A Novel Chaotic State Modulated Secure Communication System

Haamid Manzoor Gazi, Omar Farooq and Sekharjit Datta

Abstract: In this paper a new, efficient algorithm for secure digital communications in error free networks is presented. The proposed scheme uses pseudo chaotic random number generator (PCRNG) for secure communication. A quantized version of the PCRNG is used and the number of bits used for quantization decides the bandwidth expansion factor of resulting spread sequence. The proposed scheme utilises deterministic chaotic encryption via the logistic map and requires 3 keys. The initial seed, the chaotic equation and the value of constant $\alpha$. This scheme has been successfully tested for the encryption of images and audio signals.

Index Terms; Spread spectrum, Chaos, Security, Encryption.

I. INTRODUCTION

The increasing development of broadband networks and services, alongside the recent demand for privacy and paid services, has led to the need for systems and algorithms to encrypt information. Among the most important applications include the encryption of video messages for pay-TV services, voice over IP (Internet Protocol), and data messages transmitted over telematic networks (electronic signatures, electronic banking and commerce, etc.). The ability to be nomadic is of increasing importance to meet the demands of business and domestic users. Mobile computing over a wireless link is inherently insecure and requires encryption in order to render it unintelligible to an eavesdropper. The IEEE802.11 standards include WEP as a security model but it has been demonstrated to be easily crackable. Although Bluetooth was developed with security in mind its level of protection is insufficient and needs to be more seriously addressed. In addition, wireless mobile computing is restricted by resource constraints such as limited wireless bandwidth[5]. This means that cryptographic systems must be efficient. Public Key cryptosystems are too calculation intensive and hence incur a cost which is the extra time needed to encrypt and decrypt the message. A parallel stream cipher has been suggested in order to bypass these difficulties. Most businesses don’t need absolute encryption schemes. What they need is an encryption scheme that provides a sufficient level of protection with a low computational cost. Many cryptographic schemes and protocols have been proposed, most of these require a source of random or pseudo random numbers. The quality of this source is crucial for the security of the scheme or protocol in question. In recent years chaotic cryptography has attracted much attention, both digital and analog chaotic crypto systems have been proposed and analyzed. The principal feature of chaos is that simple deterministic systems arising in many areas can generate trajectories, which appear to be random. The essential property of these systems is the extreme sensitivity of construction of cryptographic algorithms. The advantage of using methods based on chaos theory lies in the high level of security chaotic systems offer as compared with traditional encryption techniques. At the same time they are very competitive due to the fact that they are inexpensive to implement [3]. The application scenario of chaotic encryption mainly considered in literature is a traditional analog or digital communication system in which the transmitter and receiver must be synchronized in order to have a correct decoding phase. In particular in this paper, we describe the potential of a new chaotic cipher applied to a secure communications.

Various techniques have been proposed in the area of chaotic encryption, however, all of these schemes used the chaotic pseudo random number in place of the conventional pseudo random number as a key. In this work a new scheme is proposed where the output of the chaotic system is itself quantized and transmitted depending upon the input bit.

II. CHAOTIC MODELS AND ENCRYPTION

A chaotic system is formed by some basic function $f$, which is iterated on some set $X$. In particular, the mapping $f: X \rightarrow X$ is said to be chaotic on $X$ if:

• $f$ has sensitive dependence on initial conditions;
• $f$ is topologically transitive;

Intuitively, a map possesses sensitive dependence on initial conditions if there exist points arbitrarily close to $x$ where $x$ is an element of $X$ which eventually separate from $x$ by at least $\delta > 0$ under iteration of $f$. whereas a topologically number transitive map has points which eventually move under iteration from one arbitrarily small neighborhood to any other. Thus a chaotic map presents three important features: unpredictability, indecomposability, and an element of...
regularity. A chaotic system is unpredictable because of the sensitive dependence on initial conditions. It cannot be broken down or decomposed into two subsystems, which do not interact under \( f \) because of topological transitivity. In the mid of this random behavior, we have an element of regularity, namely the periodic points which are dense. Any chaotic system should be mixing, i.e. the phase space \( X \) should be randomly mixed by repeated action of \( f \). Further, most chaotic systems depend on some control parameters and exhibit sensitivity with respect to those parameters[4].

Another important property of chaotic system is their bifurcation, i.e.divergence of the trajectories for different adjacent starting points. A common measure of the bifurcation is lyapunov exponent, denoted by \( \lambda \) and is defined for continuous state discrete system by equation 1as:

\[
\lambda(x_0) = \lim_{n\to\infty} \lim_{\varepsilon\to 0} \frac{1}{n} \log\left| f^n(x_0 + \varepsilon) - f^n(x_0) \right| (1)
\]

For a system to be chaotic this factor should be positive [1].

The advantage of chaotic encryption is that the sequence is very sensitive to changes in the original seed. A change in value of the original seed of a few parts per billion will cause a deviation away from the original sequence. It is this sensitivity that makes chaotic systems ideal for encryption.

There are a number of chaotic systems used in cryptography, with the most commonly used chaotic system being the logistic map. The logistic map is defined on the unit interval \( \{0,1\} \) and is given by

\[
x_{n+1} = \alpha x_n (1 - x_n) \tag{2}
\]

where \( x_n \) is the \( n^{th} \) value in the sequence, \( x_{n+1} \) is the next value in the sequence and \( \alpha \) is a scaling factor. It stretches \( x_n \) by \( \alpha \) and then folds it back by \((1-x_n)\). This gives rise to chaos given a suitable choice of the logistic map has been suggested for use as a symmetric encryption method [4] with the initial seed \( x_0 \) being secret. As far as the encryption is concerned the three values, which we can say, act as key are

- The initial seed
- The chaotic equation
- The value of \( \alpha \)

Let the chaotic equation be

\[
y(i + 1) = \alpha y(i)(1 - y^2(i)) \tag{3}
\]

Initial value of the \( y \) is set to be equal to 0.0271 \( y(i) \) versus \( \alpha \) is plotted which is shown in Fig 1. The value of \( \alpha \) is that value for which the system behaves chaotically and can be obtained from Fig 1.

As seen from the Fig 1. the value of \( \alpha \) for this equation is equal to 3.

III. CHAOTIC ENCRYPTION

1) Transmitter side:

Two separate pseudo chaotic random number generator (PCNRG) were used for the encryption of 0 or 1. The equation and the initial seed of both the chaotic encrypters is different from each other. Equation 2. is used for PCNRG ‘0’ and Equation 3 for PCNRG ‘1’. First of all the value of \( \alpha \) is calculated for the two equations for which the system behaves chaotically. While designing the PCNRG we can choose any number of quantization levels. But the number of quantization levels used is also responsible for the bandwidth expansion.

The basic algorithm for this transmitter is that first of all next state of both of the PCNRG is checked, if the next state of both of them are same then PCNRG’s make transition into their next state until the states of the two PCNRG are different. The incoming bit is checked whether it is zero or one. Depending on the value of the incoming bit the state of that PCNRG will be transmitted. Suppose the incoming bit is one then the quantized output of PCNRG ‘1’ will be transmitted, and the process will continue until all the bits have been coded. The block diagram representation of the transmitter is given by Fig.2.
2) Receiver side:

Fig.3 gives Block diagram of the Receiver. On the receiver side same PCNRG as that on the transmitter side are used. The value of the initial seed and the equation are to be taken same as that on the transmitter side. Next state of both the PCNRG is checked whether they are equal or not if they are equal then the states of both the PCNRG are allowed to make the transition and again we check. If the the states are not equal then we compare the received quantized value with the quantized output of PCNRG ‘1’ and PCNRG ‘0’. Suppose if the output of PCNRG ‘1’ is equal to received value then the received bit is assigned the value 1. In the similar manner all the received symbols are checked and assigned value one or zero.

IV. RESULT AND DISCUSSION

We have obtained the results for both the binary images as well as gray level images. In case of the binary images the process is simple, the pixel information is given in binary form, we use this binary information as the input for the chaotic encoder we have used two level chaotic encoder so that there is no bandwidth expansion. At the receiver end we receive an encoded version of the original image which is entirely different from the original image it is more or less like a noise, the encoded bits are processed using same chaotic generators at the receiver with same initial conditions as that in the transmitter we see that the receiver is able to decrypt the image without any error and the decrypted image is same as original image. The results are shown in Fig.4.

![Fig.4: Encryption and decryption of a binary image using the proposed algorithm](image1)

![Fig.5: Encryption and decryption of a gray level image using the proposed algorithm](image2)

In case of gray level images the data is in the form of 255 gray levels so we first convert the data into binary form and then encrypt it using chaotic model, at the receiver end the image is perfectly decrypted. The data is encoded successfully and at the transmitter side the data is decoded without any error. The resulting images after encryption and decryption are shown in Fig.5. The gray level image requires more time for processing because we have to first convert the pixel information into binary form so a single pixel information is represented in 8 bits hence total number of bits required as compared to binary image also increases, therefore for processing same size gray level image we require more time than in binary image.

For the gray level images we have also plotted the histogram for the original as well as encrypted image shown in Fig.6 and Fig.7. As seen from the Fig.6 it is evident that in the original image the levels are not equally distributed, level 255 occurs above 900 times. But for the encrypted image as shown in Fig.7 the levels are evenly smoothed this shows that the chaotic encrypter is functioning in a chaotic manner.

![Fig.6: Plot of histogram for the original image shown in Fig. 5](image3)

![Fig.7: Plot of histogram for the encrypted image shown in Fig. 5](image4)

V. CONCLUSION

We have given a novel concept of encryption where the encrypted symbols vary chaotically and it is impossible to decode the data without the knowledge of the initial seed, the chaotic equation and the value of α. Another reason for the security of the encryption is because of the fact that it is very difficult to determine the equation and the initial seed from the encrypted data.

One of the main drawbacks of this system is that it requires
large amount of time for processing, inorder to overcome that problem we should have fast processing computers. However increasing the number of levels in PCNRG can reduce the number of computations required, but this will lead to bandwidth expansion. Thus there is a tradeoff between the number of computations required and the bandwidth expansion. Also this system works efficiently in error free transmission medium.

References


