Chaotic Algorithms for Data Encryption

Mohamed I. Sobhy and Alaa-eldin R. Shehata
The Electronic Engineering Laboratory
The University of Kent at Canterbury
Canterbury Kent CT2 7NT, UK
Phone +441227 823236 Fax +44 1227 456084 email: M.I.Sobhy@ukc.ac.uk

Abstract: A system of encryption based on chaotic algorithms is described. The system is used for encrypting text and image files for the purpose of creating secure data bases and for sending secure email messages. The system is also implemented on an FPGA for real-time applications. Levels of security several orders of magnitude better than published systems have been achieved.

1. INTRODUCTION

In this paper we present a computer based algorithm for encrypting text messages and images. The encrypted files are used as either secure data bases or for communication via email. Analogue chaotic encryption systems [1-4] suffer from poor synchronisation between transmitter and receiver due to the fact that the values of analogue components cannot be adjusted accurately for this purpose. In all reported systems to date one of the state variables is used as the carrier and this requires that the receiver includes differentiators in order to recover the signal. Differentiators give rise to high noise outputs. For these reasons, only signal to chaos ratios of –30 to -40 dB have been achieved. This is inadequate for a secure system.

Most communication at present is through computers and even real-time communication systems are mostly digital not analogue. A computer-based algorithm will be able to match the transmitter and receiver exactly and will be independent on the communication channel. Furthermore the algorithm could be written such that the receiver does not require any differentiators. This would improve the synchronisation between transmitter and receiver and achieve signal to chaos ratios in the order of –240 dB which previously were unheard of. Furthermore the system parameters could me made non-linear functions of the state variables to achieve extremely high security.

We shall describe an example of such a system that achieves degrees of synchronisation, security and reliability that cannot be achieved otherwise. The system is used for secure data bases and secure email.

The system has been configured on Field Programmable Gate Arrays (FPGA) which enables the communication to be run in real-time

2. COMPUTER-BASED CHAOTIC SYSTEMS

The algorithms developed are based on the Chua circuit, the Rössler system or the Lorenz system of equations. Combinations of these systems are also possible. We shall describe here the algorithm based on the Lorenz system. Other systems are treated in a similar way.

We write the state equations for the transmitter, which are the normal Lorenz equations modified to include the input signal which is the plaintext to be encrypted. The plaintext is not a simple addition to the chaotic signal as in the case of chaos masking systems. This adds to the security of the encryption as a simple subtraction process will not recover the encrypted message.

$$\begin{aligned} x_1 &= A_1 \int x_2 - x_3 \, dt \\ x_2 &= \int A_2 x_1 - x_2 - x_1 x_3 + A v_{in} \, dt \\ x_3 &= \int x_1 x_2 - A_3 x_3 \, dt. \end{aligned} \tag{1}$$

The plaintext is also multiplied by a constant *A* to reduce its value with respect to the chaotic signal. We shall present results later where $A = 10^{-12}$ which results in a signal to chaos ratios of about -240 dB. The transmitted signal is dx_2/dt instead of any of the state variables and this has the crucial advantage that differentiation is avoided in the receiver. The derivative dx_2/dt is of course readily available in the transmitter before integrating the second equation.

The receiver equations are given by:

$$\begin{aligned} x_1' &= A_1 \int x_2' - x_1' \, dt \\ v_{out} &= \frac{1}{A}\left(\frac{dx_2}{dt} - A_2 x_1' + x_2' + x_1' x_3' \right) \\ x_3' &= \int x_1' x_2' - A_3 x_3' \, dt. \end{aligned} \tag{2}$$

The above arrangement has the following advantages:

1. The plaintext is not simply added to the chaotic signal and thus cannot be retrieved by subtraction.
2. Differentiation is avoided anywhere in the system and thus eliminating the spikes that are always generated by the process of differentiation of abruptly changing signals. This allows very low signal to chaos ratios.

Next we identify the key for the encryption system. There are three parameters in the system (A_1,A_2 and A_3). These together with the initial conditions of the three integrators form the key of the system.

Eqs. (1) and (2) can be easily represented using SIMULINK©. The simulations are shown in Figs 1 and 2.

The steps in the algorithm are as follows:

1. Encryptor

- Load plaintext
- Call encryptor key file
- Run encryptor algorithm
- Send the ciphertext through the LAN or WLAN.

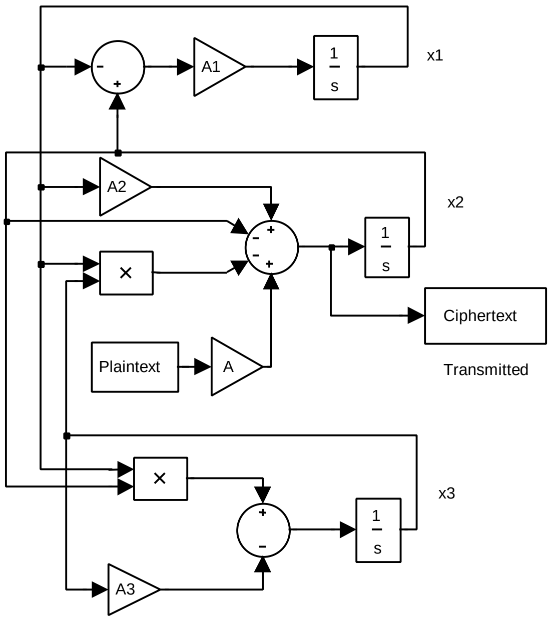


Fig 1 The Lorenz encryption system

2. Decryptor

- Load the received ciphertext
- Call decryptor key file
- Run decryptor algorithm
- Put the recovered data into a file

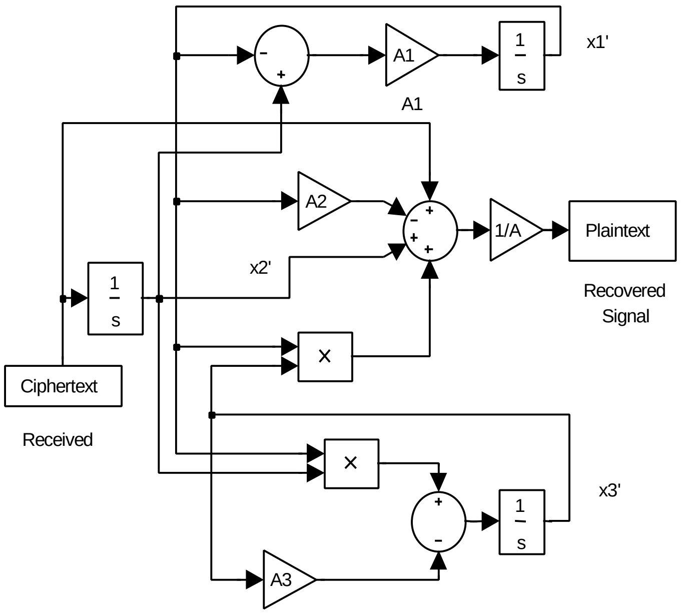


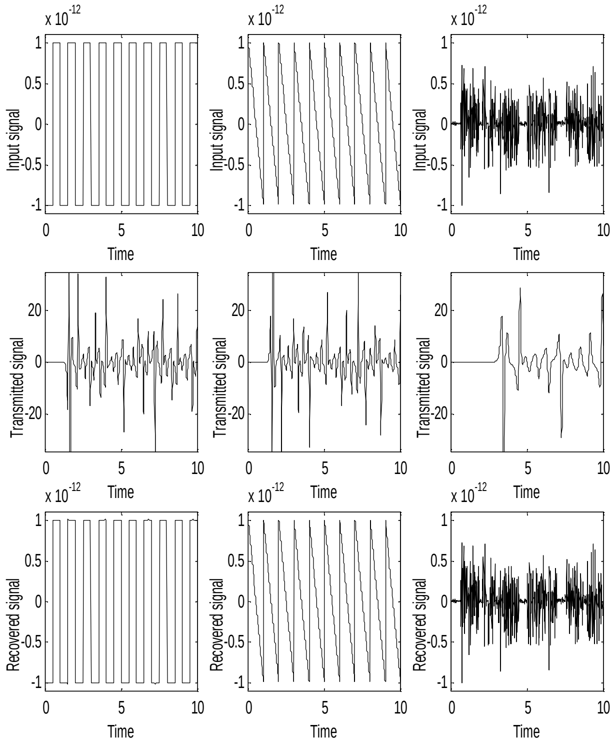
Fig 2 The Lorenz decryption system

The key is a 90 digit number representing the parameters of the system and the initial condition. Not shown in Figs 1 and 2 is a system of demultiplexing the key and providing the values of the parameters and initial conditions to the system.

3. SYSTEM SECURITY

The most important aspect of security is the identification of the key and the computational effort required to determine it. If we consider the Lorenz system, there are three constants in the equations and three initial conditions in the integrators. Each of these has to be adjusted to an accuracy of one part in 10^{15} to achieve synchronisation between transmitter and receiver. One could consider that these are the system keys and that 10^{90} mathematical steps are required for brute force cryptanalysis. This however is not true as chaotic systems can be analysed using more systematic approaches, which drastically reduce the computational effort required. The evaluation of the mathematical efforts required will be made in a separate paper [6]. We wish to mention here that the constants in the equations can also be non-linear functions of the state variables of any desired complexity and any number of parameters provided that they are bounded and do not take the system out of chaos. This adds considerably to the security of the system.

A very important feature of the systems is the ability to transmit very low signal to chaos ratios and recover the message fully without loss of information. Signals to chaos ratios between -200 dB and -244 dB have been achieved. The exact ratio depends on the complexity of the plaintext and the desired accuracy of the recovered signal. This low signal to chaos ratio makes it almost impossible to retrieve the plaintext from knowledge of the ciphertext alone. Results on the effect of the signal to chaos ratio on the recovery of the signal are given later in this chapter. Fig. 3 shows how a square-wave, a saw-tooth and a voice signal are accurately recovered with a signal to chaos ratio of approximately -240 dB.



(a) (b) (c)

Fig. 3 Results of the system simulation for (a) square, (b) saw-tooth and (c) speech signals.

Another aspect of security is the sample time of the signal and the algorithm time constants have to be adjusted such that the spectrum of the signal falls within the spectral band of the chaos for maximum security. The step size of the solution affects the signal to chaos ratio that can be used. Reducing the step size will allow a reduction in the signal to chaos ratio but will increase the processing time. Fig. 4 shows a comparison of the spectrum of the signal and the chaos (Lorenz system) for an ASCII message. We note that the ASCII signal has a high DC value as to be expected.

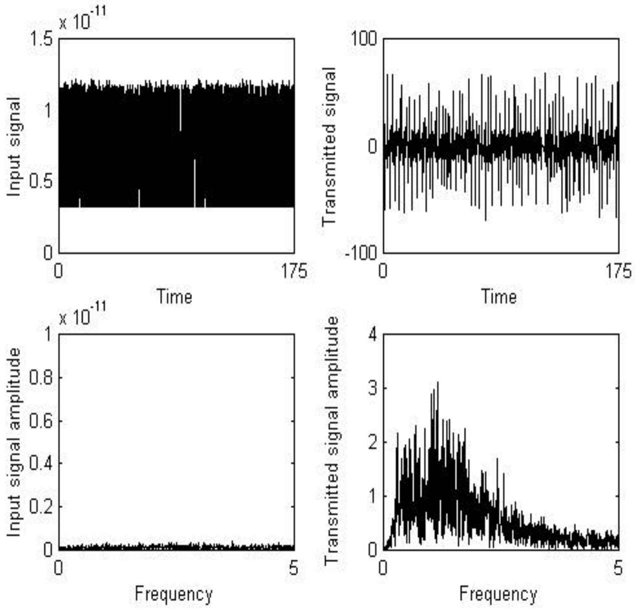


Fig 4. Comparison in the time and frequency domains between the information and chaotic signals

Another aspect of security is that the sample time of the signal and the algorithm time constants have to be adjusted such that the spectrum of the signal falls within the spectral band of the chaos for maximum security. The step size of the solution affects the signal to chaos ratio that can be used.

4. RESULTS

Next, we will introduce the results of encrypting and decrypting text and image files. First, we give results of encrypting and decrypting an ASCII text file which was sent via email. The file size of the plaintext is 395 bytes and the cipher text is of the same size. The time for the encryption is 0.598 seconds and the time taken for the decryption is 0.974 seconds.

Plaintext

Recently, Pecora and Caroll demonstrated the possibility of synchronizing the chaotic systems [5]. Makoto et al introduce 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_O_
-_&__(S07q_O_/_'#__PG_w*L
8_______/!_&V72v_Q%%____ _)0__CW iR<H___2%
A;__7[_Z`,L_#__ __1*__RK
_z+M:___<__O$__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_,______*_ %O20o
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 [5]. Makoto et al introduce 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.

The results of sending an image via email using the Lorenz system are given below. Fig. 5 shows the original image, fig 6. shows the encrypted image which was transmitted via email and Fig 7 shows the received image after it has been decrypted.

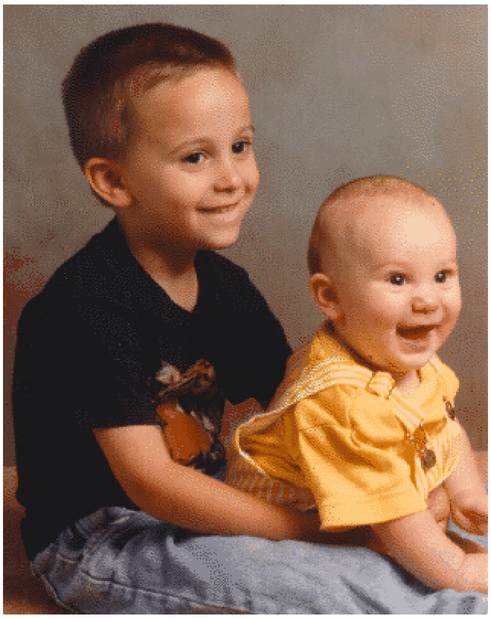


Fig 5. The original image

Fig 6. The encrypted image

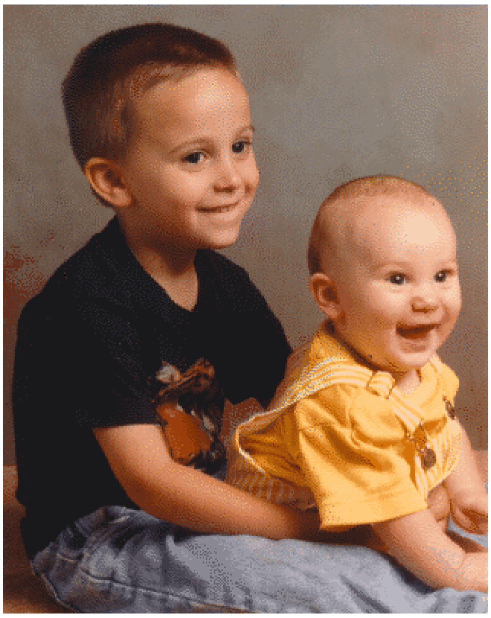


Fig 7. The recovered image

In the above example the signal to chaos ratio was –240 dB. The time taken by the encryption and the decryption processes was about 20 seconds. The signal was transmitted as an appended file in an email message. The image used is kids.tif which is included in the image library of MATLAB©. The file size is 93kB.

Black and white images are two dimensional arrays and colour images are three dimensional arrays. The algorithms deal only with time sequences and hence image files have to be redimensioned as a one dimensional array before processing. This process is automatically reversed in the decryptor.

5. METHODS OF ATTACK

As mentioned before, the system derives its security from the following characteristics:

- The very high chaos to information ratio makes it impossible to attack the ciphertext using any signal processing techniques such as Fourier transform.
- The long key length makes is difficult to attack the system by brute force methods.

However if we assume that the system, apart from the key, is known, then it is possible to devise an optimisation routine that will discover the key by minimising the output. This technique will be discussed more fully in a separate paper [6].

To counter this method of attack, the system parameters are made non-linear functions of the state variables. The only limitation on the functions used is that they have to be bounded so that the system in not taken out of chaos. In such systems the cryptanalist has to know all the functions and their parameters. So far we have not discovered a method that can attack such systems.

6. CONCLUSIONS

We have presented an encryption method based on chaotic algorithms that can be used for generating secure data bases and for sending secure email. The method offers very high security and there are no known methods of attack. The algorithm can be used either for text files, images or formatted files. The study of the system security and methods of attack is continuing.

7. REFERENCES

[1] Corron, N. J. & Hahs, D. W. “A new approach to communications using chaotic signals”, *IEEE Trans. Circuits and Systems* I, vol 44(5), pp 373-382, 1997.

[2] Cuomo, K. M., Oppenheim, A. V. & Strogatz, S. H. [1993] “Synchronisation of Lorenz-based chaotic circuits with applications to communications”, *IEEE Trans. Circuits and Systems* II, vol 40(10), pp 626-633, 1993.

[3] Feldmann, U., Hasler, M. & Schwartz, W. “ Communication by chaotic signals: The inverse system approach”, *Int. J. Circuit Theory and Applications*, vol 24, pp 551-579, 1996.

[4] WU, C. W. & Chua, L. O. “A simple way to synchronize chaotic systems with applications to secure communication systems”, *Int. J. Bifurcation and Chaos*, vol 3(6), pp 1619-1627, 1993.

[5] Pecora L.M. and Caroll T.L. “Synchronising Chaotic circuits”, IEEE Tran. Circuits and Systems, vol CAS-38 No4, p453-456, April 19991.

[6] M.I. Sobhy and A.R. Shehata , “Chaotic Algorithms for Data Encryption”, paper submitted for presentation in this conference.