An audio steganography system using Chua Chaotic Noise Generator

ATHCON 2013

Antonios Andreatos (1) and 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

We present an audio steganography telecom system for data cryptography, based on a Chua’s circuit chaotic noise generator. A two-phase process is used. First, the plain text is encrypted using a symmetric cryptographic function based on Chua's circuit, to produce the ciphertext. Next, the ciphertext is padded w. 0's, shuffled & hidden in a cover sound. The resulting stego sound is transmitted over the insecure channel.
Abstract (2)

- At the receiver the ciphertext is retrieved from the incoming sound and then it is fed to an identical Chua’s circuit to produce the initial clear text.

- Matlab simulation results which demonstrate the proof of concept will be presented.
Abbreviations

- TRNG: True Random Number Generator
- PRNG: Pseudo Random Number Generator
- CRNG: Chaotic Random Number Generator
- ODE: Ordinary Differential Equation
1. INTRODUCTION
Steganography

Steganography is a technique for concealing data within other, different types of data, usually redundant, e.g., images.

However, audio as well as video signals may be used.
At the Transmitter, the clear text (an ASCII string) is encrypted character-by-character with chaotic values produced by a standard Chua's circuit.

Chua's circuit is a CRNG.

The ciphertext is then padded with 0's, shuffled and hidden in an audio signal. A PRNG is used to produce the random positions for placing the ciphertext bytes in the audio signal.
At the receiver...

... the inverse process takes place to recover the original text message. An identical Chua circuit is used.

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 discretisation time step ($dt$) for solving the continuous ODEs using the Euler method;
- the seed as well as the algorithm of the PRNG used to distribute the ciphertext on the cover sound;
- the audio signal.
2. CHUA’S CIRCUIT

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 characterised 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. Therefore, it has found many applications, especially in cryptography.
Figure 1. (a) Standard Chua's circuit; (b) i-V characteristic of the nonlinear device
Implementation of the non-linear device Nr
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. 1b. $G_a$, $G_b$ are the slopes in the inner and outer regions, while $\pm E$ denotes the breakpoints.

By solving the above circuit we get the following differential equations (1-3):
Chua circuit differential equations

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

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

\[ L \frac{di_L}{dt} = -V_{C2} - R_0 i_L \]  \hspace{1cm} (3)

\[ g_{Nr}(V_{C1}) = G_b V_{C1} + \frac{1}{2} (G_a - G_b) (|V_{C1} + E| - |V_{C1} - E|) \]  \hspace{1cm} (4)
$V_{c_1}$, $V_{c_2}$ 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.
Double-scroll chaotic attractor
Standard sets of values

Chaotic behaviour is observed for specific sets of component values. Example:

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>C2</td>
<td>L</td>
<td>R0</td>
<td>Ga</td>
<td>Gb</td>
<td>Bp</td>
</tr>
<tr>
<td>10nF</td>
<td>100nF</td>
<td>22mH</td>
<td>22Ω</td>
<td>-.75ms</td>
<td>-.4ms</td>
<td>1.75V</td>
</tr>
</tbody>
</table>

Response of Chua's circuit is very sensitive to component values, as well as, their tolerance.
Chaotic noise $N(t)$

The chaotic noise $N(t)$ is an 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 intruders.

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

The continuous differential equations of $X_1(t)$, $X_2(t)$ and $X_3(t)$ [equations 1-3], are solved using the Euler method, using a constant time-step $dt$.

Another example: $N(t) = X_1^2(t) + X_2(t) + X_3(t)$
Chua's circuit response is very sensitive to the initial conditions

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

- Blue line: $X_1(0) = 1.0; X_2(0) = 0.0; X_3(0) = 0.0$
- Green line: $X_1(0) = 1.0; X_2(0) = 1.0; X_3(0) = 0.0$
- Red line: $X_1(0) = 1.0; X_2(0) = 0.0; X_3(0) = 0.0005$

Time sec

$X_1(t)$
3. SYSTEM DESCRIPTION
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 sound
5) PRNG algorithm + seed
6) Step of Euler method dt
4. SIMULATION RESULTS

- The whole system was simulated in Matlab. Some results will be presented below. A wav signal was used as a cover audio signal.
- The following paragraph was used as cleartext (386 characters including spaces):
All paper submissions are expected to be written in and will be reviewed in English. You are welcome to submit material, regardless of your organisation. AthCon welcomes cutting edge information security research from industry, researchers, professionals, academics, government and the underground security community. As a guideline, the following topics are rendered relevant for 2013

- Boo#setiw%y{htpz{qwv{(iyI'k~ujgxi#up!ce wrriufp#mr%gtj'~ptt(jm'yl| ok|jh$Lq"Fohlish. Zpv"dvi%|krjvtl(|w'z|isoy%rexhulcm-! sfhbtfixy'wn)x{}x{oivpzhznus1!Btf@lj#sah_kibp#asrshnh!fehf! inemoj]qejh#l^nkbn$#mbqc`rci#jsr %otj{yzx~1%viwhduejgtu."ruskjr{qzwju| 5)jlmtjpy2%lsxeqljajo#i_#pdb#tmddrhtqwqg#wigyvmx}$gsqqyrny~4&Gz'h'o}qlmtqvl3&zmj$jsoopxjng topict! buh$wtjyklk'ylsl!htz&ktw$64460
Cleartext
Ciphertext
Cover audio signal
Stego signal
Part of stego signal with ciphertext
Received Cleartext
Our cipher is resilient, since neither monoalphabetic nor polyalphabetic nor even block cipher is used; instead, chaotic encryption maps the same plaintext to different ciphertext per occurrence, as demonstrated by the following example:

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Athcon 2013 Athcon 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ciphertext</td>
<td>Bwkfrr$6569&amp;G{ojwv(:89;</td>
</tr>
</tbody>
</table>
Key of the Crypto/Stegosystem

We may consider that the key of the system is the exact values of the following set of parameters:

C1, C2, L, Ro, R,
Ga, Gb, E;
dt; N(t); cover audio; PRNG algorithm, PRNG seed.

Thus, the proposed system is highly parameterisable.
5. ADVANCED SECURITY FEATURES

The system presents advanced security based on the following features [5]:

- the unknown Chua's circuit component values;
- the unknown initial conditions of the continuous differential equations describing the Chua's circuit;
- the unknown discretisation time step (dt) for solving the continuous differential equations using the Euler method;
- the unknown function N(t) producing the chaotic noise;
ADVANCED SECURITY FEATURES (2)

- the unknown cover audio signal;
- the unknown starting place of the message within the stego audio signal;
- the unknown places which store the message in the stego audio signal (PRNG) and finally,
- resistance to common (known, chosen) text attacks.

The encryption of each character of the plaintext is different each time, due to the CRNG.

Triple security: Even if the steganography is broken, the message won't be revealed since it is encrypted and randomly shuffled.
6. CONCLUSION

- We have presented an innovative audio steganography system with advanced security features.
- The plaintext gets encrypted using CRNG before being padded and hidden in a cover audio signal. Cryptography is based on two identical Chua’s circuits, one at the transmitter and the other at the receiver; this is imperative for getting the original plain text at the receiver, given the ciphertext, after being extracted from the stego audio signal (see block diagram).
- The system works with both mono & stereo audio signals.
CONCLUSION (2)

• A special security feature of the proposed system is that the ciphertext is placed in (pseudo) random places, uniformly distributed in the whole stego audio signal; however, this can be achieved only if the whole text message is available in advance.

• 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 initialisation phase, through a secure channel.
Future work

- A proper modification of the system will enable it to operate in real-time (stream cipher mode).
- The use of video as cover signals will be considered.
- Other methods -instead of the Euler method- for solving ODEs will be tried (e.g. Runge-Kutta 4th order).
- Padding of the cipherext with random numbers instead of 0's.
Demo: cover audio (stereo)
Stego audio signal (mono)
Comments

Notice the ciphertext at the beginning of the cover audio signal!

This is because the cover audio signal starts with silence.
END of the PRESENTATION

• Thank you for your attention

  – Any questions?

More:
http://t-h.wikispaces.com/chua-chaos
REFERENCES


REFERENCES (2)


Keywords - Stegosystem; Steganography; Cryptography; cover audio signal; Chaotic Random Number Generator; Chua’s Circuit; Chaotic Noise Generator; Simulation; Matlab.