A Stegosystem with advanced security features
Simulated in Matlab
16th Panhellenic Conference on Informatics (PCI 2012)

Prof. Antonios Andreatos (1) and Prof. Apostolos Leros (1,2)

(1) Div. of Computer Engineering & Information Science
Hellenic Air Force Academy
Dekeleia, Attica, TGA-1010, GREECE
informatics.hafa@haf.gr, aandreatos@gmail.com

(2) Department of Automation
School of Technological Applications
Technological Educational Institute of Chalkis
34400 Psachna, Euboea (Evia), GREECE
lerosapostolos@gmail.com
Abstract

This paper presents a Steganography Telecom System for data cryptography, based on a Chaotic Noise Generator.

Characteristics:

- The ciphertext is randomly distributed on a cover image in a stochastic mode.
- The whole system presents advanced security features.
- Simulation results which demonstrate the proof of concept are presented.
Abbreviations

- TRNG: True Random Number Generator
- PRNG: Pseudo Random Number Generator
- CTRNG: Chaotic True Random Number Generator
- LSBs: Least Significant Bits
1. INTRODUCTION

This paper presents a secure steganography telecom system (Stegosystem) with advanced security features.

In the Transmitter, the text message (an ASCII string) is encrypted character-by-character with chaotic values produced by a standard Chua's circuit.

The ciphertext is then hidden in an image (steganography).
In the receiver...

... the inverse process takes place to recover the original text message.

**The receiver needs to know:**

- the initial conditions of the continuous differential equations describing the Chua's circuit;
- the equation generating the chaotic Noise $N(t)$;
- the discretization time step ($dt$) for solving the continuous differential equations using the Euler’s method;
- the **seed** as well as the algorithm of the **PRNG** used to distribute the ciphertext on the cover image;

Given the same seed, receiver's PRNG produces exactly the same seq. as the that of the transmitter.
Steganography

Steganography is a technique for concealing data within different types of data, usually redundant, such as images.

For the past decade, many steganographic techniques for still images have been presented both in the spatial and frequency domains. The simplest and most popular method in the spatial domain is the Least Significant Bits (LSBs) Substitution.
LSB Steganography

LSB steganography is the process of adjusting the least significant bit pixels of a carrier image in order to hide a message. In its simplest form, the bits of the secret message substitute the LSBs of consecutive pixels of an image, one bit in each pixel. For this method to work, the pixels of the image must have fixed length, e.g. 8 bits for grayscale images or 24 bits for color images.
Chua's (standard) circuit is a simple non-linear circuit, producing chaotic behavior for a specific set of component values; in particular, its behavior is characterized by a double-scroll chaotic attractor.

The circuit was proposed by Prof. Leon O. Chua in Japan [1983], in his effort to demonstrate chaos in an actual physical model and to prove that the Lorenz double-scroll attractor is chaotic.

Chua's circuit suits the study of chaos well, because one can precisely control its parameters and observe the results on an oscilloscope. Therefore, it has found many applications.
Figure 1. (a) Standard Chua's circuit; (b) i-V characteristic of the nonlinear device Source: [18].
In Figure 1

- $V_{C1}$ and $V_{C2}$ denote the voltages across the capacitors $C1$ and $C2$, respectively,
- $i_L$ is the current through the inductor $L$, and
- $g_{NR}(V_{C1})$ is the nonlinear function which defines the $i$–$V$ characteristic (conductance) of the nonlinear device represented by the piecewise-linear function of Fig. 2b.

By solving the above circuit we get the following differential equations (1—4):
Chua circuit differential equations

\[
C_1 \frac{dV_{C1}}{dt} = \frac{1}{R} (V_{C2} - V_{C1}) - g_{Nr}(V_{C1}) \tag{1}
\]

\[
C_2 \frac{dV_{C2}}{dt} = \frac{1}{R} (V_{C1} - V_{C2}) + i_L \tag{2}
\]

\[
L \frac{di_L}{dt} = -V_{C2} - R_0 i_L \tag{3}
\]

\[
g_{Nr}(V_{C1}) = G_b V_{C1} + \frac{1}{2} (G_a - G_b) (|V_{C1} + E| - |V_{C1} - E|) \tag{4}
\]
$V_{C1}$, $V_{C2}$ and $i_L$ are the state variables of the chaotic system; in our code they are represented by three discrete-time variables: $X_1(t)$, $X_2(t)$ and $X_3(t)$. For $t=0$ we have the initial conditions.

The chaotic noise $N(t)$ is a arbitrary, secret function of state variables $X_1(t)$, $X_2(t)$ and $X_3(t)$; this provides an additional level of security to our system, in case the topology of Chua's circuit becomes known to opponents.

$$N(t) = X_1^2(t) + X_2(t) + X_3(t)$$

The continuous differential equations of $X_1(t)$, $X_2(t)$ and $X_3(t)$ [equations 1-3], are solved using Euler’s method, in order to achieve a constant time-step.
Chua's circuit response is very sensitive to the initial conditions

Plot of Chua Variable $X_1(t)$ for Different Initial Conditions

- $X_1(0) = 1.0; X_2(0) = 0.0; X_3(0) = 0.0$
- $X_1(0) = 1.0; X_2(0) = 1.0; X_3(0) = 0.0$
- $X_1(0) = 1.0; X_2(0) = 0.0; X_3(0) = 0.0005$
Master-Slave configuration

The proposed system uses two identical Chua's circuits, one in the Transmitter and one in the Receiver, in a Master-Slave configuration. This configuration coordinates the two identical Chua's circuits and also compensates the varying tolerance of their components so that they produce the same output.

To produce exactly the same noise at the Receiver, the Slave Chua's circuit needs to get some information concerning the initial state of the Master Chua circuit [X1(0), X2(0) and X3(0)].

This information must be transferred to the Receiver via a secure channel.
Figure 3.

Simplified block diagram of the proposed Stegosystem

Info. thru the Secure channel:
1) Component values
2) Initial conditions
3) Chaotic noise function N(t)
4) Cover image
5) PRNG algorithm + seed
V. Simulation results

ORIGINAL MESSAGE (1st paragraph):

Like his teacher Plato, Aristotle's philosophy aims at the universal. Aristotle, however, found the universal in particular things, which he called the essence of things; while Plato finds that the universal exists apart from particular things, and is related to them as their prototype or exemplar.

CIPHERTEXT (1st paragraph):

Mlni%nq},fww|……–Fy–Œž~RCaŽ ‘‡„{sj*u"rjknqvrsk|#emt}.sŠ:ŠŠǴ—‘œ %o“̀ z·? Kynwvrng."krzhyhu0$myf y9`®E„”÷™†Žx€0vx(veuvlewncu#wlouq,? $—”œWîÝX”—‘{1€oi!ettiwpv4†~9€,x,8*œonqh"Rncup!hlsl€0‰.€™KœœœB-¥ž!—‘z. œ nwww&j}q…‰7|‡f 0~l{{ogyodu#wlmsm{6-r…·C’®T^á¥Ô¥™Oœéc8†tlp at"zs\Œ=Ž‰šŒq*wx$hzgoroew3
Figure 4. Chaotic variable $X_1(t)$ produced by Chua’s circuit
Figure 5. Stem plot of Chua noise $N(t)$
Figure 6. Stem plot of the Ciphertext
Figure 7. Original (cover) image
Figure 8. Stem plot of the distribution of random positions; proves that the distribution of the information in the stego image is uniform. Note: the cover image has 151194 pixels.
Figure 8a. Detailed stem plot of the distribution of random positions for the first 30 consecutive positions. E.g., pos. 5 will occupy place no. 16503 after the permutation.
Figure 9. Stem plot of ciphertext values spread in random positions over the dimension of stego image before transmission.
Figure 9c. Detail of Stem plot of ciphertext values spread in random positions; most values are zeros
Figure 10. Stego image containing ciphertext bytes in random pixels
Figure 3.

Simplified block diagram of the proposed Stegosystem
Figure 11. Stem plot of recovered ciphertext
VI. Advanced security features

The system presents advanced security, based on the following features:

- **the unknown Chua’s circuit topology**;
- **the unknown initial conditions** of the continuous differential equations describing the Chua's circuit;
- **the unknown discretization time step** (dt) for solving the continuous differential equations using the Euler’s method;
- **the unknown function of state variables** \(X_1(t), X_2(t)\) and \(X_3(t)\) producing the chaotic noise \(N(t)\);
- **the unknown, random places** of the ciphertext in the stego image.

Note that the encryption of each character of the plain text is different each time, due to the CTRNG;
VII. Conclusion

In this paper we have proposed an innovative stego telecom system with advanced security features. The system is based on a CTRNG implemented by two Chua’s circuits connected in a Master-Slave fashion; this is imperative for getting the same chaotic signal at the receiver, in order to reproduce the ciphertext by subtraction from the transmitted signal (stego image).

To achieve the Master-Slave configuration in practice, the two Chua’s circuits must be coupled; this is achieved via a specific controller/compensator, which guides the trajectory of the Slave chaotic system to specific areas producing specific behavior (the same with the Master Chua circuit); see ref. [10].
Conclusion (2)

A special security feature introduced in the proposed system is that the ciphertext is placed in (pseudo) random places, uniformly distributed in the whole stego image; this feature makes the revealing of the ciphertext more difficult than typical schemes traditionally used (such as the LSB’s method), which are predictable.

A PRNG is used to produce these random places; hence, its initial seed must also be transferred to the Receiver during the initialization phase, through the secure channel.

The proposed system works with both grayscale and color images.
END of the PRESENTATION

- Thank you for your attention

- Any questions?

Downloaded from:
http://t-h.wikispaces.com/


Metadata


Keywords - Stegosystem; Steganography; Chua’s Circuit; Chaotic Noise Generator; Cryptography; Simulation; Matlab.

Full paper: available through IEEE Computer Society's Conference Publishing Services [IEEEXplore].