A generalized chaotic encryption system for multimedia applications

R. Hasimoto-Beltrán
Center for Research in Mathematics (CIMAT),
Jalisco s/n, Col. Mineral de Valenciana, 36240 Guanajuato, Gto, México,
Phone: +(52)-(473) 732-7155, Fax: +(52)-(473) 732-5749,
e-mail: hasimoto@cimat.mx

Recibido el 3 de julio de 2007; aceptado el 4 de septiembre de 2007

Recently, several encryption schemes based on 1, 2, and 4 one-dimensional chaotic maps have been presented in the literature (see Ref. 1). The idea of increasing the number of maps is to provide more security and robustness to chaos-based cryptographic systems. In this paper, we propose a generalized encryption scheme based on N one-dimensional coupled chaotic maps, where only a window of m maps at a time ($m \leq N$) is active for the encryption process. The *m-map* window is randomly updated by shifting it circle-wise one map at a time through the entire *N-map* system. To add more security to the system, we randomly perturb the coupling parameter using current cyphertext output (spatiotemporal or global feedback); so that any change in the input data (plaintext) is reflected instantly in the total system (not only locally). Our generalized implementation is based on the scheme presented in Ref. 1, but it can also be implemented in any chaos based encryption scheme. Our approach adds more robustness to the system, maintaining excellent statistical properties and fast performance for real-time multimedia applications.

Keywords: Discrete chaotic encryption; block ciphers; symmetric encryption; coupled maps.

Recientemente se han publicado una serie de esquemas de cifrado caótico basados en 1, 2 y 4 mapas caóticos unidimensionales (ver Ref. 1). El propósito de incrementar el número de mapas caóticos es el de dar mayor seguridad y robustez a los sistemas de cifrado basados en caos. En este trabajo se propone un esquema generalizado de N mapas caóticos acoplados donde solo una ventana de m mapas a la vez es usada en el proceso de cifrado, para $m \leq N$. La ventana de m mapas acoplados es actualizada después de un periodo aleatorio de iteraciones mediante un recorrido circular a través de los N mapas en el sistema inicial. Para incrementar la seguridad del sistema, el factor de acoplamiento es perturbado por el valor más reciente de texto cifrado (conocido como retroalimentación global o espacio-temporal), permitiendo una reacción rápida y global ante cambios en el texto de entrada original y/o parámetros de los mapas caóticos. La implementación del esquema generalizado es basada en la Ref. 1, pero prácticamente cualquier método basado en caos puede ser utilizado. El método propuesto provee mayor robustez, mantiene excelentes propiedades estadísticas y puede fácilmente ser aplicado a sistemas de multimedia en tiempo real (video y audio).

Descriptores: Cifrado caótico discreto; cifrado simétrico; mapas acomplados.

PACS: 05.45.Gg/Pq/Ac

1. Introduction

Due to recent developments in the field of multimedia communications, applications such as Voice over IP (VoIP), videoconferencing, e-learning and digital TV/HDTV are part of our everyday life. We are immersed in a world-wide network where people do business on line, have access to news, bank accounts, etc., at the shield of their office or home. These digital commodities have some inherent risks: communication networks (wired/wireless) are vulnerable to attacks violating the use's right of privacy. We need fast and secure systems for current multimedia applications.

Discrete chaotic dynamical systems (DCS) were proposed in the late 80's as a viable alternative for secure data communications [3]. DCS have many of the good properties required in cryptography: the most prominent are sensitivity to parameters, sensitivity to initial conditions and unpredictable trajectories [4-6]. Current research in chaotic systems focus on two main lines: *Perturbance-based* schemes and *Network-based* chaotic maps. Perturbation–based schemes transform stable chaotic cycles into non-stable ones by perturbing their trajectory as was done in Ref. 2. Network-based chaotic Maps or Coupled Map Lattices (CML) on the other hand considers an array of chaotic maps governed by a coupling transformation over some defined neighborhood in the array [9]. New states represent the weighted interaction between each individual map (local term) and the coupling transformation (linear/nonlinear interaction term). When the weight of the coupling is weak, the system can be regarded as a local map perturbed by contributions from other sites, thus maintaining its main individual properties. On the other hand, when the weight of the coupling is large, the system reaches an asymptotic collective behavior characterized by intermittent periodic chaotic cycles (cycling chaos). Dellnitz, 1995 [10], found that when an individual map is active (presents chaotic behavior), the rest of the system elements remain quiescent. This process is repeated forever for each element of the system. Palacios and Juárez, 2002 [11], applied cycling chaos theory to improve Baptista's encryption scheme security [7]. Shujun Li, 2001 [8], proposed a Pseudo-Random bit generator based on CML, reporting perfect cryptographic properties for the construction of stream ciphers. Wang *et al.*, 2005 [12], combined a CML with bit-reverse operation applicable to symmetric cryptosystem and pseudo-random number generators.

In this paper we merge perturbance-based schemes with network-based schemes and propose a generalized block-based symmetric-key encryption system based on an *N-array* of coupled chaotic maps taking m maps at a time for the encryption process. We make use of a modified 3-level perturbation scheme proposed in [1] to increase the system space analysis in the case of brute-force and differential attacks. Our difference is that the first and third level perturbations modify the coupling parameter (not individual map variables) using the spatiotemporal feedback. The *spatiotemporal* feedback along with coupled chaotic maps makes the system extremely sensitive to plaintext and system-key changes.

The paper is organized as follows. In the next section we describe the proposed scheme. In Sec. 3 experimental results and security of the proposed systems are analyzed. Conclusions are presented is Sec. 4.

2. Chaotic encryption scheme

We take the system presented in Ref. 1 as the backbone for our generalized scheme, and consider the chaotic logistic map as the basis of the CML. Other chaotic systems can also be used without generally affecting the proposed algorithm. Following [1], the generalized system can be described as follows.

2.1. System-key generation

The initial system-key (K) of size B bits, for $B \geq 128$ and multiple of $n \in \{16, 32\}$ (bits to cipher per chaotic map) is shared between cipher and decipher. $N = B/n$ chaotic logistic maps are generated from K according to the following relationship:

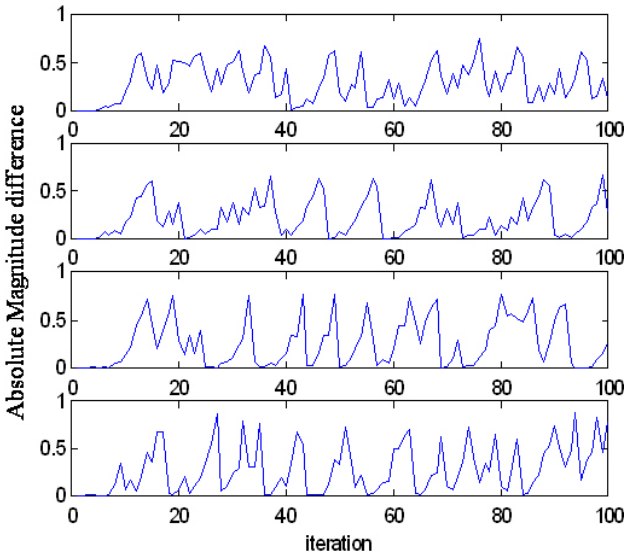

FIGURE 1. Absolute magnitude difference between four independent logistic map trajectories and their corresponding coupled map trajectories.

$$
\begin{aligned}
X_{i,0} &= K(2i-1), \\
\lambda_i &= 3.73364 + \frac{\left[\dfrac{K(2i)}{2^{B/2N}} + \dfrac{K(2i)}{10^{h_{2N}}} + \dfrac{a \oplus b}{2^{B/4N}}\right]}{10} \\
&\quad \times \frac{0.26506}{MAX}, \\
i &\in \{1, 2, ..., N/2\},
\end{aligned} \tag{1}
$$

where $X_{i,0}$ and λ_i are thei^{th} map initial variable and parameter respectively, with $0.2 \leq X_{i,0} \leq 0.8$ (except $X_{i,0} \approx 0.5$) and $3.73364 \leq \lambda_i \leq 3.9987$, h_{2N} is the number of digits in the largest decimal number represented by $2N$ bits, $a \oplus b$ term is the eXclusive-OR (XOR) of the most and least significant bits of $K(2i)$ respectively, having both equal size bit representation of $B/4N$, and MAX is the maximum value of $[K(2i)/2^{B/2N} + K(2i)/10^{h_{2N}} + a \oplus b/2^{B/4N}]/10$. To increase the sensitivity of the system to bit changes in K, $X_{i,0}$'s and K are de-correlated by iterating $X_{i,0}$ an *RT* random number of times over all coupled logistic maps as follows:

$$
\begin{aligned}
X_{i,j} &= (1-\varepsilon) f(X_{i,j-1}) + \varepsilon H(X_{1,j-1}, ..., X_{N,j-1}), \\
f(X_{i,j-1}) &= \lambda X_{i,j-1}(1 - X_{i,j-1}) \\
H(X_{1,j-1}, ..., X_{N,j-1}) &= \sum_{i=1}^{N} w_i X_{i,j-1},
\end{aligned} \tag{2}
$$

where j is the current map state iteration, $f(X_{i,j-1})$ is the logistic map, ε is the coupling parameter, and H is the coupling function with weights w_i, where

$$\sum_{i=1}^{N} w_i = 1.$$

H takes the weighted average of previous iteration map variables over all maps. Equation (2) guarantees that a one-bit change in K, will affect all maps variables and therefore the system's output (cyphertext). The output of Eq. (2) after *RT* iterations becomes the initial state for each map in the encryption process, that is $X_{i,0}, 1 \leq i \leq N$. The same process can be performed on the map parameters if needed (λ and X). Figure 1 shows the absolute magnitude difference between four original chaotic maps and their respective coupled chaotic maps trajectories. Modifying only one parameter (ε) affects the whole system (every single map trajectory) rather than only one map as in Ref. 1.

2.2. Cipher scheme

The N coupled map array is used as an N circular list of ciphers, but only a subset defined by a cipher window $W_{m,k} = ((i-1) mod N) + 1\{|k \leq i \leq k+m-1\}$, for $m \leq N$, and $k \in \{1, 2, \ldots, N\}$ is used in the encryption process at a time as shown in Fig. 2. k represents the minimum index of $W_{m,k}$ at a given time and m is the size of

the window. For a fixed state j, the m ciphers in $W_{m,k}$ are defined by the following equation [1]:

$$\begin{aligned} C_{i,l} &= ([P_l + X'_{i,j}] \bmod 2^n) \oplus X'_{i,j} \\ &\oplus ([X'_{i+1,j} + X'_{i+2,j}] \bmod 2^n) \\ &\oplus ([C_{i-1,l} + C_{i,j-1}] \bmod 2^n), \\ &i \in W_{m,k}, l = (mj + i - 1), \end{aligned} \tag{3}$$

where P_l is the l^{th} plaintext input, $X'_{i,j}$ is the corresponding integer representation of $X_{i,j}$ using $n = B/N$ bits, $C_{i-1,l}$ is the $i-1$ cyphertext in current iteration *l=mj+i-1*, and $C_{i,l-1}$ is the previous cyphertext output of the same i^{th} map, but from the $j-1$ iteration. $C_{i-1,l}$ and $C_{i,j-1}$ represent the global and local feedback respectively. The initial spatiotemporal feedback for a new map window $C_{k-1,j}$ is the last cyphertext output of the previous window iteration. A total of *mn* bits are encrypted per iteration state j (n encrypted bits per map). $W_{m,k}$ is periodically rotated one map at a time by setting $k = k + 1$; when *(N-k)* $\leq$ *m*, the cipher index wraps around taking the corresponding first, second, up to the $m-1$ initial maps (when $k = N$ the current cipher window is $W_m = \{N, 1, 2, \ldots, m-1\}$).

To increase the encryption system security, cyphertext output $C_{i.l}$ is masked using two map variables:

$$C^M_{i,l} = (C_{i,l} + X'_T) \bmod 2^n, \quad X'_T = X'_{i,j} \oplus X'_{i-1,j} \tag{4}$$

Therefore, the decipher cannot use $C^M_{i,l}$ directly to find its corresponding plaintext data; it needs to know X'_T.

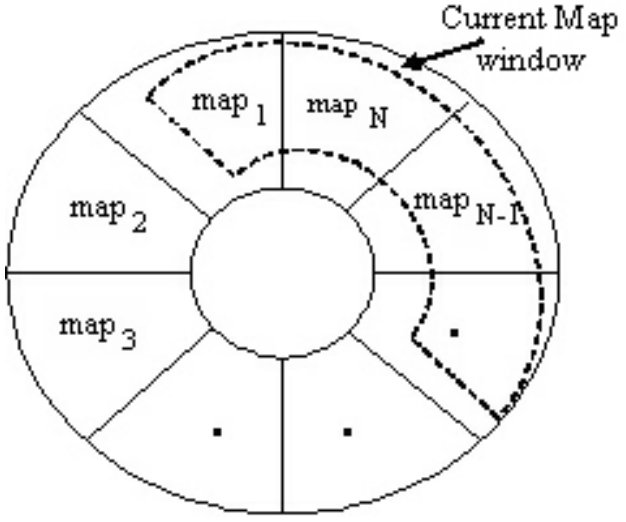

FIGURE 2. Array of N chaotic maps viewed as a circular list. Current map window represents the active maps in the encryption process.

The corresponding decryption system can be written as:

$$\begin{aligned} C_{i,l} &= (C^M_{i,l} + 2^n - X'_T) \bmod 2^n; \\ P_l &= [C_{i,l} \oplus X'_{i,j} \oplus ([C_{i-1,l} + C_{i,l-1}] \bmod 2^{B/N}) \\ &\oplus ([X'_{i,j+1} + X_{i,j+2}] \bmod 2^{B/N}) \\ &+ 2^{B/N} - X'_{i,j}] \bmod 2^{B/N}, \\ &i \in W_{m,k}, l = (mj + i - 1) \end{aligned} \tag{5}$$

where P_l represent the plaintext.

2.3. Three-level perturbation scheme

The three perturbation levels proposed in Ref. 1 are maintained in the generalized scheme with some modifications. Originally, the first perturbation level modifies the local trajectory in order to increase its cycle length; the second perturbation creates a new system trajectory by modifying the system variable; and for the third perturbation level, the system-key value is renewed using [13]. The third perturbation represents a reset operation, since the entire encryption/decryption system parameters are completely modified (system-key, map variable and parameter). Since we are now using coupled chaotic maps, our first perturbation level modifies the coupling parameter ε using the global feedback (spatiotemporal feedback) affecting the entire system at once (first perturbation level in Ref. 1 affects local maps only). The first-level perturbation for the i^{th} logistic map is expressed as:

$$\varepsilon_l = \frac{\sum_{n_1=1}^{n/8} C_{i-1,l}(n_1)}{10^{h_8}} \qquad i \in W_{m,k}, \tag{6}$$

where $C_{i-1,l}(n_1)$ is the n_1^{th} byte of the global feedback in the state l and h_8 is the number of digits in the largest decimal number represented by $B/8$. The coupling parameter is set to take 2^{10} distinct values in the interval $0 \leq \varepsilon \leq 0.1024$. In the case of a differential attack, Eq. 6 exacerbates every single plaintext change by disturbing not only future cyphertext outputs through global and local feedback, but also the coupled chaotic system in the current cipher window. The combined effects (feedback and perturbation) generate totally different trajectories for any pair of plaintexts when iterated by the system. The second-level perturbation adds $C_{i,l-1}$ to each map variable and cross-iterates the outcome through all maps, and the third level perturbation replaces current system-key using [13] every random number of iterations [see Eq. (2)].

The period of the perturbations represented by $PT_l, 1 \leq l \leq 3$ can be randomly selected to increase the system-key space in the case of brute force attack (the opponent tries every possible system-key combination until the right one is found). We define the perturbation cycles as follows: PT_1 = *[(a_random_number) modulus 10] + 15*, $PT_2 = n_1 \, .PT_1$, and $PT_3 = n_2 \, .PT_2$, for n_1 and n_2 positive integers greater than one. The value of PT_1 is related to the

sensitivity of the coupled logistic map to a magnitude change of $1/2^{10}$ in the coupling parameter.

3. Security analysis and experimental results

Our proposed scheme has been applied to the same audio (.wav) and video (.mov) data presented in Ref. 1 with respective sizes of 91Kb and 16Mb. For the experiment we use the following setting: $B = 384$ bits, $n = 32$, generating a *12-map* array of coupled logistic maps ($N = 384/32$), initial feedback (global and local) is selected randomly using RANROT, $0 < \varepsilon \leq 0.1024$ (small values for dominant local behavior), $w_1 = w_2 = \ldots = w_N = 1/12$, *RT = 20*, $PT_1 = 35$ iterations, $PT_2 = n_1$ .PT_1, and *PT3*= n_2.PT_2, for $n_1 = n_2$ = 3 (RT, n_1,$n_2$variables could have also been computed randomly to increase system space search).

3.1. Security analysis

We shall question the security of our scheme considering the sensitivity of the system to key changes, sensitivity to plaintext changes, and statistical independency. Figure 3 shows the histograms of plaintext and corresponding cyphertext of data files. For each plaintext we use two randomly chosen keys in order to prove statistical independence from the scheme. In both cases, the cyphertext histogram is uniform and independent of the plaintext histogram and system-key. on the average, 99.5% of the total bytes and 50% of the total bits were changed during the encryption process, providing the best protection against attacks. The scheme response to a slight change in the system-key (flipping the least significant bit) is shown in Fig. 4. Because of the coupled chaotic decorrelation process between the system-key and maps variables and parameters [Eq. (2)], the cyphertext output diverges right from the first iteration.

Let us now analyze the effect of the difference (the least significant bit) of a pair of plaintexts on the cyphertext output sequence without perturbation (this is known as differential attack). Figure 5 shows that the scheme using only global and local feedback scheme needs approximately 22 iterations for the sequences to diverge chaotically. Applying our perturbation scheme (first and second perturbations) from iteration 5, the sequences take different trajectories, immediately influencing future cyphertext output values (Fig. 6). Since perturbation modifies map variables and coupling parameters, the rest of the cipher trajectory is completely different from the unperturbed case.

If the opponent chooses the brute force attack, he will need to search for at least 2^B key possibilities in our current setting, where B can be any multiple of 16 and 32 bits. In addition, there are five more random numbers with a 5-bit representation each, *RT*, P_1, P_2, P_3 and $w_i, 1 \leq i \leq m$, two more with a *7-bit* representation N (number of maps) and m

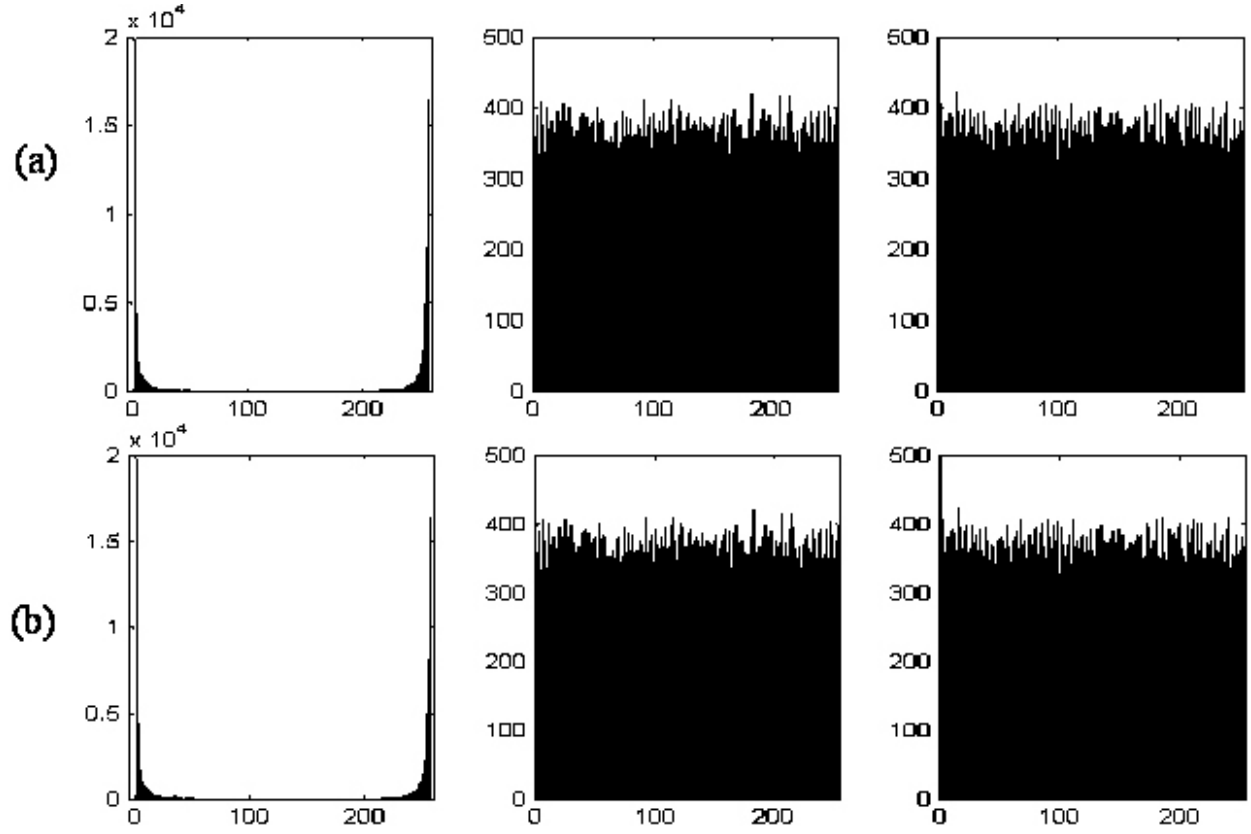

FIGURE 3. Histogram of plaintext (left column) and corresponding cyphertext for two different system-keys (center and right columns). Plaintext corresponds to audio (a) and movie (b) data.

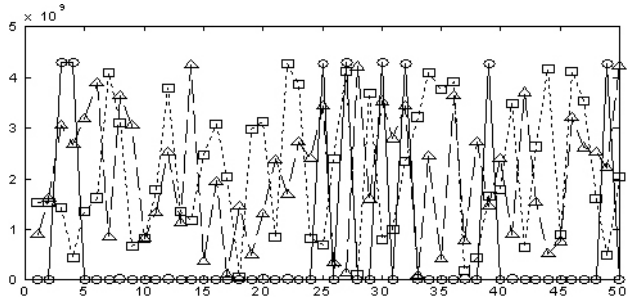

FIGURE 4. Sensitivity to system-key changes. Plaintext (circled continuous line) encrypted with two slightly different system-keys (least significant bit changed).

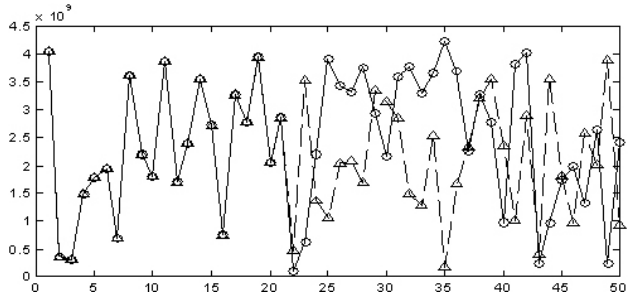

FIGURE 5. Sensitivity to plaintext changes without perturbation scheme. Cyphertexts of a pair of chosen plaintexts with the least significant bit changed.

(size of the $W_{m,k}$), and the coupling parameter with a *10-bit* representation. Considering the minimum bit representation of $B = 128$, a brute force attack will need a total space analysis of $(2^{128}).(2^{20}).(2^{25})(2^{7})(2^{7})(2^{10})$ = 5.9×10^{59}, much higher than [1].

Finally, a C-language implementation of the cryptosystem on a 940 Mhz Pentium®-III, with 190 Mb of memory

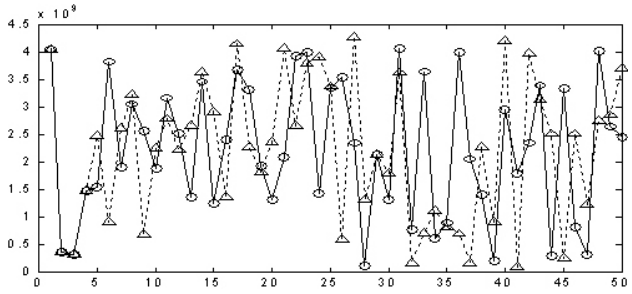

FIGURE 6. Same as in Fig.5 with initial perturbation at 5th cipher iteration (vertical dotted line).

under Red Hat Linux operating system version 2.4.20-28.9, shows an average speed of 170Mbs and 258Mbs using non-optimized and optimized compilation respectively. A 3 Ghz Pentium®-IV with 1 Gb of memory using the same operating system shows an average of 540 Mbs and 1088 Mbs using non-optimized and optimized compilation respectively. This is not as fast as Ref. 1 because of the additional complexity, but still higher than any other scheme reported in the literature and fast enough to support real-time multimedia communications.

4. Conclusions

We have proposed a generalized and robust symmetric block-cipher cryptosystem based on an *N-array* of coupled chaotic logistic maps taking an *m-map* window size for the encryption process. Both the coupling parameter and map chaotic map parameters are perturbed in order to increase the scheme sensitivity to initial conditions. A software implementation of the system shows excellent statistical properties and good performance in fulfilling current multimedia application demands, such as real-time audio and video communications.

1. R. Hasimoto-Beltrán, *Rev. Mex. Fís.* **53** (2007) 58.
2. G. Chen, Y. Mao, and C.K. Chui, *Chaos Solit. & Fract.* **21** (2004) 749.
3. M. Yang, N. Bourbakis, and S. Li, *IEEE Potentials* **23** (2004) 28.
4. R. Matthews, *Cryptology* **13** (1989) 29.
5. G. Álvarez, F. Montoya, G. Pastor, and M. Romera, *Proc. IEEE Int. Carnahan Conf. Security Technology* (1998) 332.
6. G. Jakimoski and L. Kocarev, *IEEE Trans. Circ. Syst.-I* **48** (2001) 163.
7. M.S. Baptista, *Physics Letters A* **240** (1998) 50.
8. S. Li, M. Xuanqin, and C. Yuanlong, *Lecture Notes in Computer Science* **2247** (2001) 316.
9. Y. Dobyns and H. Atmanspacher, *Chaos Solitons & Fractals* **24** (2005) 313.
10. M. Dellnitz, M. Field, M. Golubitsky, A. Hohmann, and J. Ma, *IEEE Trans. Circ. Sys.-I* **42** (1995) 821.
11. A. Palacios and H. Juárez, *Physics Letters A* **303** (2002) 345.
12. X. Wang, M. Zhan, X. Gong, and C.H. Lai (2005) Construction of a secure cryptosystem based on spatiotemporal chaos and its applications in public channel cryptography, http://arxiv.org/abs/nlin/0502026
13. Fog A. Chaotic random number generators with random cycle lengths. http://www.agner.org/random/theory/chaosran.pdf.