Design of a synchronized Chaotic Secure Communication in multipath fading channel

A. A. Elkouny

Faculty of Information Systems & Computer Sciences October 6 University, Cairo, Egypt
aelkouny@gmail.com

Abstract: This paper focuses on the synchronization of two chaotic systems, when they are connected, using a multipath fading channel. The proposed algorithm is then applied to secure communication and realizing it using VHDL. The results reveal that signals to chaos ratio of -248 dB and synchronization are achieved. Performance analysis have been conducted to investigate the robustness of the encryption system against different types of attacks.

[A. A. Elkouny. **Design of a synchronized Chaotic Secure Communication in multipath fading channel.** *J Am Sci* 2014;10(11):114-121]. (ISSN: 1545-1003). http://www.jofamericanscience.org. 16

Keywords: Chaotic; encryption; fading channel; synchronization

1. Introduction

The rapid development of the multimedia technology, digital image is becoming an important carrier of information communion for people. With the advance of information security requirement, the encryption technology is applied widely to multimedia communications. In typical communication systems, based on chaos synchronization schemes, the information to be transmitted is carried from the transmitter to the receiver by a chaotic signal. The decoding of the information signal in the receiver can be carried out by means of either coherent or non-coherent demodulation schemes. Different approaches for designing cryptosystems have recently been introduced [1-4]. Nevertheless, chaotic synchronization is in general sensitive to additive noise and channel delay. Knowing that low dimension chaos has a distinct pattern that allows a third party to extract the information easily by constructing a return map [5-6].

This paper consider the problem of combating different channel distortions like time varying fading and multi-path with very high security then it present a chaotic communication system in which security, synchronization and reliability are simultaneously achieved.

2. Rössler encryption algorithm

In chaos-cryptography it is recommended to use complex signal, that to make the encryption algorithm more robust to the statistical attacks. Therefore using higher dimensional dynamical systems is preferable than the lower systems. The proposed cipher is built depending on 3D discrete Rössler map scheme; this chaotic attractor is based on the 3D continuous Rössler flow, which has a very complex dynamical behavior. The main reasons of having high limitation on the signal to chaos ratios is that the receivers use differentiators to decrypt the signal [7]. Differentiators will always produces large spikes and high error if the signal contains discontinuities, which is always the case for images and text signals. To overcome the above problem the derivative of a state variable is used as the transmitted signal rather than the state variable itself. The transmitter equations are given by:

$$x = -\int (dy + dz)\, dt$$
$$y = \int (dx + Ady + Sv_{in})\, dt \qquad (1)$$
$$z = \int (B + z(x - C))\, dt$$

Where v_{in} is the information signal, S is a scaling factor to reduce the value of the information signal with respect to the chaotic signal, A =0.398, B =2 and C =4. The transmitted signal is dy/dt instead of any of the state variables (x, y, z). The receiver equations are given by

$$x' = -\int (dy' + dz')\, dt$$
$$v_{out} = \frac{1}{S}\left(\frac{dy}{dt} - x' - Ay'\right) \qquad (2)$$
$$z' = \int B + z'(x' - C)\, dt$$

Where v_{out} is the recovered information signal and dy/dt is the received signal.

3. Synchronization approach

Our aim in this section is how to achieve synchronization between the drive and the response system in the presence of a variable time channel delay and where to insert the encryption keys in the Rössler chaos generator. These generator keys are chosen in a way that will not affect the chaotic generator and simultaneously attains the optimum needed security. An ordinary differential equation (ODE) solver is a computational method for producing an approximate solution to an initial value problem [8]. Starting with initial value x_0, the method calculates approximate values of the solution $x(t)$. The simplest ODE solver is the Euler method. The Euler method produces approximations by an iterative formula of the initial value problem. For a step size $\Delta t > 0$ Euler's method replaces x by

$$\frac{x(t)-x(t-\Delta t)}{\Delta t} \qquad (3)$$

Using the same principle, the alteration to discrete time for the Rössler chaotic generator can be achieved by replacing the integration blocks with the discrete integrator model

Where for $\Delta t > 0$

$$x_1(t) = x(t)\Delta t + x_1(t-\Delta t)$$

$$x(t) = \frac{x_1(t)-x_1(t-\Delta t)}{\Delta t} = \frac{\Delta x_1}{\Delta t} \qquad (4)$$

However, this substitution will generate algebraic loops. Consequently, a modification of the discrete integrator model is required to implement this model in digital hardware. Inserting another time delay block, as shown in Figure 1, solves the algebraic loop problem.

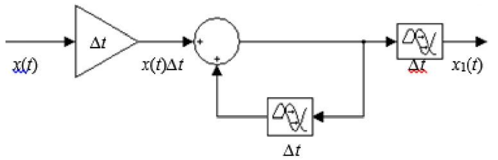
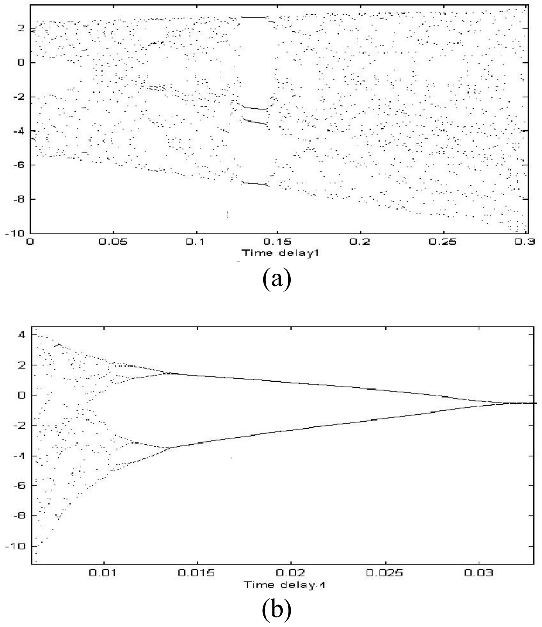


Figure 1. Modified discrete integrator.

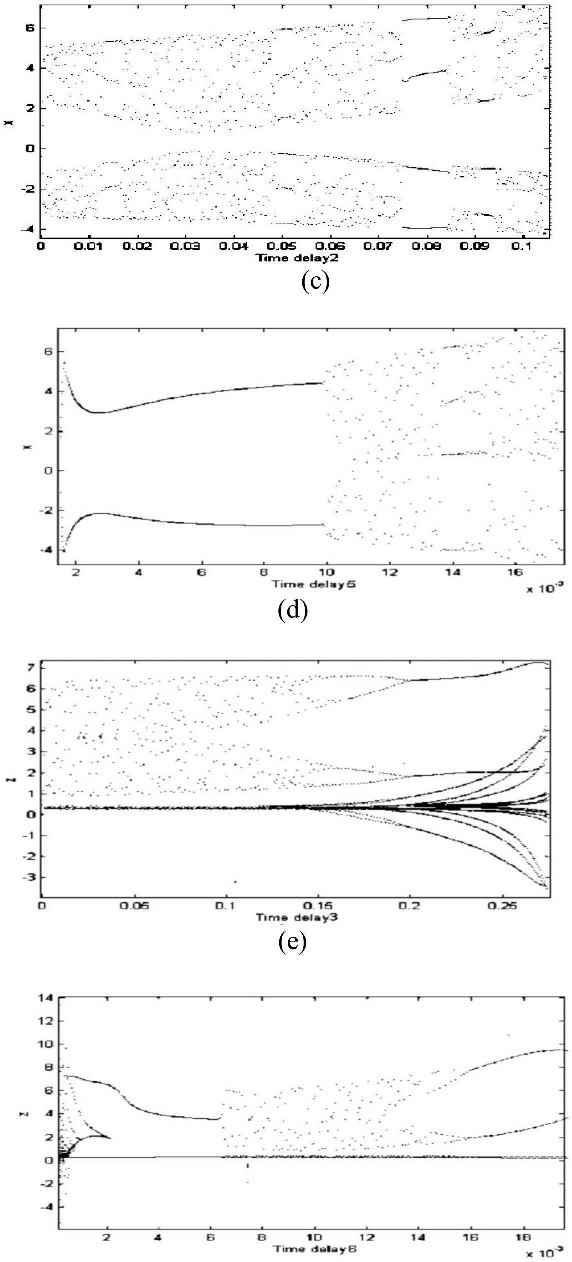
Where for $\Delta t > 0$

The bifurcation diagrams of the different time delays values that preserve the chaotic behavior versus the variables x, y and z of the state equations are shown in Figure 2.



(a)

(b)



(c)

(d)

(e)

(f)

Figure 2 Bifurcation diagrams of (a) state variable *y* versus time delay 1, (b) state variable *y* versus time delay 4, (c) state variable *x* versus time delay 2, (d) state variable *x* versus time delay 5, (e) state variable *z* versus time delay 3 and (f) state variable *z* versus time delay 6.

The equations for the Rössler transmitter will be as follows;

$$x_{n+1} = \Delta t\big(S_1(-y_n - z_n)\big) + x_n$$
$$y_{n+1} = \Delta t\big(S_2(x_n + Ay_n + Sv_{in})\big) + y_n$$
$$z_{n+1} = \Delta t\big(S_3\big(B + z_n(x_n - C)\big)\big) + z_n \qquad (5)$$

In Equation 5 the information signal v_{in} is added to the second equation. The information is also multiplied by a constant S to reduce its value with respect to the chaotic signal. The scaling factors S_1, S_2 and S_3 are used to control the frequency band of the output signals. The equations for the Rössler receiver are given by

$$x_{n+1} = \Delta t\left(S_1(-y_n - z_n)\right) + x_n$$

$$v_{out} = \frac{1}{S}\left(\frac{1}{S_2}\frac{y_{n+1} - y_n}{\Delta t} - x_n - Ay_n\right)$$

$$z_{n+1} = \Delta t\left(S_3\left(B + z_n(x_n - C)\right)\right) + z_n \qquad (6)$$

Replacing the integrators of the Rössler chaotic model with the above-mentioned blocks the following communication system is shown in Figure 3.

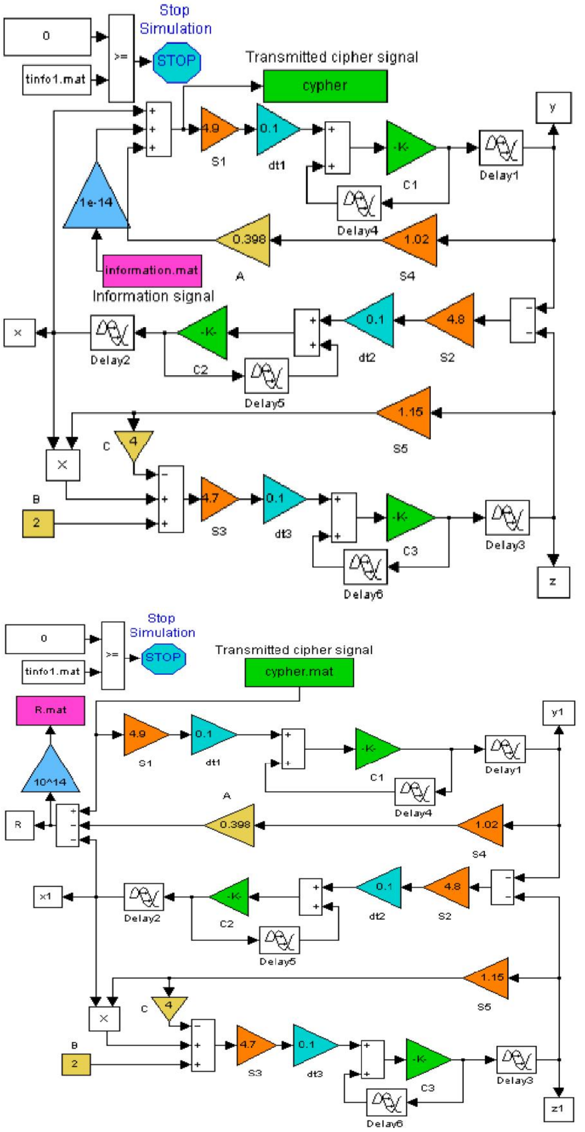


Figure 3. Rössler transmitter & receiver subsystems.

Applying the above communication system as a security application. The encryption and decryption algorithms are detailed as follows.

Encryption algorithm:

1. The information file is read and the total number of characters inside the file is calculated.
2. The encryption keys are chosen by the user and stored.
3. The total number of the characters and the encryption keys file are stored into one file called the key file.
4. The key file is loaded then converted from a one-dimensional array into individual values to be manipulated by the encryption algorithm.
5. The information is loaded to the algorithm and is encrypted using the encryption keys.
6. The clock is an up-counter used to compare its instantaneous value with the total number of characters. When these are the same and all the plaintext characters are encrypted, the encryption algorithm is stopped.
7. The resultant cipher is stored into a file or sent to through the LAN or WLAN.

Decryption algorithm:

1. The key file is loaded then converted from a one-dimensional array into individual values to be manipulated by the decryption algorithm.
2. The decryption algorithm is a direct representation of the Equation 6.
3. The received cipher is loaded to the algorithm and is decrypted using the decryption keys.
4. The clock is an up-counter whose instantaneous value is compared to the total number of cipher characters. When these are the same and all the cipher are decrypted, the decryption algorithm is stopped. Finally, the recovered information is stored into a file.

The main advantage of this model is that the transmitter will not transmit any signal unless there is an initiator, which is represented by the information signal. Consequently, the receiver is awaiting an encrypted signal to initiate it.

4. CDMA communication system

The most important properties of Spread spectrum communication are its multiple access capability, multipath interference rejection and narrow band interference rejection [9]. In CDMA the modulated information-bearing signal (the data signal) is directly modulated by a digital signal. The receiver correlates the received signal with a synchronously generated replica of the code signal to recover the original information-bearing signal. This implies that the receiver must know the code signal used to modulate the data. The data signal can be either an analogue signal or a digital one. In our case it will be a digital signal. The code signal, which is a noise-like sequence, consists of a number of code bits that can be either '+1' or '-1'. The most important demand for the development of suitable codes is to have a low cross-correlation between the codes assigned for different users and to have local autocorrelation in order to well synchronize and lock the locally generated code signal to the received signal. To obtain the desired spreading of the signal the bit rate of the code signal must be much higher than that of the information signal. Several families of binary PNcodes exist as m-sequences, Gold codes and Kasami sequences [9-10]. In the transmitter part of our developed communication system, the encrypted signal is binary coded then transformed into bipolar (+1, -1). After that, the data signal is multiplied by the Kasami sequences as shown in Figure 4.

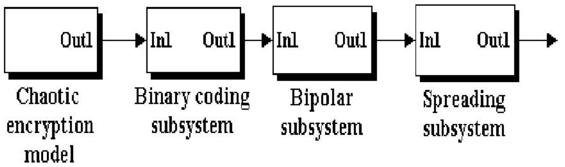


Figure 4. Transmitter part.

For the receiver part, we have developed two models depending on the value of the Doppler frequency. If the Doppler frequency is less than or equal to 1 Hz then we can use the simpler receiver shown in Figure 5.

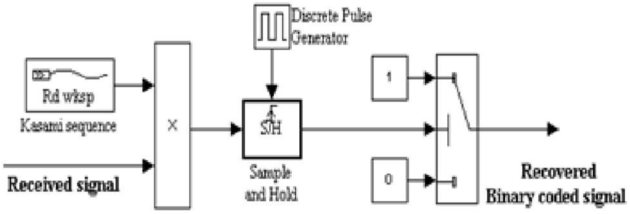


Figure 5. Simpler version of the receiver.

While for higher Doppler frequency, we have constructed a more complicated one shown in Figure 6. Using multipath channel with Doppler frequency 1 Hz and two delay vectors equal to 0.01, 0.02 and 0.03 the experiment results are shown in Figure 7.

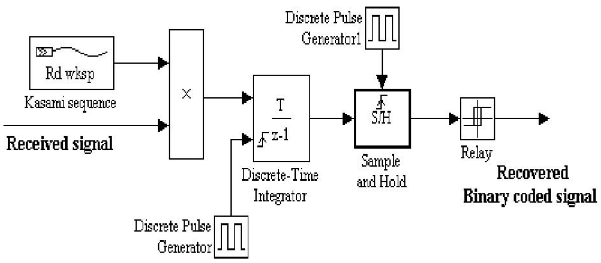
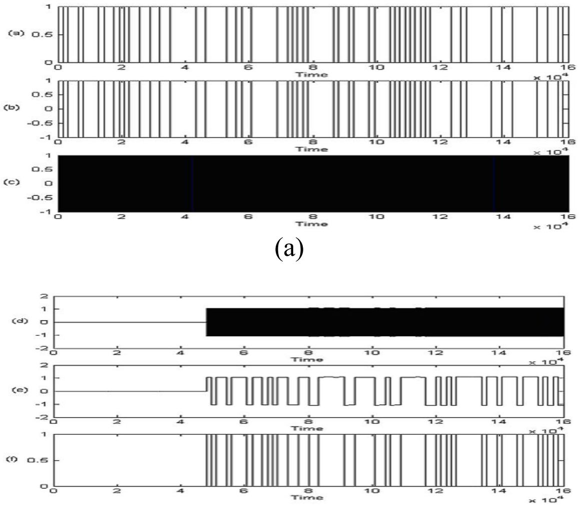


Figure 6. Complex version of the receiver.



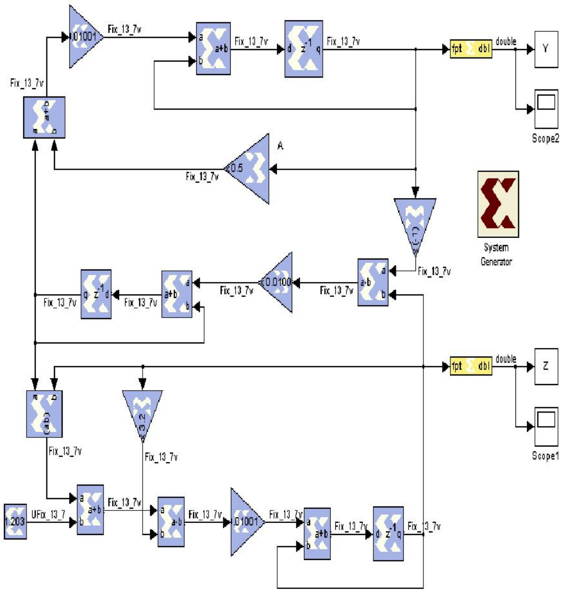
(a)

(b)

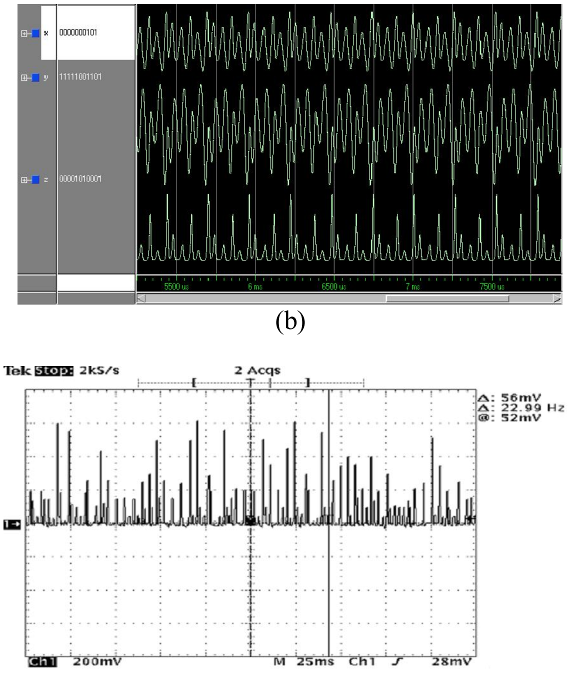
Figure 7. (a) The ciphered binary signal, bipolar signal and the spreading signal. (b) Received signal, after sample and hold and finally and after the control switch (recovered ciphered binary signal).

5. Hardware Implementation Using VHDL

High gate count and switching speed of modern FPGA is enabling high data-rate DSP processing to be performed. Static RAM based FPGA also enable solutions to be reprogrammable. The soft solutions offer flexibility (changing encryption key), which is an important attribute of a modem cipher system. FPGA is adopted here due to the parallel architecture and flexibility to implement. The framework for the Rössler chaotic generator, its VHDL results using ModelSim and its real time output are shown in Figure 8.



(a)

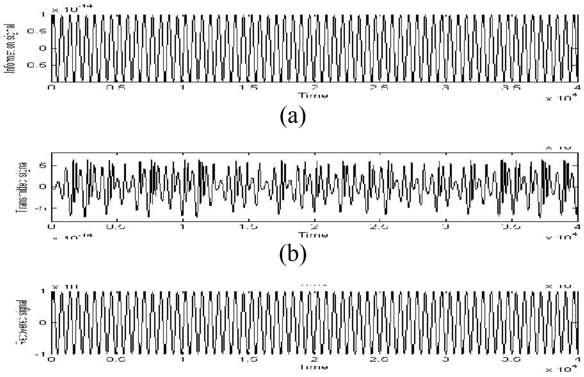


(b)

(c)

Figure 8 (a) Framework,VHDL (b) ModelSim output and (c) real time output of the FPGA Rössler chaotic generator.

Two very important features are observed in this system shown in Figures 7 and 8. The first is its ability to transmit very low signal to chaos ratio and to recover the information without any loss. Signal to chaos ratios between -220 dB and -252dB have been achieved depending on the complexity of the information signal. The second is that any error in each of the cipher keys of order 10-16 of its original value will not recover the information signal. Figure 9 shows how a sine wave is accurately recovered at a signal to chaos ratio -220 dB, Figure 10 show a JPEG image transmitted then recovered at -242 dB signal to chaos ratio.

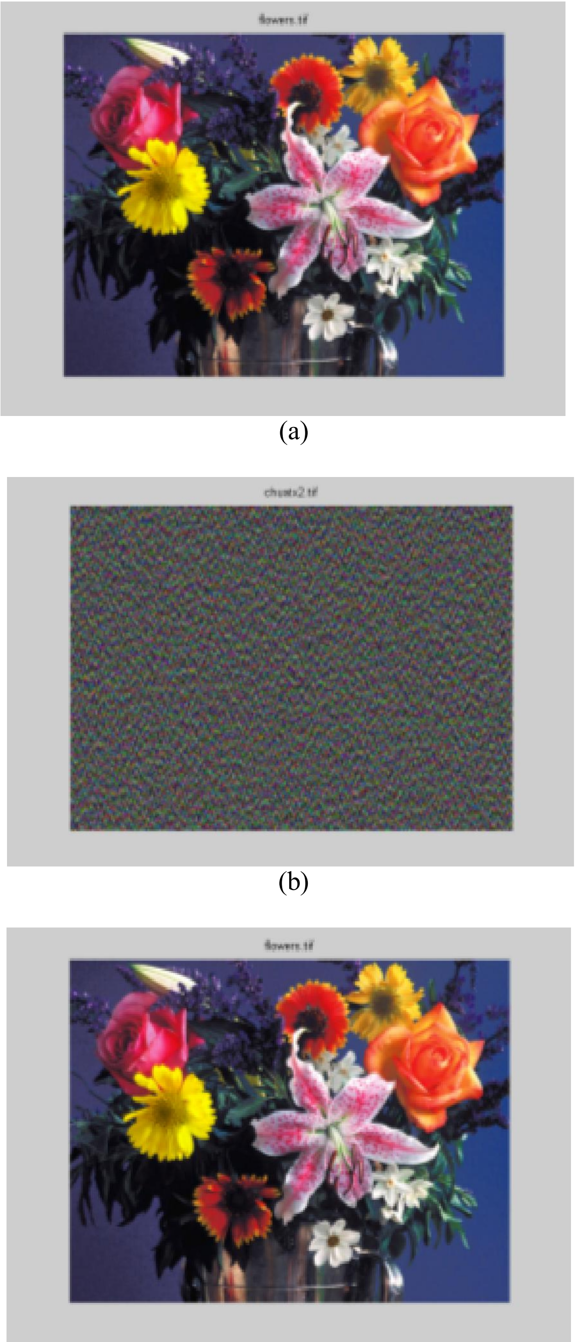


(a)

(b)

(c)

Figure 9. (a) Original, (b) Encrypted and (c) Recovered signal.



(a)

(b)

(c)

Figure 10. The original JPEG image (a), the encrypted (b) and the recovered image (c).

6. Security and performance analysis

Security analysis is the major challenge in any cryptosystem. The security analysis of the proposed algorithm is discussed on the parameters such as brute-force attack, statistical analysis, differential attack, key sensitivity attack [11-14].

a) Statistical analysis

Statistical analysis on cipher image is of crucial importance for any encryption algorithm. Actually, an ideal cipher should frustrate the powerful attacks based on statistical analysis. Statistical analysis has been performed on the correlations of the ciphered signal. Figures 11 show the low correlation of the modulated transmitted signals, like the correlation of the attractor. This gives a proof about the randomness of the generated signals, and the difficulty from exploiting it.

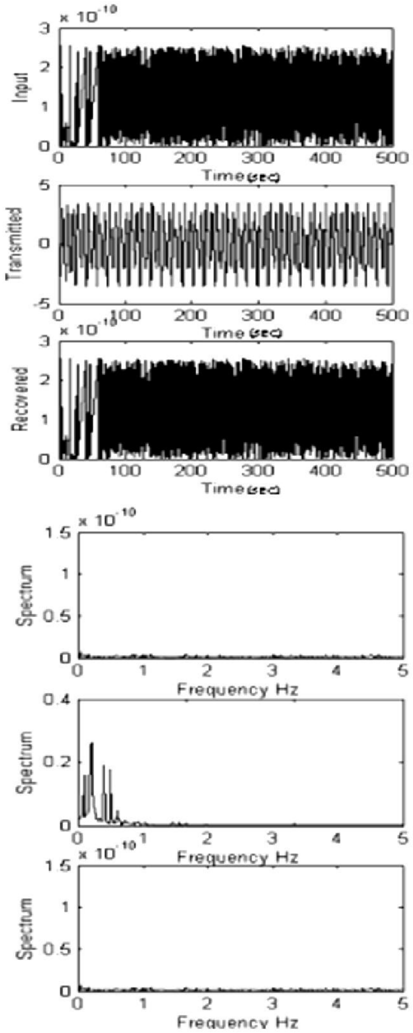
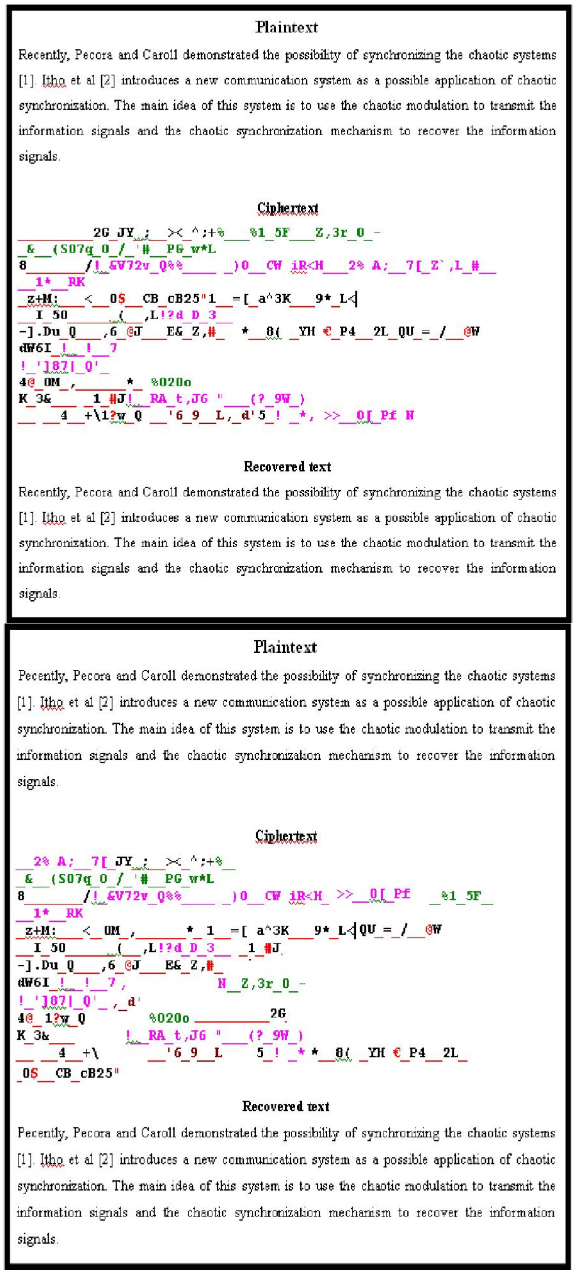


Figure 11. Information signal, transmitted signal and recovered signals in the time and the frequency domains.

b) Differential analysis

Differential attack is another important attack that can be used to measure the security of the encryption algorithm. In this attack, the cryptanalyst is assumed to have the capability of modifying one character/single pixel of the plain message and observing the resultant encrypted signal. If such a change results in a significant change in the encrypted image, then the attack is considered to be inefficient and impractical. Changing only the first sample of the text message to be Letter P instead of R. The difference between the encrypted signal shown in Figure 12 and the original cipher text is 100%.



Plaintext

Recently, Pecora and Caroll demonstrated the possibility of synchronizing the chaotic systems [1]. Itho et al [2] introduces a new communication system as a possible application of chaotic synchronization. The main idea of this system is to use the chaotic modulation to transmit the information signals and the chaotic synchronization mechanism to recover the information signals.

Ciphertext

```
__________2G_JY_;__><_^;+%___%1_5F___Z,3r_0_-
_&__(S07q_0_/_'#__PG_w*L
8________/!_&V72v_Q%%_____ _)0__CW iR<H___2% A;__7[_Z`,L_#__
__1*__RK
_z+M:____<__0$__CB_cB25"1__=[_a^3K___9*_L<
__I_50_______(___,L!?d_D_3__
-].Du_Q___,6_@J___E&_Z,#_  *__8(_YH €_P4__2L_QU_=_/__@W
dW6I_!__!__7
!_']87|_Q'_
4@_OM_,________*_ %020o
K_3&____ _1_#J!__RA_t,J6 "___(?_9W_)
__ __4__+\1?w_Q __'6_9__L,_d'5_!_*, >>__0[_Pf N
```

Recovered text

Recently, Pecora and Caroll demonstrated the possibility of synchronizing the chaotic systems [1]. Itho et al [2] introduces a new communication system as a possible application of chaotic synchronization. The main idea of this system is to use the chaotic modulation to transmit the information signals and the chaotic synchronization mechanism to recover the information signals.

Plaintext

Pecently, Pecora and Caroll demonstrated the possibility of synchronizing the chaotic systems [1]. Itho et al [2] introduces a new communication system as a possible application of chaotic synchronization. The main idea of this system is to use the chaotic modulation to transmit the information signals and the chaotic synchronization mechanism to recover the information signals.

Ciphertext

```
__2% A;__7[_JY_;__><_^;+%__
_&__(S07q_0_/_'#__PG_w*L
8________/!_&V72v_Q%%_____ _)0__CW iR<H_ >>__0[_Pf   __%1_5F__
__1*__RK
_z+M:____<__OM_,_________*_1__=[ a^3K___9*_L<|QU_=_/__@W
__I_50_______(___,L!?d_D_3___ _1_#J
-].Du_Q___,6_@J___E&_Z,#_
dW6I_!__!__7,           N__Z,3r_0_-
!_']87|_Q'_,_d'
4@_1?w_Q        %020o ___________2G
K_3&____         !__RA_t,J6 "___(?_9W_)
__ __4__+\        __'6_9__L    5_!_* *__8(_YH €_P4__2L_
_0$__CB_cB25"
```

Recovered text

Pecently, Pecora and Caroll demonstrated the possibility of synchronizing the chaotic systems [1]. Itho et al [2] introduces a new communication system as a possible application of chaotic synchronization. The main idea of this system is to use the chaotic modulation to transmit the information signals and the chaotic synchronization mechanism to recover the information signals.

Figure 12. Encrypting and decrypting a text file.

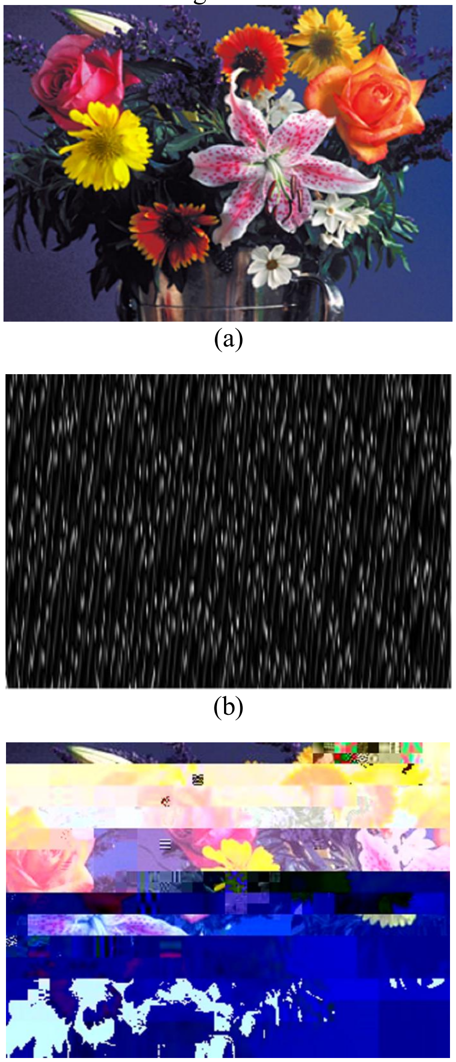
c) Key space analysis and brute-force attack

The key space of an encryption algorithm is the set of different keys that can be used for the encryption purpose. From the cryptography point of view, the size of the key space should not be smaller than 2^{100} to provide high level of security [15]. The key length for the proposed cipher includes the values of six-transport delay, three parameters *A, B, C*, three $C_{1,\,2,\,3}$

scaling parameters one for each state equation, three scaling factors and three gain factors. From the experiments the key length is 342 digits according to that the key space is 10^{342}, which gives a sufficient proof about the robustness against the brute-force attack.

d) Key sensitivity

Highly sensitive to the change in cipher parameters provides further resistance against cryptanalytic attacks. Thus, for example if the user set the value of the parameter A=0.99123456789123**4** the transmitted encrypted signal will not be recovered until unveil all 15 decimal fraction of the parameter A. To verify our claim assume that all the parameters of the transmitter and the receiver are synchronized except the parameter A=0.99123456789123**5** the last decimal fraction is changed from 4 to 5. Figure 13 show the results of recovered image.



(a)

(b)

(c)

Figure 13. The original JPEG image (a), the encrypted image (b) and the recovered image (c).

7. Conclusion

In this work, an approach has been developed to resolve the chaotic synchronization in the presence of a multipath fading channel and its application to secure communications. This proposal utilizes modified discrete integration to overcome the synchronization problem. The developed model can be used for text, images and voice signals with extremely high security. Results confirm the proposed scheme's effectiveness in synchronizing a Secure Communication in multipath fading channel.

Corresponding Author:
Dr. Abdellatif Elkouny
Faculty of Information Systems & Computer Sciences, October 6 University, Cairo, Egypt
E-mail: aelkouny@gmail.com

References

1. Ramesh Kumar Yadava, Dr. B. K.Singh, S. K. Sinha and K. K. Pandey, "A New Approach of Colour Image Encryption Based on Henon like Chaotic Map", Journal of Information Engineering and Applications, vol. 3, no. 6, pp. 14-20, 2013.
2. Alireza Jolfaei and Abdolrasoul Mirghadri,"An Image Encryption Approach using Chaos and Stream Cipher", Journal of Theoretical and Applied Information Technology, pp.117-125, 2010.
3. YAO Xiang-hui, YU Si-min. Digital video encryption based on Lorenz chaotic system. Image Processing and Multimedia Technology, 2011, pp. 41-43.
4. Jun Peng, Shangzhu Jin, Guorong Chen, Zhiming Yang, Xiaofeng Liao, An image encryption scheme based on chaotic map, IEEE Conference Proceedings: Fourth international conference on natural computation 10.1109/ICNC.2008.227.
5. Tao Yang, Lin-Bao Yang, Chun-Mei Yang, Breaking chaotic secure communication using a spectrogram, Phys. Rev. Lett. A, vol. 247, pp. 105-111, 1998.
6. Migkai Nan, Chak-nam Wong, Kim-fung Tsang, Xiangquan Shi, Secure digital communication on linearly synchronized chaotic maps, Phys. Rev. Lett. A, vol. 268, pp. 61-68, 2000.
7. Pecora L.M., T. L. Carroll, G Johnson, D. Mar, "Volume-preserving and volume-expanding synchronized chaotic systems", Phys. Rev. E , vol. 56, pp. 5091-5100, 1997.
8. Alligood K., T. D. Sauer, J. A. Yorke, Chaos an introduction to dynamical systems: Springer, 1997.

9. Ramjee Prasad, CDMA for Wireless Personal Communications, Artech House, 2002.
10. Viterbi J., CDMA: Principles of Spread Spectrum Communication.Addison-Wesley, 2010.
11. Yang T., L. Yang, C. Yang, "Cryptanalyzing Chaotic Secure Communications using return Maps", Physics Letters A, 245 495-510, 1998.
12. Li S., G. Alvarez, G. Chen, "Breaking a Chaos-based Secure Communication Scheme desiged by an improved modulation method", Chaos, Solitons and Fractals, Vol. 25 pp. 109-120, 2005.
13. Li S., G. Alvarez, G. Chen, "Return-Map Cryptanalysis Revisited", International Journal of Bifurcation and Chaos, vol. 16, no. 5, pp. 1157-1168, 2006.
14. Wu X., H. Hu, B. Zhang, Analyzing and improving a chaotic encryption method, Chaos, Solitons and Fractals 22 (2) (2004) 367–373.
15. Schneier B., "Applied Cryptography: Protocols, Algorithms, and Source Code in C", second ed., John Wiley & Sons, New York, 1996.

10/12/2014