Journal of Information Security and Applications 000 (2017) 1–8

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Securing digital voice communication using non-autonomous modulated chaotic signal

Mahmoud F. Abd Elzaher[a,*], Mohamed Shalaby[b], Yasser Kamal[b], Salwa El Ramly[a]

[a] Department of Electronics and Electrical communications, Ain Shams University, Cairo, Egypt
[b] Department of Computer Science, Arab Academy for Science, Technology, Maritime Transport, Cairo, Egypt

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Voice encryption
Chaotic modulation
Non-autonomous modulation
Lorenz chaotic flow
Qi hyperchaotic flow

ABSTRACT

In this paper, we present an encryption approach for voice communication systems based on direct chaotic modulation (non-autonomous modulation), in which voice is injected into one variable of the master system (using either Lorenz chaotic flow or Qi hyperchaotic flow) without changing the value of any control parameter. This approach is based on the change of chaotic signal by injecting voice samples into one variable in chaotic system and hence generating a new chaotic signal. The voice signal is then extracted from the chaotic signal in the receiver side. Furthermore, we use a high dimension chaotic flow which increases the security of the encrypted signal. Non-autonomous modulation technique is suitable for secure real-time applications. We also presented a comparative study between the two approaches with their conventional chaotic masking counterparts. Experimental results show that non-autonomous methods give better performance than their chaotic masking counterparts when they are analyzed against Signal-to-Noise-Ratio (−38.55 dB vs. 38.51 dB and 59.22 dB vs. 58.11 dB), Segmental signal-to-Noise-Ratio (38.91 dB vs. 38.84 dB and 54.20 dB vs. 53.16 dB), Log-Likelihood Ratio (0.88 vs. 0.80 and 1.59 vs. 1.50), and Correlation Coefficient Analysis (0.0345 vs. 0.021 and 0.0002 vs. 0.01012). Statistical analyses show that the second proposed approach has the best results for the encrypted signal. Modifying conventional chaotic approaches increases the security of the encryption system.

© 2017 Elsevier Ltd. All rights reserved.

1. Introduction

Nowadays multimedia applications such as video and voice are crucial, and their service is the foundation of the telephone industry, video conference, and broadcast news. Thus, securing such systems is very important to overcome intrusion and eavesdropper attacks. Modern voice communication systems demand a huge amount of information to be exchanged across local networks and the Internet every day so our need for encryption and security has increased. The conventional cryptographic techniques may be efficient for the text data, however, they are unsuitable to the bulk data capacity. One of the techniques that provide fast and highly secure encryption methods is chaos-based techniques.

Continuous cryptographic systems have been developed which use the synchronization between the transmitter and receiver to retrieve data transmitted through an insecure medium. The first generation of these systems is masking. A voice masking technique based on Lorenz System is presented in [1] which uses Lorenz equation to generate chaotic signals, these signals are used as a base carrier signal on which the information signal is modulated at the transmitter side. The information signal is then recovered at the receiver side. In [2] the authors presented a technique of speech masking with feedback and recovery information using Lorenz chaotic flow. The results obtained showed that this technique provides higher security and immunity against noise than the technique presented in [1]. The method of masking has been shown to be insecure as there are various cryptanalysis methods [3] that make it possible to estimate the sender dynamics and decoding of the message signal. The second generation is the parameter and non-autonomous modulation techniques. Non-autonomous techniques were developed to overcome the chaotic parameter modulation break, which includes the return map, and adaptive observer [4]. Non-autonomous modulation is considered to be more secure than parameter modulation. The main goal of this paper is proposing a voice encryption system that provides users with a high degree of confidence and key sensitivity, and preserving a good quality of the reconstructed speech signal by chaotic flows. In Section 2, we discuss chaos-based cryptography systems. In Section 3, we present the proposed encryption ap-

* Corresponding author.
E-mail addresses: 8273@eng.asu.edu.eg (M.F.A. Elzaher), myousef73@hotmail.com (M. Shalaby), dr_yasser_omar@yahoo.com (Y. Kamal), salwa_elramly@eng.asu.edu.eg (S.E. Ramly).

http://dx.doi.org/10.1016/j.jisa.2017.03.002
2214-2126/© 2017 Elsevier Ltd. All rights reserved.

Please cite this article as: M.F.A. Elzaher et al., Securing digital voice communication using non-autonomous modulated chaotic signal, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.03.002

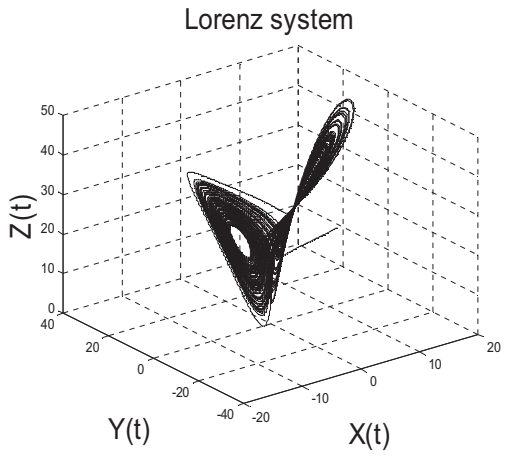

Fig. 1. The 3D figure of Lorenz chaotic flow.

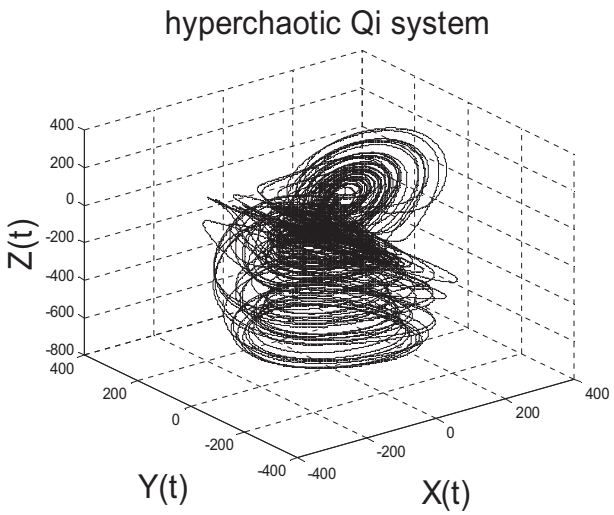

Fig. 2. The 3D figure of hyperchaotic Qi system.

proach. In Section 4, we show the results of applying our proposed approaches. Finally, we conclude our work in Section 5.

2. Chaotic system

Chaos-based cryptography plays an important role in modern cryptography area. Chaos theory has been developed by physicists and mathematicians. Chaos theory has eligible features such as determinism, nonlinearity, irregularity, and sensitivity to initial conditions. Therefore, and based on chaos theory features, security research community adopts chaos theory in modern cryptography. A function that possesses kind of chaotic behavior is defined as a chaotic flow or map. In the following subsections, we discuss two types of chaotic flows (using which we implement our proposed system), namely, Lorenz chaotic flow and hyperchaotic Qi chaotic flow.

2.1. Lorenz system

Lorenz chaotic flow can be described as three dimensions as shown in Eqs. (1)–(3).

$$\dot{X}(t) = \sigma(Y(t) - X(t)) \tag{1}$$

$$\dot{Y}(t) = rX(t) - X(t)Z(t) - Y(t) \tag{2}$$

$$\dot{Z}(t) = X(t)Y(t) - pY(t) \tag{3}$$

where $\dot{X}(t)$, $\dot{Y}(t)$, $\dot{Z}(t)$ are the Lorenz chaotic variables, $X(0)$, $Y(0)$, $Z(0)$ are initial conditions, and σ ,r and p are positive constants with $r > 24.74$. Fig. 1 shows a 3D figure of Lorenz chaotic flow.

2.2. Hyperchaotic Qi system

The Qi hyperchaotic flow is described by the 4-D dynamics Eqs. (4)–(7):

$$\dot{x}(t) = a(y(t) - x(t)) + y(t)z(t) \tag{4}$$

$$\dot{y}(t) = b(x(t) + y(t)) - x(t)z(t) \tag{5}$$

$$\dot{z}(t) = -cz(t) - ew(t) + x(t)y(t) \tag{6}$$

$$\dot{w}(t) = -dw(t) - rz(t) + x(t)y(t) \tag{7}$$

where $\dot{X}(t)$, $\dot{Y}(t)$, $\dot{Z}(t)$ *and* $\dot{w}(t)$ are the hyperchaotic Qi variables, $x(0)$, $y(0)$, $z(0)$, $w(0)$ are initial conditions and a, b, c, d, e, r are positive constant parameters. Fig. 2 shows the 3D figure of hyperchaotic Qi system.

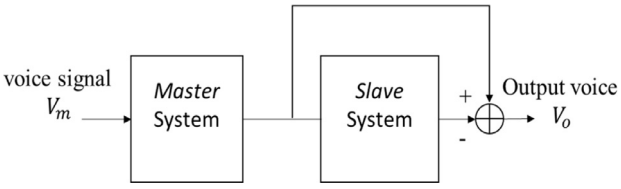

Fig. 3. Cryptosystem Transmitter and Receiver.

3. The proposed cryptosystem

The proposed cryptosystem is shown in Fig. 3. The samples of voice signal V_m are injected into the chaotic generator (master system) which also acts as driving signal for synchronization purpose as will be explained later. The voice signal is precisely recovered at the receiver side (slave system) by the subtraction of the receiver's regenerated drive signal from the received signal [4]. We implement our proposed system using two different chaotic flows, Lorenz system and hyperchaotic Qi system.

3.1. The proposed system using Lorenz chaotic flow

Here, we implement the master subsystem using Eqs. (8)–(10) related to Lorenz Eqs. (1)–(3). We note that V_m is the input voice sample, it is clear that V_m is now a parameter of function F.

$$\dot{X}_m = F((X_M + V_m), Y_M, Z_M) \tag{8}$$

$$\dot{Y}_m = G(X_M, Y_M, Z_M) \tag{9}$$

$$\dot{Z}_m = W(X_M, Y_M, Z_M) \tag{10}$$

The slave subsystem uses Lorenz Eqs. (11)–(14) to decrypt the encrypted signal.

$$\dot{X}_s = F(X_s, Y_s, Z_s) \tag{11}$$

$$\dot{Y}_s = G(X_M, Y_s, Z_s) \tag{12}$$

$$\dot{Z}_s = W(X_M, Y_s, Z_s) \tag{13}$$

$$V_O = X_M - \dot{X}_s \tag{14}$$

Please cite this article as: M.F.A. Elzaher et al., Securing digital voice communication using non-autonomous modulated chaotic signal, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.03.002

Download English Version:

https://daneshyari.com/en/article/4955716

Download Persian Version:

https://daneshyari.com/article/4955716

Daneshyari.com