CHAOTIC ENCRYPTION ALGORITHMS BASED ON MODIFIED DIGITAL FILTER STRUCTURES

Ph.D. Cvetko D. Mitrovski [1] and Ph.D. Ljupco M. Kocarev[2]

[1] Technical Faculty - Bitola , P.O. Box 99, 97 000 Bitola, Republic of Macedonia , fax: + 389 97 48 320, e-mail: mcvetko@soros.org.mk

[2] Faculty of Electrical Engineering-Skopje, P.O. Box 574, 91000 Skopje, Republic of Macedonia , fax: +381 91 364 262 ; e-mail: lkocarev@cerera.etf.ukim.edu.mk

Abstract: In this paper we present a class of chaotic encryption algorithms, developed by modeling the modified structure of the conventional chaotic self synchronized encoder-decoder system, based on an n-th order digital filter with 2's complement overflow non linearity. The modification of the initial structure is obtained by reducing the order of the filter to one and by introducing feedback connections from the states of an added stable nonlinear subsystem which is realized as a cascade of stable first order IIR digital filters, each driven by a) a linear combination of the delayed encoder signal and the states of the preceding stages, and b) a nonlinear transformation of the state of the preceding stage.

1. Introduction

In the last few years, there is an ever increasing interest for use of chaos in secure communications. Although the most of the presented studies are concentrated on analog systems [1], there are already some new tendencies for studying the discrete systems [2],[3],[4], due to their advantages over the analog circuits, and the possibility of their practical implementation either with software or with hardware. In both cases, the basic encoder-decoder structure is based on synchronization (or self-synchronization) of the inverse system with the driving chaotic one. This concept enables chaotic masking (encryption) of the information in the driving system (encoder), and its extraction at the output of the driven system (decoder), after its synchronization with the driving one.

This idea is already recognized in the model of an n-th order non autonomous digital filter with 2's complement overflow characteristic f(.), connected to its inverse system (Fig-1). If the first digital filter exhibits chaotic behavior, then it is a typical example of chaotic encoder-decoder system with self-synchronizing structure which was fully investigated as a cryptographic system in [4]. There, it was shown that this system has very low security due to the simplicity of its dynamic and due to the fact that the encoded signal, y(k),(chipertext) contains complete information about the states of the encoder.

In this paper, we try to explain how to overcome those cryptographic weaknesses of the digital filter, by proposing its modification in order to obtain a new model, with same structure but with improved cryptographic characteristics [6].

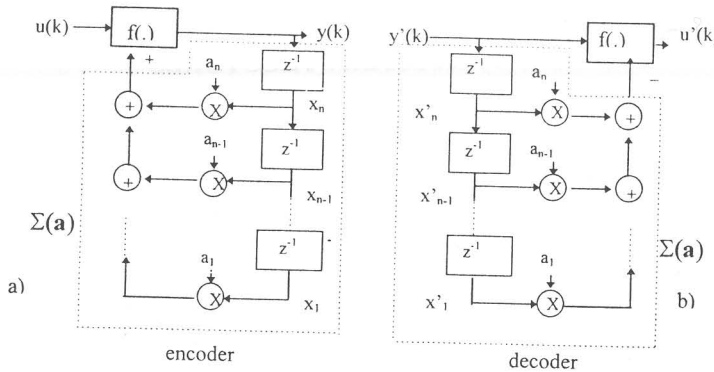

Fig-1 Encoder-decoder pair realized by an n-th order digital filter structures

2. General characteristics of the digital filter structure

On the schema depicted in Fig-1, two identical subsystems in both the encoder and the decoder can be identified. They are:

- arithmetic unit with 2's complement overflow characteristic, f(.) and
- dynamic subsystem, $\Sigma(\mathbf{a})$, with a parameter vector, $\mathbf{a}$.

In the encoder, the output of the dynamic system is feedback to the arithmetic unit, while in the decoder, the output is feed forwarded to the arithmetic unit. Hence, the cryptographic weaknesses of the digital filter are caused only by the structure of the SISO subsystem, $\Sigma(\mathbf{a})$ (designed as a chain of n-delay elements). Therefore, we have decided to design a new encoder model with the same global structure, but with a modified subsystem $\Sigma_1(\mathbf{a}_1)$. The modified subsystem must satisfy the following demands: a) it must be stable, and b) it has to provide chaotic behavior of the whole system for a wide range of its parameters.

3. Modified encoder structure

By following the global demands for $\Sigma_1(\mathbf{a}_1)$ we have derived the modified encoder structure, depicted in Fig-2. It is obtained by reducing the order of the filter to one and by introducing feedback connections from the states of newly added stable nonlinear subsystem which is realized as a cascade of stable first order subsystems, each driven by a) a linear combination of the delayed encoder signal y(k-1) and the states of the preceding stages, and b) a nonlinear transformation of the state of the preceding stage.

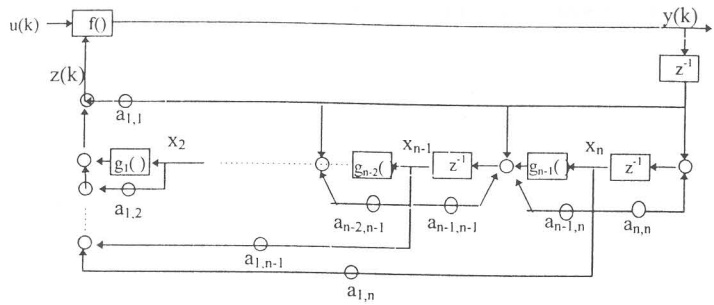

Fig-2 Modified encoder with self synchronized structure

The dynamics of the encoder is modeled by the following set of difference equations

$$
\begin{aligned}
x_1(k+1) &= y(k) = f(z(k)+u(k)) \\
x_i(k+1) &= g_i(x_{i+1}(k)) + x_1(k) + \sum_{j=1}^{n} a_{1,j}x_j(k) \;\; ; \; i = 2,3,\ldots,n-1 \\
x_n(k+1) &= a_{n,n}x_n(k) + x_1(k) \\
z(k) &= g_1(x_2(k)) + \sum_{j=1}^{n} a_{1,j}x_j(k)
\end{aligned}
\qquad (1)
$$

where: x_i, i = 1,2,...,n, are the encoder states, g_i, i=1,...,n-1 - are nonlinear functions, $a_{i,j}$ (i=1,2,..,n ; j=i,i+1,...,n) - are parameters, and u(k), y(k) and f( ) have the same meaning as in the previous text.

The new encoder has much more complex structure which prevents direct internal state information into the driving encoded signal y(k) (chipertext).

The nonlinear functions in the model have two roles: a) to perplex any attack attempts based on the analysis of the chipertext and b) to prevent appearance of attracting fixed points in autonomous regime of operation.

In order to fulfill the second role, the nonlinear functions must satisfy the following condition - $|dg_i(x)/dx| > 1$, on their whole definition range. The parameters of the nonlinear functions, g_i, i=1,...,n-1, can also be considered as a part of an encryption key. Hence, each nonlinear function g_i affects both directly and indirectly the size of the parameter key space. The direct influence is obvious, while the indirect one is affected by increasing the sensitivity of some parameters of the encryption algorithm. Actually, since the nonlinear functions satisfy the condition $|dg_i(x)/dx| > 1$, the nonlinear blocs act as

amplifiers, which directly affects the sensitivity of each parameter on the signal path from the output of the encoder, up to the input of the nonlinear block.

The parameters of the model can be categorized in tree groups:

- parameters which determine the convergence process, $a_{i,i}$, i =2,…,n.
- rest of the "a" parameters and
- parameters of the nonlinear functions.

The parameters from the first group are restricted to satisfy the condition $|a_{ii}| < 1$, while the other parameters can be chosen quite arbitrary. With the parameters of the first group we can adjust the speed of the synchronization between the encoder and the decoder.

3.1 Decoder and error model

The decoder is modeled by the following set of difference equations:

$$x_1'(k+1) = y'(k)$$

$$x_n'(k+1) = a_{n,n}x_n'(k) + x_1'(k);$$

$$x_i'(k+1) = g_i(x_{i+1}'(k)) + x_i'(k) + \sum_{j=i}^{n} a_{i,j}x_j'(k) \quad ; \; i = 2,..,n-1 \tag{2}$$

$$u'(k) = f(y'(k) - z'(k)) = f(y'(k) - g_1(x_1'(k)) - \sum_{j=1}^{n} a_j x_j'(k))$$

where: $x_i'(k)$, i=1,2,…,n, are states of the decoder, y'(k) is driving chaotic input and u'(k) is decoded signal. In case when the transmission channel is ideal, y(k) = y'(k), we can subtract the corresponding equations from (1) and (2). So we derive the error model

$$e_1(k+1) = 0$$

$$e_n(k+1) = x_n(k+1) - x_n'(k) = a_{n,n}e_n(k) \tag{3}$$

$$e_i(k+1) = g_i(x_{i+1}(k)) - g_i(x_{i+1}'(k)) + \sum_{j=i}^{n} a_{i,j}e_j(k) \; ; \quad i = 2,\ldots,n-1$$

The error model is stable due to the stability of the IIR filters, $|a_{ii}| < 1$, i =2,…,n. From it, we can conclude that the convergence process of the internal states is asymptotic, and that it has the following sequential order: $x_n'(k) \rightarrow x_n(k)$; $x_{n-1}'(k) \rightarrow x_{n-1}(k)$; … ; $x_1'(k) \rightarrow x_1(k)$, after which, the original information is decoded on the output of the decoder, $u'(k) \rightarrow u(k)$.

This means that if each parameters of the decoder is identical to the corresponding one of the encoder we can reconstruct the original information asymptotically. In any other case, the reconstruction can be disturbed (Fig-3d), or even completely disallowed if the difference between any pair of corresponding coefficients exceeds certain analytically determined level (Fig-3e).

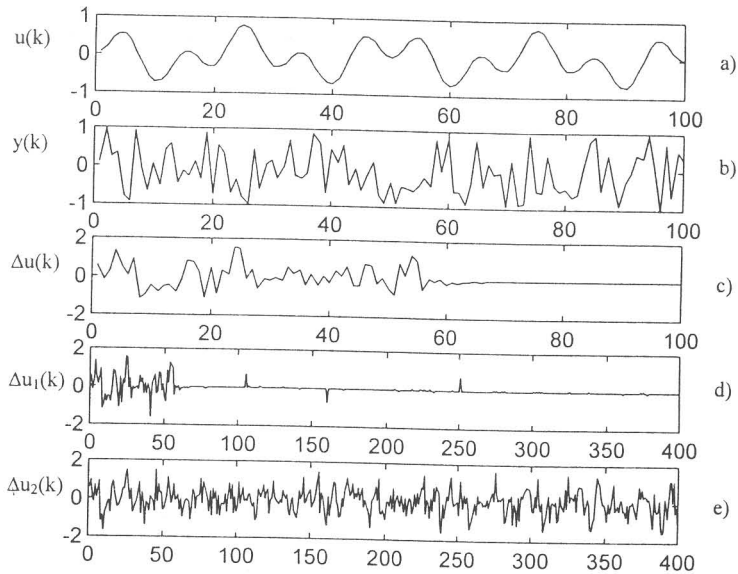

Fig-3. Simulations on model with parameters:$a_{1,1}$=3.2; $a_{2,2}$=-0.8; $a_{3,3}$= -0.4; $a_{1,2}$=2.3; $a_{1,3}$=-3.4; $a_{2,3}$=5.6, a) information signal u(k), b) encoded signal y(k), c) synchronization, d) reconstruction disturbances due $\Delta a_{33} = 10^{-6}$ e) reconstruction error due $\Delta m_1 = 10^{-5}$, m -module parameter in g_1.

4. Experimental results

In our experiments we have used simple, low order encoder models with nonlinear blocks realized by piece wise-linear functions with sharp slopes in combination with a module operator. The module operator was used in order to limit the output ranges of the nonlinear blocks. On our models we have performed extensive simulations, as illustrated in Fig-3, which have enabled us to state the following remarks:

1. We have confirmed the dependence of the synchronization process and the parameters $a_{i,i}$, i = 2,…,n. If any of those parameters has nonzero value, then the duration of the synchronization is always much longer than the order of the model (Fig-3b).
2. The sensitivity of each parameter $a_{i,j}$; i >1, i<j, which is positioned in a cascade before the nonlinear block function g_{i-1} , increases with increasing

the slopes of the piece-wise linear functions. The other parameters are not affected.

3. Very small variations of the parameters $a_{i,j}$, $i>1$, causes small disturbances of the reconstructed signal, but with sporadic high level picks (Fig-3d).
4. The parameters of the nonlinear functions g_i are extremely sensitive (Fig-3e)
5. The decoder is very sensitive to a transmission noise.

5. Conclusions

In this article we have presented a systematic approach for designing encryption algorithms starting from conventional schema of a digital filter with 2's complement overflow. The derived encoder consists nonlinear elements which can be realized by any set of properly designed nonlinear functions. Therefore, the obtained schema offers great flexibility in designing various encryption algorithms, which has to be further investigated.

The introduction of nonlinear elements in the encoder schema also increases the key parameter range (by increasing the sensitivities of the parameters) and security of the whole system, while simultaneously decreases the noise immunity of the decoder. Therefore this cryptographic algorithm is suitable only for use in reliable environment, like digital computer networks.

6. Literature

[1] L.Kocarev, K. Halle, K. Eckert, L. O. Chua, U. Parlitz, "Experimental demonstration of secure communications via chaotic synchronization", International Journal of Bifurcation and Chaos, Vol 2., pp 709-713, 1992

[2] D. R. Frey, "Chaotic Digital Encoding: An Approach to Secure Communication", IEEE Transactions on Circuit and Systems -II: Analog and Digital Signal Processing, Vol. 40, pp 660-666, 1993

[3] M.Gotz, K. Kelber, W. Schwarz, "Discrete-time coders for information encryption, Part 1:Systematic structural design", NDES'96, pp 21-26, Sevila, 1996

[4] K. Kelber and T. Kilias, "Analysis of an Encoder-Decoder system based on digital filter structures with two's complement overflow characteristics", ISACS'96, pp 166-169, Sevila, 1996

[5] S. Papadimitiou, A. Bezerianos and T. Bountis, "Secure Communication with Chaotic Systems of Difference Equations", IEEE Transactions on computers, Vol. 46. No. 1, pp 27-38, 1997

[6] C. D. Mitrovski: " Complex behavior in digital filters and application in encoding of information " Ph.D thesis, Skopje, 1997