High-performance multimedia encryption system based on chaos

Rogelio Hasimoto-Beltrán
Center for Research in Mathematics (CIMAT), Jalisco s/n, Col. Mineral de Valenciana, Guanajuato, Gto, Mexico 36240

(Received 6 June 2007; accepted 10 March 2008; published online 29 April 2008)

Current chaotic encryption systems in the literature do not fulfill security and performance demands for real-time multimedia communications. To satisfy these demands, we propose a generalized symmetric cryptosystem based on N independently iterated chaotic maps (N-map array) periodically perturbed with a three-level perturbation scheme and a double feedback (global and local) to increase the system's robustness to attacks. The first- and second-level perturbations make cryptosystem extremely sensitive to changes in the plaintext data since the system's output itself (ciphertext global feedback) is used in the perturbation process. Third-level perturbation is a system reset, in which the system-key and chaotic maps are replaced for totally new values. An analysis of the proposed scheme regarding its vulnerability to attacks, statistical properties, and implementation performance is presented. To the best of our knowledge we provide a secure cryptosystem with one of the highest levels of performance for real-time multimedia communications. © *2008 American Institute of Physics*. [DOI: 10.1063/1.2903758]

A digital chaotic encryption system consists of a digital chaotic system (nonlinear dynamic equation or map), which takes an input message known as plaintext and produces an independent masked output message known as ciphertext. Digital chaotic systems have many of the good properties required in cryptography; the most prominent are sensitivity to parameters, sensitivity to initial conditions and unpredictable trajectories. The first two properties are related to diffusion, and the last one to confusion in the cryptographic nomenclature. Confusion is intended to make the relationship between ciphertext and plaintext statistically independent, while diffusion is intended to spread out the influence of a single plaintext digit over many ciphertext digits to hide the statistical structure of the plaintext. General purpose (data or compression independent) chaotic encryption schemes iterate a single one-dimensional chaotic map; in this work we propose a generalized encryption system based on N one-dimensional coupled (interdependent) chaotic maps along with three levels of perturbation (in order to change the trajectory of the chaotic system) that increase significantly the system security with respect to previous schemes. Additionally, our system software implementation is fast enough to deal with current multimedia communication demands (real-time audio and video transmission).

I. 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 user right of privacy. Building secure multimedia communications demands new challenges difficult to handle by currently adopted encryption schemes (DES, RSA, AES, and IDEA).[1,2] It requires the processing of huge amounts of information at speeds going from kilobits/sec (Kbs) to the order of megabits/sec (Mbs); in particular those applications involving real-time audio and video transmission.

Digital chaotic dynamical systems (DCS) have been proposed in the late 1980s 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] The first two properties are related to diffusion, and the last one to confusion in the cryptographic nomenclature.[7] Even though a lot of research has been published in the literature, some schemes are weak or have already been broken.[8–19] DCS are still in search to position as a strong competitor to current standard cryptosystems regarding to security.

Contrary to its continuous counterpart where the cycling length (number of states) can be infinite, digital chaotic encryption systems are represented by a finite-state machine with 2^L states (chaotic degradation), where L is the bit precision of the machine. This means that DCS are short cycled, with largest theoretical cycle length $\mathrm{CL}=2^L$.[20] In practice, $\mathrm{CL}\ll 2^L$ for almost every chaotic trajectory,[21] with a maximal length of $O(2^{\varepsilon L})$, where $0<\varepsilon<1$. Along with the cycle-length reduction, a DCS may experience a degraded distribution and correlation, and a reduced control parameter interval, making the system vulnerable to attacks. Current research focuses on improving the security of chaotic cryptosystems by two main approaches: perturbance-based schemes (to increase the chaotic cycle length) and network-based chaotic maps (to increase the number of parameters in

the system). Perturbation-based schemes transform stable chaotic cycles into nonstable ones by perturbing its trajectory. Sang *et al.*[23] proved that periodic perturbations increase the cycle length of chaotic systems by $\sigma\Delta(2^L-1)\gg 2^L$, where σ is a positive integer and Δ is the perturbation period. They obtained a lower bound of $\Delta(2^L-1)\gg 2^L$, which improves considerably the maximum cycle length with respect to the unperturbed case ($O(2^{\varepsilon L})$). Ideally, perturbation magnitudes should be obtained by a uniform pseudorandom number generator (PRNG) to improve the dynamical properties of digital chaotic systems.[20,22,23] Network of chaotic maps or coupled map lattices (CMLs) consider an array of chaotic maps governed by a coupling transformation over some defined neighborhood in the array.[24] 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[25] found that, when an individual map is active (having chaotic behavior) the rest of the system elements remains quiescent. This process is repeated forever for each element of the system. Palacios and Juárez[26] applied cycling chaos theory to improve Baptista's encryption scheme security.[10] Wang *et al.*[27] combined a CML with bit-reverse operation applicable to symmetric cryptosystem and pseudorandom number generators.

In order to change the system dynamics more effectively under a drastic chaotic degradation or an attack, we propose a novel block-based symmetric-key encryption system based on multiple chaotic maps. Multiple chaotic maps and higher dimensional chaotic maps are considered as the future trend for secure chaotic encryption systems.[1,31,33] Our method considers an N-array of chaotic maps with an intermittent three-level perturbation scheme. In our system (contrary to CML) every single map is independently iterated and perturbed to encrypt a portion of the input data. Interdependency is created by adding a global and local feedback during the encryption process, so that the new ciphertext depends on the history of previous ciphertext values in the current iteration (global feedback) and the history of previous ciphertext values in the same map (local feedback). We additionally propagate this interdependency into the array of chaotic maps by perturbing each element with the most recent global ciphertext output rather than with a predefined data-independent distribution function.[27] This represents the first level of the hierarchical perturbation. The second-level perturbation is more drastic in the sense that it completely changes the system map variables (not the map parameters). These two perturbations are necessary to immediately change the dynamics of the system when it becomes trapped in a fixed point or short length periodic window. Third-level perturbation, on the other hand, represents a whole system perturbation, where the original system-key is updated and postprocessed using a CML system. Our goal is to develop a fast, simple, and secure encryption system independent of the compression scheme for current real-time multimedia demands.

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

II. CHAOTIC ENCRYPTION SCHEME

An important step in any digital chaotic encryption is the selection of the map. Chaotic maps have different behavior regarding complexity, chaotic properties (cycle length, chaotic interval, periodic windows, etc.), sensitivity to initial conditions and reaction to trajectory perturbations, etc., that influence the structure or behavior of the chaotic encryption system. In fact, some systems have been broken for not considering the weaknesses of the chosen chaotic map (see Refs. 21 and 32). As a complement to our main goals discussed in Sec. I (security and efficiency), it is desirable to provide some independency between the cryptosystem and the chaotic map under consideration. This independency means that, a full knowledge of the selected chaotic map is not needed to fulfill the security and efficiency requirements of a good cryptosystem.

For their mathematical simplicity there are two options: logistic map and tent map. The logistic map is represented by

$$X_n=\lambda X_{n-1}(1-X_{n-1}),\quad \lambda\in[1,4],\quad X\in[0,1]. \tag{1}$$

It involves a single variable (X) and a single control parameter (λ) representing two multiplications and one addition per iteration. This simplicity has several disadvantages:

(a) Reduced chaotic interval: As λ increases from 1 to 4, the map experiences a period doubling to chaos. In particular for $\lambda\geqslant 3.5699$ (known as accumulation point) it presents a chaotic behavior, however there are many periodic windows (with all kinds of periods) that appear abruptly. A very well-known and prominent period-3 window appears at $\lambda=1+\sqrt{8}=3.8284$. Fixed points ($f(X)=X$) are also present at $X=0$ and $X=(\lambda-1)/\lambda$, which define a regular pattern in the logistic map.[24]

(b) Digital chaotic degradation: It affects all computerized chaotic maps by reducing their cycle lengths.

The tent map (also called piecewise linear) represented by $X_n=\lambda\min(X_{n-1},1-X_{n-1})$, has better chaotic behavior than the logistic map. It has only one fixed point at $X=0$ for $\lambda<1$, and chaotic behavior for nearly all values of X with $1<\lambda<2$, without periodic windows. The tent map is of course affected by the digital degradation as well, which includes a reduced chaotic interval, short-cycle length, degraded distribution and correlation.[21] Despite of the tent map advantages, our selection for this work is the logistic map because of its challenging chaotic properties for a secure cryptosystem (fixed points, periodic windows, degraded distribution, etc.). Our scheme should be robust enough to deal with logistic map digital degradations.

To overcome the reduced chaotic interval, the digital degradation, and to increase the security of the cryptosystem we propose an N-array of logistic maps along with a pertur-

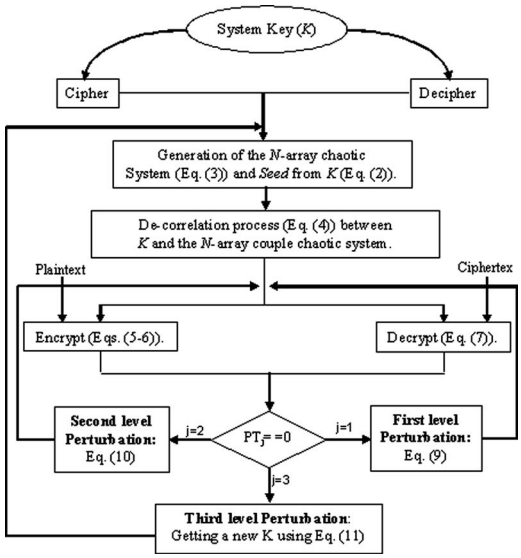

FIG. 1. Flow diagram of the encryption/decryption system scheme.

bation and feedback scheme to drive every cycling chaotic signal away from its original trajectory. Our aim is to develop a cryptosystem with the following properties: (a) sensitive to initial conditions (system-key and plaintext); (b) robust to opponents attack; and (c) fast software implementation for real-time multimedia communications. The overall system is described as follows (Fig. 1).

A. Chaotic system generation

The proposed scheme is symmetric, therefore the initial system-key (K) of size B bits, for $B \geqslant 128$ and multiple of

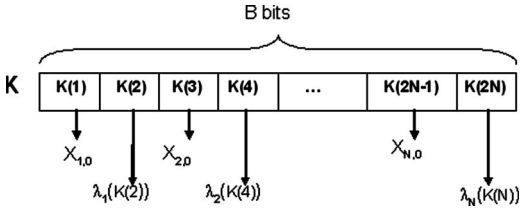

FIG. 2. System-key (K) partition ($n/2$) for the creation of maps variables ($X_{i,0}$) and corresponding parameters (λ_i).

$n=32$ (bits to cipher per chaotic map) is shared between cipher and decipher. Any suitable key establishment/distribution protocol (public-key or authenticated protocol) in the literature can be used for the key exchange, the only restriction is that every session requires a new and independent system-key.

The encryption system uses K to compute the array of chaotic maps and a system Seed for a pseudo-random number generator (PRNG). A PRNG is used to generate all random variables supporting the N-map system, such as current number of active maps, initial global and local feedbacks, and system perturbation frequencies. Any good PRNG can be used in the scheme.

The value of Seed is calculated as follows:

$$\text{Seed} = K_n(1) \oplus \cdots \oplus K_n(B/n), \tag{2}$$

where $K_n(i)$ is the ith n-bit element of K (considered as an array of B/n elements) and $\oplus$ is the exclusive-OR (XOR) operator. n can also be 64 bits if 64-bit arithmetic is available (this is why we use n instead of directly using 32).

The N-array of chaotic maps for $N=B/n$ is defined as (see Fig. 2)

$$X_{i,0} = K_{n/2}(2i-1)/2^{n/2},$$
$$\lambda_i = 3.68 + \frac{[K_{n/2}(2i)/2^{n/2} + K_{n/2}(2i)/10^{h_{n/2}} + (a \oplus b)/2^{n/4}]}{10} \frac{[0.3187]}{\text{MAX}}, \quad i = 1,2,\ldots,N, \tag{3}$$

where $X_{i,0}$ and λ_i are the ith map initial variable and parameter respectively, with $0.2 \leqslant X_{i,0} \leqslant 0.8$ (except $X_{i,0} \approx 0.5$) and $3.68 \leqslant \lambda_i \leqslant 3.9987$ for $\lambda_i \neq \lambda_j$ and $i \neq j$, $h_{n/2}$ is the number of digits in the largest decimal number represented by $n/2$ bits, $a \oplus b$ term is the XOR between the half-most and half-least significant bits of $K_{n/2}(2i)$, respectively, yielding an $n/4$-bit outcome, and MAX is the maximum value of $[K_{n/2}(2i)/2^{n/2} + K_{n/2}(2i)/10^{h_{n/2}} + (a \oplus b)/2^{n/4}]/10$, which happens to be when $K(2i)=2^{n/2}-1$. The valid interval for λ is set between the merge point of the two main bifurcation bands found in the interval $3.0 < \lambda < 3.68$ and (strictly speaking) the highest real number less than 4.0 represented by the precision of the corresponding machine (we selected 3.9987 as the upper limit). To increase the sensitivity of the system to a magnitude change in the system-key, $X_{i,0}$ is iterated an $RT=\text{PRNG(Seed)}$ random number of times over the couple chaotic system:

$$X_{i,j} = (1-\varepsilon)[\lambda_i X_{i,j-1}(1-X_{i,j-1})] + \varepsilon H(X_{1,j-1},\ldots,X_{N,j-1}),$$
$$H(X_{1,j-1},\ldots,X_{N,j-1}) = \frac{1}{N}\sum_{i=1}^{N} X_{i,j-1}, \tag{4}$$

where j is the current map state iteration and H is the coupling function with coupling parameter ε. H takes the average of previous iteration map variables over all maps. Equation (4) guarantees that a one-bit change in K, will affect all maps variables and therefore the system's output (ciphertext). The output of Eq. (4) after RT iterations becomes the initial state for each map in the encryption process; that is,

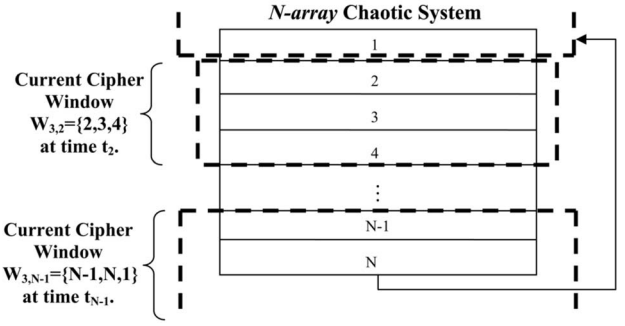

FIG. 3. Representation of the N-array chaotic system and active encryption window ($W_{m,k}$) at different periods of times.

$X_{i,0}$, $1 \leqslant i \leqslant N$. The same process can be performed for the corresponding map parameters if needed.

B. Cipher/decipher scheme

The N-map array is used as an N circular list of ciphers, but only a subset defined by a cipher window $W_{m,k}=\{((i-1)\bmod N)+1 \,|\, k \leqslant i \leqslant k+m-1\}$, for $m=[\mathrm{PRNG(Seed)}\bmod N]+4$ and $k \in \{1,2,\ldots,N\}$ is considered in the encryption process at a time (Fig. 3). k represents the minimum index of $W_{m,k}$ at a given time and $1 \leqslant m \leqslant N$ is the size of the window. For simplicity, the elements of $W_{m,k}$ are renamed by $W(i)$, for $1 \leqslant i \leqslant m$ and some N. $W(i)$ represents the ith element of $W_{m,k}$; i.e., if $W_{3,5}=\{5,1,2\}$ and $N=5$, then $W(1)=5$, $W(2)=1$, $W(3)=2$.

Let j and l represent the system state (iteration) and plaintext-ciphertext absolute indexes, respectively ($l=(j-1)m+i$). For a fixed state j, the m ciphers in $W_{m,k}$ are defined by the following equation:

$$\begin{aligned} C_l &= C_{W(i),j} \\ &= ([P_l + X'_{W(i),j}]\bmod 2^n) \oplus X'_{W(i),j} \\ &\quad \oplus ([X'_{W((i+1)\bmod m),j} + X'_{W((i+2)\bmod m),j}]\bmod 2^n) \\ &\quad \oplus ([C_{W(i-1),j} + C_{W(i),j-1}]\bmod 2^n), \\ 1 &\leqslant i \leqslant m, \quad l=(j-1)m+i, \end{aligned} \tag{5}$$

where P_l is the lth plaintext input, $X'_{W(i),j}$ is the corresponding integer representation of $X_{W(i),j}$ using n bits, $C_{W(i-1),j}$ ($=C_{l-1}$) is the previous ciphertext output $(i-1)$ in current iteration (jth), and $C_{W(i),j-1}$ is the previous ciphertext output of the same ith map, but from the $j-1$ iteration. $C_{W(i-1),j}$ and $C_{W(i),j-1}$ represent the global and local feedback, respectively. The initial global feedback $C_{W(i-1),j}$ for the jth iteration takes in the last ciphertext output of the previous iteration ($C_{W(m),j-1}$) to spread the system changes on to future ciphertexts and current m logistic map variables (see next subsection). 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 $k=k+1$ (see Fig. 3); when $(N-k+1)<m$, the cipher index wraps around taking the corresponding first, second, up to the $m-(N-k+1)$ initial maps (when $k=N$ the current cipher window is $W_{m,N}=\{N,1,2,\ldots,m-1\}$).

To increase the encryption system security, and as an optional step, the ciphertext output $C_l=C_{W(i),j}$ can be masked using two maps' variables:

$$C_l^M = (C_l + X'_T)\bmod 2^n, \quad X'_T = X'_{W(i),j} \oplus X'_{W((i+1)\bmod m),j}. \tag{6}$$

Therefore, the decipher cannot use C_l^M directly to find its corresponding plaintext data; it needs to know X'_T.

The corresponding decryption system can be written as

$$\begin{aligned} C_l &= (C_l^M - X'_T)\bmod 2^n, \\ P_l &= [C_l \oplus X'_{W(i),j} \oplus ([C_{W(i-1),j} + C_{W(i),j-1}]\bmod 2^n) \\ &\quad \oplus ([X'_{W((i+1)\bmod m),j} + X_{W((i+2)\bmod m),j}]\bmod 2^n) \\ &\quad - X'_{W(i),j}]\bmod 2^n, \\ 1 &\leqslant i \leqslant m, \quad l=(j-1)m+i. \end{aligned} \tag{7}$$

Initial global and local feedbacks are calculated by

$$\begin{aligned} &\mathrm{global} = C_{0,0} = \mathrm{PRNG(Seed)}; \\ &\text{for } i=1,\ldots,N, \\ &\quad \mathrm{local}_i = C_{i,0} = \mathrm{PRNG(Seed)}. \end{aligned} \tag{8}$$

C. Three-level perturbation scheme

Under external perturbations (plaintext or system-key attacks), the global feedback in Eq. (5) will drive the original system trajectory into a different chaotic state. There are two problems though, the transition change is slow and the chaotic system (N-array) does not participate in the trajectory change (chaotic parameters and variables stay unchanged). In order to speed up the system reaction time under external perturbations, a three-level periodic perturbation scheme is proposed. The first two perturbation levels are related to the system variables and the third one is related to the system-key. In the first perturbation level, the trajectory of every map is slightly modified to increase its cycle length;[22,23] in the second perturbation level the current system variable is randomly changed, creating a totally new trajectory for the system; and, in the third perturbation level the system-key value is renewed using current system map variables. Third-level perturbation represents a reset operation, since the entire encryption/decryption system parameters are completely modified.

The first-level perturbation for the ith logistic map is expressed as

$$\mathrm{XP}_{W(i),j-1} = X_{W(i),j-1} + \frac{\sum_{l=1}^{n/8} C_{W(m),j-1}(l)}{10^{h_8}}, \quad 1 \leqslant i \leqslant m, \tag{9}$$

where $C_{W(m),j-1}(l)$ is the lth byte of the global feedback at the state $j-1$, and h_8 is the number of digits in the largest decimal number represented by 8 bits. We postprocess $\mathrm{XP}_{W(i),j-1}$ so that its first digit after the decimal point remains the same as in $X_{W(i),j-1}$; therefore, $\mathrm{abs}(\mathrm{XP}_{W(i),j-1}-X_{W(i),j-1}) < 10^{-1}$ (the

perturbation signal must be smaller than the chaotic signal to keep the good statistical properties of chaos dynamics). Note that every single change detected by the global feedback is passed on to the array of chaotic maps. In the case of a differential attack, Eq. (9) exacerbates every single plaintext change by disturbing not only future ciphertext outputs through global and local feedback, but also the map variables in the current cipher window. The combined effects (feedback and perturbation) generate different trajectories for any pair of plaintexts when iterated by the system. An additional benefit of involving $C_{W(m),j}$ in the perturbation process, is that in the long run it has uniform distribution (see Sec. III), an important requirement for perturbation schemes.[23]

Only one chaotic map may be enough if the chaotic signal reaction to Eq. (9) were instantaneous. Unfortunately, it takes a certain number of iterations (depending on the perturbation magnitude) for a chaotic map to diverge from its original signal trajectory. This reaction time may be dangerous under a differential or plaintext attack if only one map is used in the encryption process (attacker may find out current map's parameters). To avoid this problem in one-dimensional chaotic encryption systems, Pareek *et al.*[6] iterated the logistic map a random number of times. This solution affected considerably the system execution time and did not solve the security problem since the scheme was broken by Ref. 32. The use of m different chaotic maps producing m ciphertext values increases the number of variables to solve for the attacker during the reaction time without affecting the system's performance. Since we are not considering all possible chaotic flaws in the logistic map, in the low probable case where the first-level perturbation magnitude is very small for the entire m-array of chaotic maps (increasing the chaotic reaction time) or when the m-array is in a short cycle state, then a second-level perturbation comes in to play to complicate things up for the attacker by resetting the system map variables. This is the same as resetting the maps' variables maintaining the same parameters.

The second-level perturbation adds $C_{W(m),j-1}$ to each map variable and cross-iterate the outcome throughout the maps. For the $W(i)^{\text{th}}$ map in state $j-1$, the new perturbed system variable $\text{XP}_{W(i),j-1}$ is obtained by

$$\begin{aligned}
&\text{For } i = 1,m,\\
&\quad \gamma = (C_{W(m),k} + X_{W(i),j-1}) - \text{floor}(C_{W(m),k} + X_{W(i),j-1}),\\
&\quad \text{For } l = 1,m, \qquad (10)\\
&\quad\quad \gamma = \gamma\lambda_{W(l)}(1-\gamma),\\
&\quad \text{XP}_{W(i),j-1} = \gamma.
\end{aligned}$$

That is, new system variables are influenced by all maps in $W_{m,k}$ and their corresponding local feedback. For the next iteration, $X_{W(i),j-1} = \text{XP}_{W(i),j-1}$.

Since we are working with very long multimedia sequences (from minutes to hours) and not checking for either bad chaotic points (periodic window, fixed points, etc.) or perturbation frequency values, the system may face low chaotic variation due to the low perturbation frequencies and/or small perturbation magnitudes in the first and second perturbation levels. To avoid this kind of vulnerability, the third-level perturbation enters in action by replacing the system-key using current map variables:

$$K = K \oplus \text{concatenate}[X'_{1,j,\ldots,}X'_{N,j}]. \qquad (11)$$

Immediately, the system (under a differential attack) turns into a chaotic behavior and the system becomes protected. By using current map variables in the new K, it is assured that any single change in the past be spread out into future ciphertext generations. The new system-key goes through the same process as in the original one [see Eq. (2)], including chaotic parameter and variable restrictions.

The perturbation cycles represented by PT_l, $1 \leqslant l \leqslant 3$, are selected randomly 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: $\text{PT}_1 = [\text{PRNG(Seed)mod } 10] + 15$, $\text{PT}_2 = n_1\text{PT}_1$, and $\text{PT}_3 = n_2\text{PT}_2$, for $n_1 = [\text{PRNG(Seed)mod } 64] + 2$ and $n_2 = [\text{PRNG(Seed)mod } 128] + 3$. Less frequent perturbations have greater impact on the system's parameters. The value of PT_1 is related to the sensitivity of the logistic map to a magnitude change of $1/2^8$ in the initial condition. For $B = 128$ bits, the minimum magnitude change of two system variables is $\sim 10^{-3}$, which requires about 10–15 map iterations for their trajectories to diverge chaotically.[6] This result is important for the cipher in order to produce different trajectories when input values differ in the least significant bits.

III. SECURITY ANALYSIS AND EXPERIMENTAL RESULTS

Our proposed scheme has been applied to audio and video files (Table I) with different statistical properties (see original histograms in Fig. 4). For the experiment we use the following setting; $B = 384$ bits, $n = 32$, generating a 12-map array of logistic maps ($N = 384/32$), initial feedback (global and local) is selected randomly, $\text{RT} = 20$, $\text{PT}_1 = 25$ iterations, $\text{PT}_2 = n_1\text{PT}_1$, and $\text{PT}_3 = n_2\text{PT}_2$, for $n_1 = n_2 = 3$. All random numbers involved in the scheme are computed using the PRNG in Ref. 28.

A. Security analysis

As previously mentioned, a good cryptosystem must have the following properties:[29–31]

TABLE I. Sample files used in the encryption process

File type	Size (Kbytes)
Audio (.wav)	91.8
Movie (pres-clinton-final-days.mov)	16 281.6

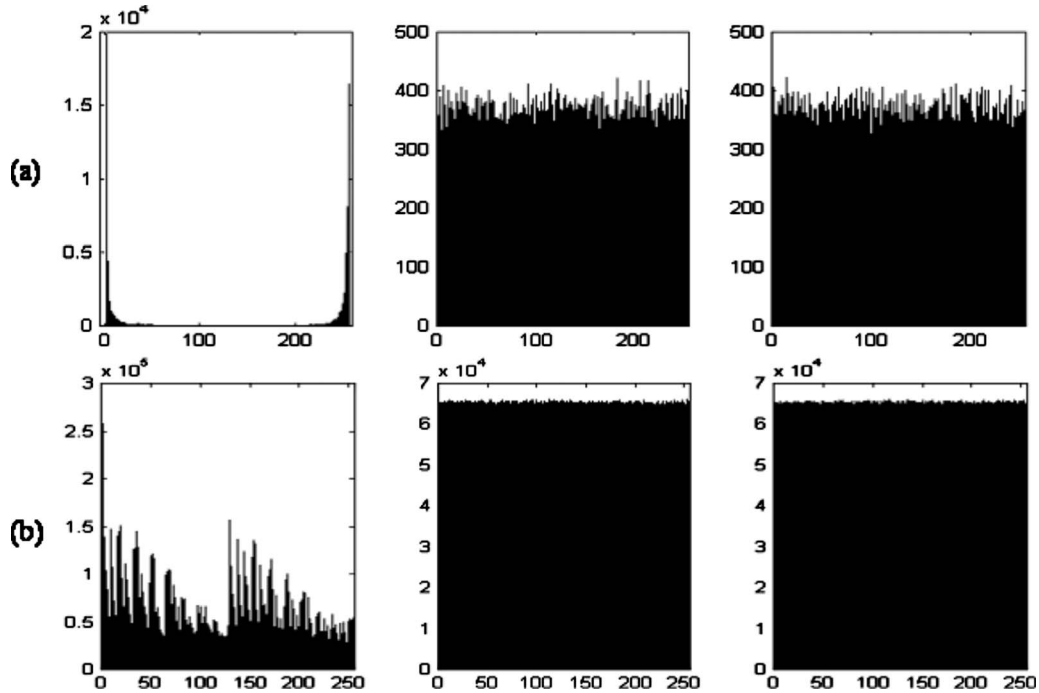

FIG. 4. Histogram of plaintext (left column) and corresponding ciphertext for two different system-keys (center and right columns). Plaintext corresponds to data shown in Table I: (a) audio file and (b) movie file.

- Sensitivity to system-key: for two keys (or plaintexts) with the slightest difference, no distinguishable difference between the corresponding ciphertext can be found by any known statistical analysis.
- Sensitivity to plaintext: flipping one bit in the plaintext should create a completely different ciphertext.
- Statistical independency: cipher text should be statistically undistinguishable from the output of a truly random function, and should be statistically the same for all keys.

We will address the security of our scheme following these three properties (not in the same order), without considering the masking step in Eq. (6).

Figure 4 shows the histograms of plaintext and corresponding ciperhtext of data files described in Table I. For each plaintext we use two randomly chosen keys to prove the statistical independency of the scheme. In both cases the ciphertext histogram is uniform and independent of the plaintext histogram and system-key. As an average, 99.6% of the total bytes and 50% of the total bits were changed during the encryption process, fulfilling a basic requirement for secure cryptosystems. The scheme response to a slight change in the system-key (flipping the least significant bit) is shown in Fig. 5. Because of the de-correlation process between the system-key and maps variables and parameters [Eq. (3)] the ciphertext output diverges since the first iteration.

Let us now analyze the effect in the difference (in the least significant bit) of a pair of plaintexts on the ciphertext output sequence without perturbation (this is known as differential attack). Figure 6 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 from iteration 5, the sequences take

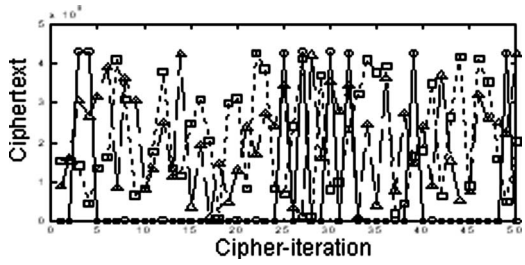

FIG. 5. Sensitivity to system-key changes. Plaintext (circled continuous line) encrypted with two slightly different system-keys (least significant bit changed).

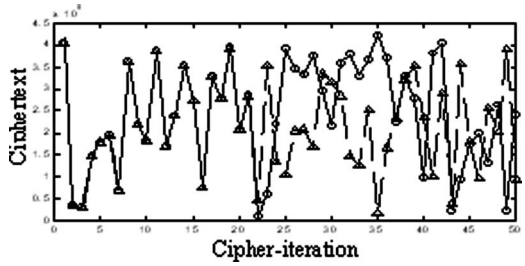

FIG. 6. Sensitivity to plaintext changes without perturbation scheme. Ciphertexts of a pair of chosen plaintexts with the least significant bit changed.

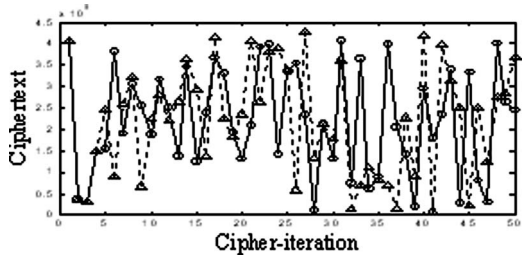

FIG. 7. Same as in Fig. 6 with initial perturbation at fifth cipher iteration (vertical dotted line)

TABLE II. Correlation coefficient between plaintext and corresponding ciphertext for the entire sample files in Table I.

File type	Bits considered in the computation		
	8	16	32
Audio (.wav)	0.002	0.0018	0.00065
Video (.mov)	0.000 11	0.000 025	0.000 18

TABLE IV. Average encryption execution time.

3 GHz Pentium®-IV with 1 GB of memory		
OS	Nonoptimized compilation (Mbs)	Optimized compilation (Mbs)
Linux-2.4.20-28.9	540	1088
Windows® XP	510	1423

different trajectories immediately, influencing future ciphertexts output values (Fig. 7). Since perturbation modifies map variables, the rest of the cipher trajectory is completely different and uncorrelated from the unperturbed case. In order to estimate the long term statistical independence of the generated ciphertext, we calculated the correlation coefficient for two different cases: (a) between plaintext and corresponding ciphertext (Table II) and (b) between two different ciphertexts (Table III). In case (b), we analyzed two additional cases: (i) the system-keys differ in the least significant bit and (ii) the plaintext sequences for the corresponding ciphertexts differ in the least significant bit of the first byte (Table III). The correlation coefficient was calculated considering the entire sample files in Table I for different ciphertext data sizes 8, 16, and 32 bits. As can be seen in Tables II and III, the correlation coefficient is practically zero in all cases.

If the opponent chooses brute force attack, it will need to search for at least 2^B key possibilities in our current setting, where $B>128$ bits. Additionally, it will need to search for four more random numbers with 5-bit representation each, RT, PT_1, n_1, and n_2, one more (m—the size of the $W_{m,k}$) with an 8-bit representation, and $N+1$ n-bit variables representing the local and global feedback.

Finally, a C-language implementation of the proposed cryptosystem (Table IV) shows that our scheme is fast enough to support real-time multimedia communications.

IV. CONCLUSIONS

We have proposed a simple and robust symmetric block-cipher cryptosystem based on an N-array of chaotic logistic maps with local and global feedback and a three-level perturbation scheme. We have shown the perfect statistical properties of the system, as well as its sensitivity to initial conditions (using coupled chaotic maps). Our system is scalable, that is the number of maps and system-key size can be modified to add security to the system (making impossible brute force attacks). Finally, a software implementation of the system shows excellent performance to fulfill current multimedia application demands, such as real-time audio and video communications.

TABLE III. Correlation coefficient between two ciphertexts produced with the least significant bit changed in the system-key and the least significant bit changed in the first byte of the plaintext sequence. The correlation coefficient is computed over the entire audio and video ciphertext sequences.

Ciphertext with	File type	Bits considered in the computation		
		8	16	32
System-key changed	Audio (.wav)	0.005	0.005	0.015
	Video (.mov)	0.0002	0.0003	0.013
Plaintext changed	Audio (.wav)	0.0004	0.002	0.006
	Video (.mov)	0.0002	0.0005	0.0005

[1] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos, Solitons Fractals **21**, 749 (2004).
[2] B. Furth and D. Kirovski, *Multimedia Security Handbook (Internet and Communications)* (CRC Press, Boca Raton, FL, 2004).
[3] R. Matthews, "On the derivation of a chaotic encryption algorithm," Cryptologia **13**, 29 (1989).
[4] G. Álvarez, F. Montoya, G. Pastor, and M. Romera "Chaotic cryptosystems," in *Proc. IEEE 33rd Annual Int. Carnahan Conf. on Security Technology*, Madrid, Spain, 5–7 October 1999 (IEEE, New York, 1999), pp. 332–338.
[5] G. Jakimoski and L. Kocarev, "Chaos and cryptography: block encryption ciphers based on chaotic maps," IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **48**, 163 (2001).
[6] N. K. Pareek, V. Patidar, and K. K. Sud, "Discrete chaotic cryptography using external key," Phys. Lett. A **309**, 75 (2003).
[7] L. Kocarev, "Chaos-based cryptography: a brief overview," IEEE Circuits Syst. Mag. **1**, 6 (2001).
[8] G. Álvarez and S. Li, "Breaking an encryption scheme based on chaotic Baker map," Phys. Lett. A **352**, 78 (2006).
[9] G. Álvarez and S. Li, "Breaking cryptography with chaos at the physical level," http://arXiv.org/PS_cache/nlin/pdf/0403/0403029v1.pdf (2004).
[10] M. S. Baptista, "Cryptography with chaos," Phys. Lett. A **240**, 50 (1998).
[11] E. Biham, "Cryptanalysis of the chaotic-map cryptosystem suggested at EUROCRYPT'91," Lect. Notes Comput. Sci. **547**, 532 (1991).
[12] J. I. Guo, J. C. Yen, and H. F. Pai, "New voice over Internet protocol technique with hierarchical data security protection," IEE Proc. Vision Image Signal Process. **149**, 237 (2002).
[13] G. Jakimoski and L. Kocarev, "Analysis of some recently proposed chaos-based encryption algorithms," Phys. Lett. A **291**, 381 (2001).
[14] S. Li, G. Chen, K. Wong, X. Mou, and Y. Cai, "Baptista-type chaotic cryptosystems: Problems and countermeasures," Phys. Lett. A **332**, 368 (2004).
[15] C. Li, S. Li, D. Zhang, and G. Chen, "Cryptanalysis of a data security protection scheme for VoIP," IEE Proc. Vision Image Signal Process. **153**, 1 (2005).
[16] S. Li, X. Mou, Z. Ji, J. Zhang, and Y. Cai, "Performance analysis of Jakimoski-Kocarev attack on a class of chaotic cryptosystem," Phys. Lett. A **307**, 22 (2004).
[17] S. Li and X. Zheng, "Cryptanalysis of a chaotic image encryption method," *Proc. IEEE Int. Symp. Circ. Sys. (ISCAS-2002)*, Phoenix-Scottsdale, AZ, 26–29 May 2002 (IEEE, New York, 2002), Vol. 2, pp. 708–711.
[18] K. Wong, "A fast chaotic cryptographic scheme with dynamic look-up table," Phys. Lett. A **298**, 238 (2002).
[19] K. Wong, K. Man, S. Li, and X. Liao, "A more secure chaotic cryptography based on Dynamic Look-up Table," Circuits Syst. Signal Process. **24**, 571 (2005).
[20] P. M. Binder and R. V. Jensen, "Simulating chaotic behavior with finite-state machines," Phys. Rev. A **34**, 4460 (1986).
[21] S. Li, X. Mou, Z. Ji, J. Zhang, Y. Cai, Z. Ji, and J. Zhang, "On the security of a chaotic encryption scheme: problems with computerized chaos," Comput. Phys. Commun. **153**, 52 (2003).
[22] J. Cernak, "Digital generators of chaos," Phys. Lett. A **214**, 151, (1996).
[23] T. Sang, R. Wang, and Y. Yan, "Perturbance-based algorithm to expand cycle length chaotic key stream," Electron. Lett. **34**, 873 (1998).
[24] Y. Dobyns and H. Atmanspacher, "Characterizing spontaneous irregular

behavior in coupled map lattices," Chaos, Solitons Fractals **24**, 313 (2005).
[25]M. Dellnitz, M. Field, M. Golubitsky, A. Hohmann, and J. Ma, "Cycling chaos," IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **42**, 821 (1995).
[26]A. Palacios and H. Juárez, "Cryptography with cycling chaos," Phys. Lett. A **303**, 345 (2002).
[27]X. Wang, M. Zhan, X. Gong, and C. H. Lai, "Construction of a secure cryptosystem based on spatiotemporal chaos and its applications in public channel cryptography," http://arXiv.org/abs/nlin/0502026 (2005).
[28]A. Fog, "Chaotic random number generators with random cycle lengths," http://www.agner.org/random/theory/chaosran.pdf.
[29]G. Álvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," Int. J. Bifurcation Chaos Appl. Sci. Eng. **16**, 2129 (2006).
[30]F. Dachselt and W. Schuwartz, "Chaos and Cryptography," IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **48**, 1498 (2001).
[31]J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," Int. J. Bifurcation Chaos Appl. Sci. Eng. **8**, 1259 (1998).
[32]G. Álvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalysis of a discrete chaotic system using external key," Phys. Lett. A **319**, 334 (2003).
[33]S. Li, X. Mou, and Y. Cai, "Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography," Lect. Notes Comput. Sci. **2247**, 316 (2001).