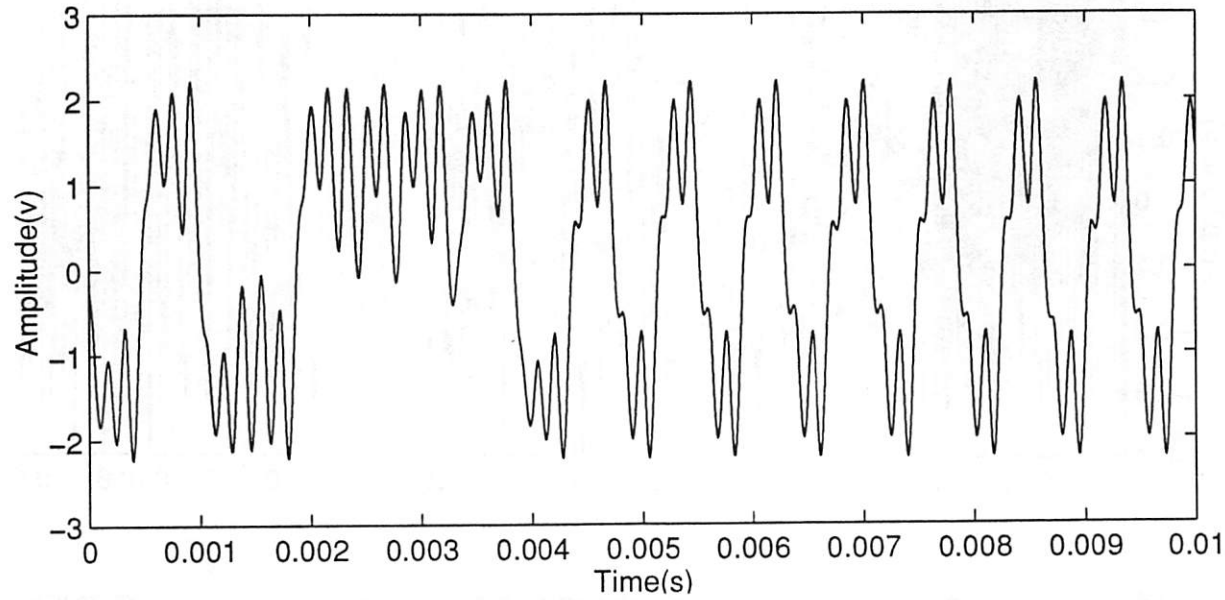
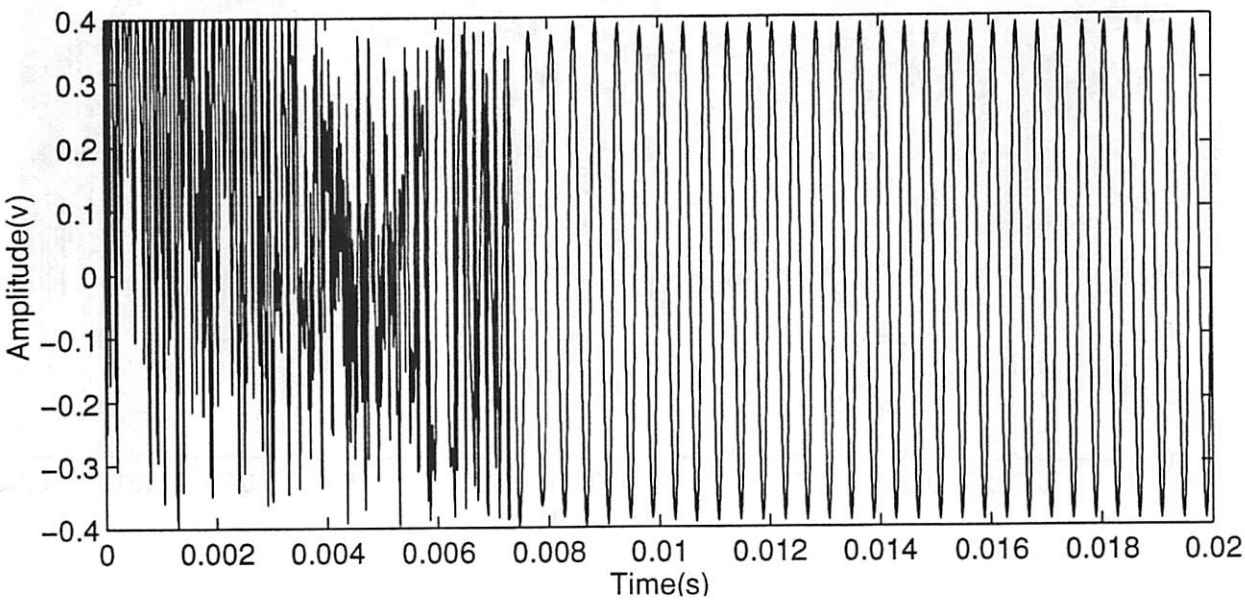


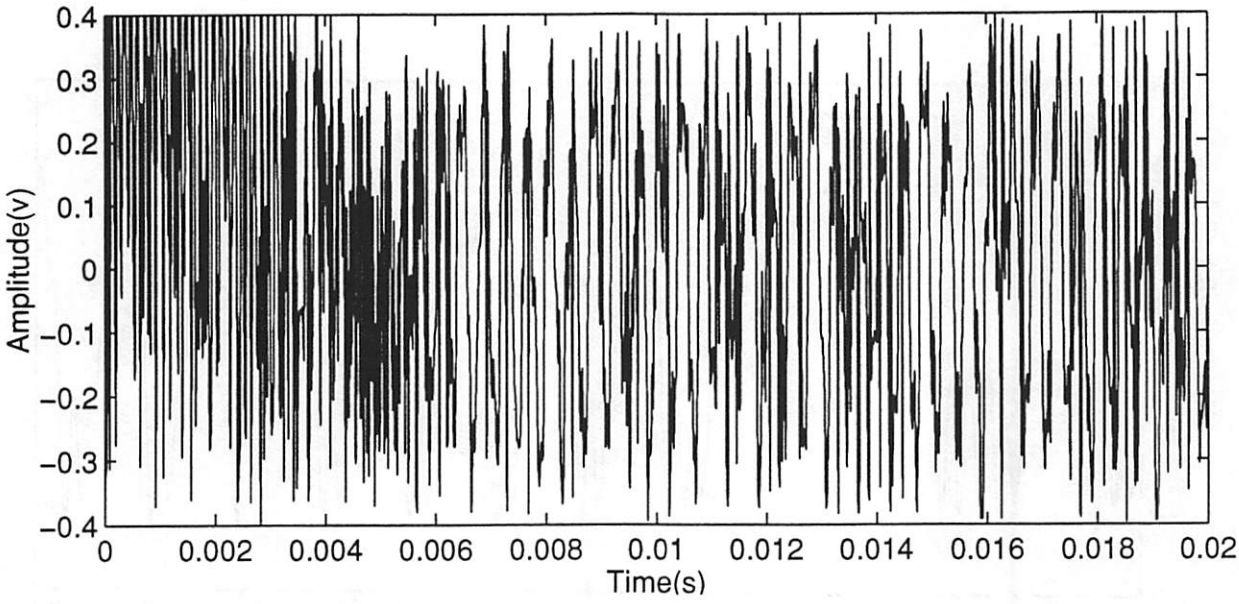
Figure 3 Nonlinear function used in continuous shift cipher.


3
2
1
0
−1
−2
−3
Amplitude(v)
0
0.001
0.002
0.003
0.004
0.005
0.006
0.007
0.008
0.009
0.01
Time(s)

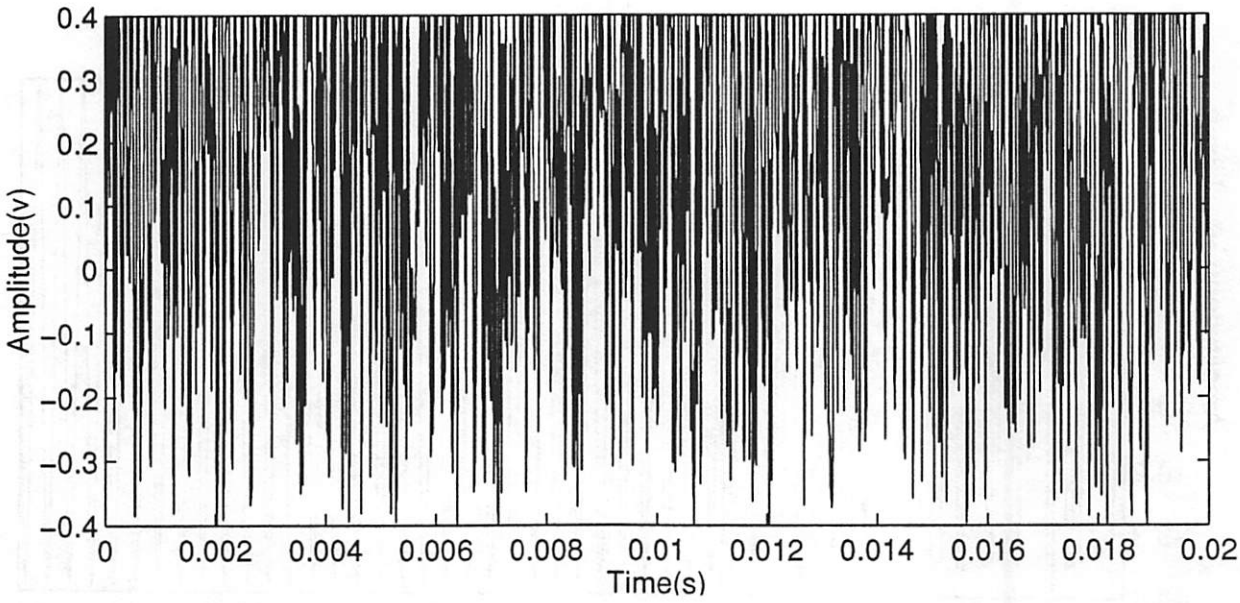
(a)


0.4
0.3
0.2
0.1
0
−0.1
−0.2
−0.3
−0.4
Amplitude(v)
0
0.002
0.004
0.006
0.008
0.01
0.012
0.014
0.016
0.018
0.02
Time(s)

(b)

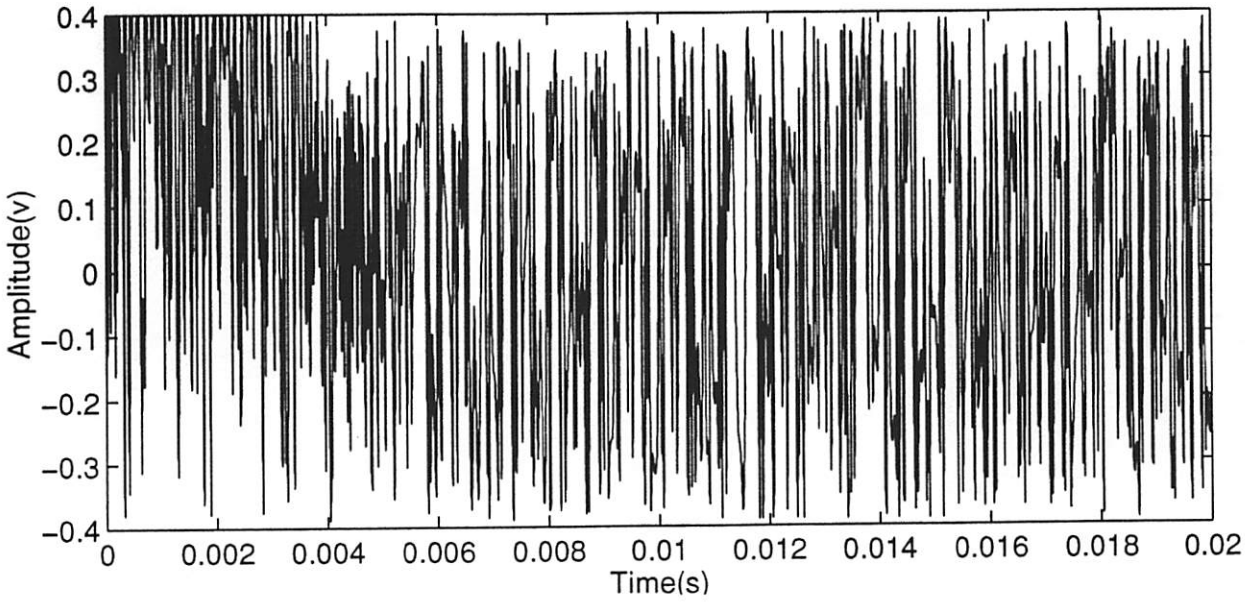


(c)

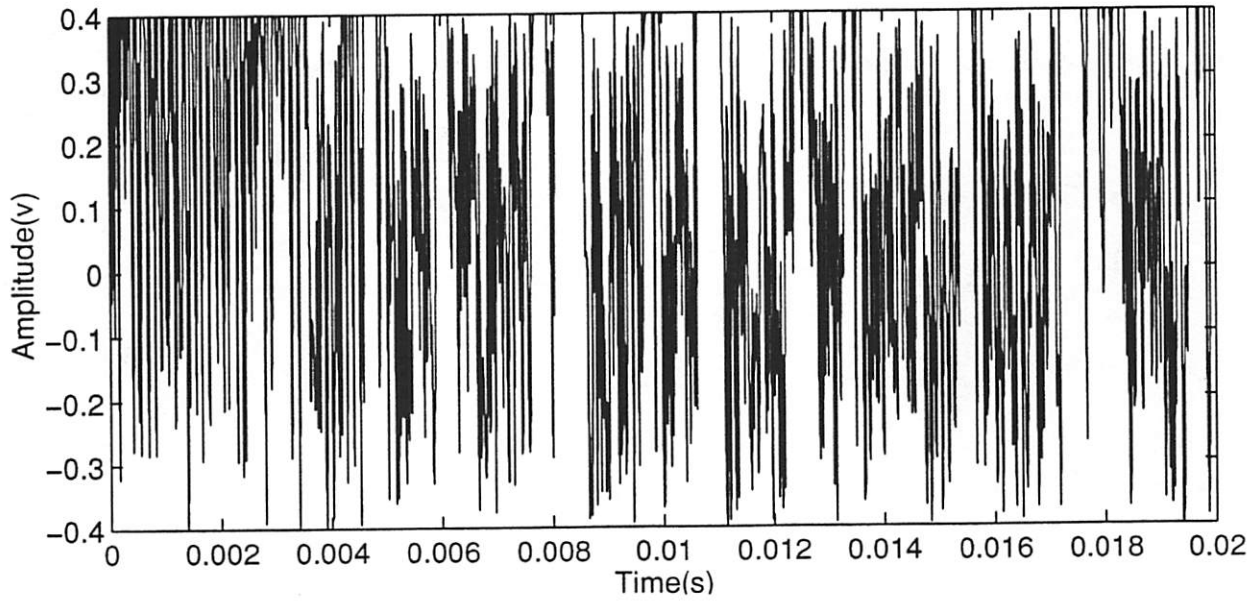


(d)

Figure 4 (a) The transmitted signal. (b) The recovered and then decrypted signal. (c) The recovered encrypted signal using the method in [8]. (d) The decrypted result of that shown in Fig.4(c).



(a)



(b)

Figure 5 (a) The decrypted signal when $0.01V$ *mismatch of* h *exists. (b) The decrypted signal when* 1% *mismatch of* G *exists.*