Design and Efficient Implementation of a Chaos-based Stream Cipher

Mohammad Abu Taha, Safwan El Assad, Audrey Queudet, Olivier Déforges

Design and Efficient Implementation of a Chaos-based Stream Cipher

Mohammed AbuTaha
Institut d'Electronique et de Télécommunications de Rennes
IETR, Université de Nantes, France
Email: mohammad.abu-taha@etu.univ-nantes.fr

Safwan EL ASSAD
Institut d'Electronique et de Télécommunications de Rennes
IETR, Université de Nantes, France
E-mail: safwan.el-assad@univ-nantes fr

Audrey Queudet
Institut de Recherche en Communications et Cybernétique de Nantes
IRCCyN, Université de Nantes, France
E-mail: audrey.queudet@univ-nantes fr

Olivier Deforges
Institut d'Electronique et de Télécommunications de Rennes
INSA de Rennes, France
E-mail: olivier.deforges@insa-rennes.fr

Abstract: We designed and implemented a stream cipher cryptosystem based on an efficient chaotic generator of finite computing precision (N = 32). The proposed structure of the chaotic generator is formed by a Key-Setup, an IV-Setup, a non-Volatile memory, an output and an internal state function. The chaotic generator uses the internal feedback mode and the generated keystream is used for secure stream ciphers. The cryptographic complexity mainly lies in the internal state containing two recursive filters, with one, two or three delays. Each recursive filter includes a perturbation technique using a linear feedback shift register (LFSR). The first recursive filter includes a discrete skew tent map, and the second one includes a discrete piecewise linear chaotic map (PWLCM). The chaotic generator is implemented in sequential and parallel versions using Pthread library. The proposed Stream ciphers have very good performance in terms of security and execution time. The parallel version of the proposed chaos-based stream cipher is faster than the eSTREAMS project, and other known chaos-based stream cipher when the data size is big. The security performance of the chaos-based stream cipher is analyzed, cryptanalytic analysis and statistical tests such as the Histogram with the Chi-square test, correlation and the NIST test are applied. Experimental results highlight the robustness of the proposed system. The security of the implemented stream ciphers is investigated by applying several software security tools.

Keywords: Stream cipher; Chaotic generator; Chaotic multiplexing; Parallel computing

Reference M. AbuTaha, S. EL ASSAD, A. Queudet and O. Deforges'Design and Efficient Implementation of a Chaos-based Stream Cipher', *International Journal of Internet Technology and Secured Transaction*, Vol. x, No. x, pp.xxx–xxx.

Biographical notes: Mohammed AbuTaha received the M.S. degree in Informatics from Palestine Polytechnic University, Hebron-Palestine, he is currently pursuing the Ph.D. degree from Nantes University, France. His research interests include security of image and video, Linux based Real time applications and embedded systems, Parallel programming.

Safwan El Assad, joints the University of Nantes, France in September 1987, where he is now an Associate Professor. Since 2005, his man research are in: Chaos-based crypto and crypto-compression systems for secure transmitted and stocked data.

Audrey Queudet graduated in Computer Engineering at Polytechnic School of the University of Nantes (France), she is an Associate Professor at the University of Nantes. Her research interests include real-time scheduling theory, quality of service guarantees for soft real-time systems, and Linux-based real-time operating systems and applications.

Olivier Deforges received the Ph.D. degree in image processing in 1995. He is a Professor with the National Institute of Applied Sciences (INSA) of Rennes since 2005. His principal research interests are image and video lossy and lossless compression, image understanding, fast prototyping, and parallel architectures.

1 Introduction

Cryptography was used in the past to keep military information and diplomatic correspondence secure and to protect national security. In recent times, the range of cryptography applications has been widely expanded, following the development of new communication means. Cryptography is used to ensure that the contents of a message are confidentially transmitted and cannot be altered. Chaos is one interesting field of research dealing with nonlinear, deterministic, and dynamic systems. It is applied to many different domains such as physics, robotics, biology, finance and encryption. The most important chaos properties are the high dependency on initial conditions and parameter variation, ergodicity and the random-like behavior. These properties entice researchers to develop chaotic secure communication systems (Kocarev (2001)), (El Assad and Farajallah (2016)), (Farajallah et al. (2016)), (Setti et al. (2005)), (Cimatti et al. (2007)), (AbuTaha et al. (2015)), (Arlicot (2014)), (Caragata et al. (2010)), (Chetto et al. (2014)). Under certain conditions, chaos can be generated by any non-linear dynamic system (Smale (1967)). For public channels including network communication and for computer communication, most data transactions (valuable information) need to be protected from malicious attacks and threats (Li and Lee (2016)), (Masoumi et al. (2016)), (Jo and Koh (2016)) . A block symmetric cipher is one of the classical encryption technique, widely used in the literature. The Advanced Encryption Standard (AES) is one of the most famous symmetric encryption for block ciphers. The stream cipher is used to secure useful information that must be transmitted continuously over the network communication for example. Generally stream ciphers are more efficient than block ciphers in two situations:1) in software applications requiring a very high encryption or decryption rate and 2) in hardware applications where physical resources(e.g: chip area, power, etc) are restricted. Handling a stream cipher encryption with block ciphers is possible by using counter and output feedback modes (CTR, OFB). Because the AES is very secure and widely adopted, its two modes, namely CTR and OFB are used as stream ciphers. However, to benefit from both advantages of stream ciphers compared to block ciphers, several stream cipher designs such as RC4 and eSTREAM algorithms have been produced. RC4 is one of the widely known stream ciphers and a hardware implementation was performed in an efficient way by Gupta et al., (Gupta et al. (2013)). However, RC4 is now broken. The eSTREAM project was a multi-year effort, running from 2004 to 2008, to promote the design of efficient and compact stream ciphers suitable for the widespread adoption of Estream (eSTREAM (2008)). Nevertheless, until now most of the eSTREAM ciphers are still not definitely secure (Manifavas et al. (2015)). Chaos-based stream ciphers are used to enhance the security issue (Machicao et al. (2012)).

In this paper, we propose a new chaos-based stream cipher. The proposed system is based on an efficient chaotic generator using two chaotic recursive filters, a technique of disturbance and chaotic multiplexing. The remainder of the paper is structured as follows. The next Section reviews the related work and Section 3 recalls the main technique used in parallel programming. The structure of the proposed stream cipher is described in Section 4. We detail the description of the proposed chaotic generator in Section 4.1 and Section 4.2 provides its parallel implementation. Next Section 4.3 gives the computation performance of the generator. In Section 5, we set out the performance of the stream cipher in terms of encryption speed and security using known cryptographic and statistical attacks. Finally, Section 6 concludes our contribution and outlines some directions for future work.

2 Related Work

In the following paper we recall the main related works in standard and chaos-based stream ciphers.

2.1 AES-CTR and eSTREAM Software

AES-CTR Mode

Counter mode, a standard introduced by Diffie and Hellman in 1979, is one of the best known modes used for stream ciphers. Counter mode switches a block cipher into a stream one. It generates the next keystream block by encrypting successive values of a counter. After each block encryption, the counter must be different and this can be done simply by incrementation of the counter by some constant, typically one. CTR mode has significant efficiency advantages over the standard encryption modes without weakening the security. In particular its tight security has been proven. On the other hand most of the perceived disadvantages of CTR mode are not valid criticisms, but rather caused by a lack of knowledge (Lipmaa et al. (2000)).

Rabbit

Rabbit is a stream cipher algorithm. Its rose/developed as a fast software encryption method in 2004. It is one of the most effective algorithm developed in the eSTREAM project. Rabbit is directed to be used in both software and hardware applications. The Rabbit Algorithm takes a 128-bit key and a 64-bit IV vector as input. At each iteration it, generates a 128-bit output. The output is pseudo-random in its nature. The heart of this cipher consists of 513 internal state bits. clearly the output generated in each iteration is some combination of these state-bits. The 513 bits are divided into eight 32-bit state variables, eight 32-bit counters and one counter carry bit. The state functions which update these state

variables are non-linear and thus build the basis of the security provided by this cipher (Boesgaard et al. (2005)), (eSTREAM (2008)). The designers provided the security analysis considering several possible attacks: algebraic, correlation, and statistical attacks. They conclude that no huge weakness of Rabbit has been found. However in 2009, Kircanski and Youssef in their paper (Kircanski and Youssef (2009)) provide a differential fault analysis attack on Rabbit algorithm. The fault model in which they analyse the cipher is the one in which the attacker is assumed to be able to fault a random bit of the internal state. The attack requires around 128-256 faults, a precomputed table of size around $2^{41.6}$ bytes, this technique enables to recover the complete internal state of Rabbit in about 2^{38} steps.

Salsa20/r

Salsa20/r is one of the eSTREAM finalist algorithms for software implementation, where $r = 8, 12, 20$ represents the number of iterations of the round function. The algorithm is constructed on a pseudo-random function based on a 32-bit addition, bitwise XOR and rotation operations, which maps a 256-bit key, a 64-bit nonce (IV initial vector), and a 64-bit stream position to a 512-bit output (Bernstein (2008)), (eSTREAM (2008)). The Salsa20/8 version is very fast but not secure enough. Its weakness comes from a differential cryptanalysis performed by Tsunoo et al. (Tsunoo et al. (2007)). Salsa20/12 and Salsa20/20 algorithms seem to be secure so far, because no better attack than the brute-force attack has been reported.

HC-128 and HC-256

HC-128 is an efficient software stream cipher, which consists of two secret tables, each one with 512 32-bit elements. At each step they update one element from one of the two tables using a non-linear feedback function. All the elements of the two tables are updated every 1024 steps. At each step, one 32-bit output is generated from the non-linear output function. HC-256 is a new version that differs from HC-128 by the size of secret tables which is 1024 32-bit elements instead of 512 32-bit ones. All the elements of the two tables are updated every 2048 steps. At each step, HC-256 produces one 32-bit output (Wu (2008)), (Wu (2004)), (eSTREAM (2008)). However, in 2010, (Kircanski and Youssef (2010)) provide in a differential fault analysis attack on HC-128 their paper. The attack is based on the fact that, some of the inner state words of HC-128 may be exploited several times without being updated. Consequently, the complete internal state is recovered using about 7968 faults.

SOSEMANUK

SOSEMANUK is a software stream cipher that has a key length ranging from 128 to 256 bits. It takes an initial value IV vector of 128 bits. SOSEMANUK has two main components: a linear feedback register (LFSR) and a finite state machine (FSM). The LFSR operates on 32-bit words and at every clock a new 32-bit word is computed. The FSM has two 32-bit memory registers: at each step the FSM takes an input word from the LFSR, updates the memory registers and produces a 32-bit output (Berbain et al. (2008)), (eSTREAM (2008)). In 2011 (Salehani et al. (2011)) made a differential attack on SOSEMANUK. The attack needed around 6144 faults to recover the secret inner state of the cipher.

2.2 Chaos-based stream cipher

Abderrahim et al. (2014) in their paper propose a chaos-based stream cipher based on symbolic dynamic description and synchronization. Their main contribution concerns a pseudo-random number generator (PRNG) based on an appropriate mixture of perturbed chaotic maps. The synchronization of the emitter/receiver is performed by a symbolic dynamic-based method. One of the characteristics of their proposed stream cipher is that the chaotic symbolic dynamic sequences are easy to produce. The obtained bit rate, with an Intel Core i7 processor clocked at 3.5 GHz, and 8G of RAM is 10 Mbps.

Lü et al. (2004), proposed a one-way-coupled chaotic map lattice for cryptography of a self-synchronizing stream cipher. The system performs an analytical computation into real numbers, and incorporates some algebraic operations on integer numbers. The encryption/decryption operations is done in parallel using multiple chaotic maps. The authors claim that the system has a good security level, and good reliability against strong channel noise. They provide an encryption speed (around 914 Mbps on a 2 GHz CPU).

In 2007Li et al. (2007) published a stream cipher also based on a spatiotemporal chaotic system as done previously in (Lü et al. (2004)). The chaotic system uses coupled logistic maps, and simple algebraic computations. The system produces parallel keystreams for encrypting plaintexts via bitwise XOR. Security analysis is performed to prove the robustness of the system. The encryption speed is 700 Mbits in a computer with a 1.8 GHz CPU and 1.5 GB RAM.

The eSTREAM project ciphers have better performance in time than the three chaos-based stream ciphers. In the following sections we will describe our chaos-based stream cipher in sequential and parallel implementation.

3 Parallel programming techniques

As processors' speeds no longer significantly increase, multicore systems have become more popular. Thus to benefit from these systems, programmers have turned to parallel programming. Therefore, programmers have to deal more and more with parallel programming. Parallelism is achieved thanks to multiple processes running at the same time on multiple processors (Rani (2011)). It explicitly breaks the task down into

small units of execution, where each unit can be executed in parallel on a single processor. In this way multiple parts of the same task can run in parallel (Sinnen (2007)), (Lozi et al. (2016)). Parallel programming can be implemented using several different software interfaces, or parallel programming models. The programming model used in any application depends on the underlying hardware architecture of the system on which the application is expected to run: *shared memory* architecture or *distributed memory* environment. In *shared-memory* multiprocessor architectures, threads can be used to implement parallelism. Threads are lightweight processes, existing within a single operating system process. Threads share the same memory address space and state information of the process that contains them. Parallel programming can be implemented for shared memory systems using *automatic parallelization* (Banerjee et al. (1993)), *POSIX threads* (Butenhof (1997)) and *Solaris threads* (Butenhof (1997)), or *OpenMP* (Dagum and Enon (1998)). Among *distributed memory* programming models, the Message Passing Interface (MPI) model (Gropp et al. (1996)) is commonly used to parallelize applications. MPI is a very explicit programming model. The programmer implements the distribution of the tasks, communication between them, and decides how the work is allocated between the various threads. With the emergence of multi-core systems, hybrid programming models have also been developed. Within a single node, fast communication through shared memory can be exploited, and a networking protocol can be used to communicate across the nodes. Programs can then take advantage of both shared memory and distributed memory. In our parallel implementation we used *POSIX threads*.

4 Description of the proposed chaos-based stream cipher

In this section we present a synchronous stream cipher based on a novel chaotic generator with its two implemented versions (sequential and parallel). In sequential implementation, each generator call produces a 32-bit sample, that is immediately converted into 4 bytes and stored in a buffer, before being Xored with 4 bytes from the plaintext to obtain 4 ciphered bytes and so on. In the parallel implementation, each generator call produces four 32-bit samples, that are immediately converted into 16 bytes stored in a buffer and then Xored with 16 bytes from the plaintext. Here, a question of synchronization between generated samples arises after each generator call. More details about this question are given in Section 4.2. For a given plaintext data, the generator produces the necessary keystreams to obtain ciphering data. In Figure 1 the general structure of stream cipher encryption and decryption processes are shown.

As with any encryption system, the secret key K and the initial IV vector must be shared between the sender and the receiver. The key must be kept secret while the IV vector is not necessarily kept secret but must be a nonce. The common method to share the secret K between the two parties is a symmetric key distribution based on either symmetric encryption using a key distribution center (KDC) or asymmetric encryption using the RSA (Rivest, Adi Shamir and Leonard Adleman) algorithm (Stallings (2006)). The IVg is changed every new session as a key session.

4.1 Description of the proposed chaotic generator

The architecture of the proposed chaotic generator is composed of several black-boxes as presented in Figure 2. The detailed description of the internal state and the output function is given in Figure 3. The secret key `K`, the initial vector `Nonce IVg` and parameters are the inputs of the chaotic generator. From these inputs, the `IV-setup` computes another three IVs values and the `Key-setup`, in case of parallel implementation, creates another three keys. Then, four IVs and four keys will be used by four threads in the system. Since chaos is sensitive to any small changes in the secret key, the creation of each new key in the `Key-setup` entity is achieved by the circular shift rotation of the three bit value of $K1\_s, K1\_p$ parameters (see Figure 3). Moreover, the creation of each new IV in the `IV-setup` entity is achieved by the circular shift rotation of the three bit value of U_s, U_p. Before the execution of the program is completed, a new IV value is generated and stored in the Non-Volatile Memory box. The generation of this new value comes from `/dev/urandom` Linux PRNG (Gutterman et al. (2006)). The internal state, which contains the main cryptographic complexity of the system, is formed by two recursive filters of order three. The first recursive cell contains a discrete Skew tent map and the second one contains a discrete piecewise linear chaotic map. These maps are used as non-linear functions. We give below the outputs of the recursive cell containing the Skew tent map and of the recursive cell containing the PWLC map respectively. Hence the output equation of the recursive cell Skew tent map is:

$$X\_s = STmap\{F1[n-1], P1\} \oplus Q1 \tag{1}$$

with

$$F1[n-1] = mod[U\_s + \sum_{i=1}^{3}[K(i)\_s \times X(n-i)\_s], 2^N] \tag{2}$$

And the output equation of the recursive cell PWLC is:

$$X\_p = PWLCmap\{F2[n-1], P2\} \oplus Q2 \tag{3}$$

with

$$F2[n-1] = mod[U\_p + \sum_{i=1}^{3}[K(i)\_p \times X(n-i)\_p], 2^N] \tag{4}$$

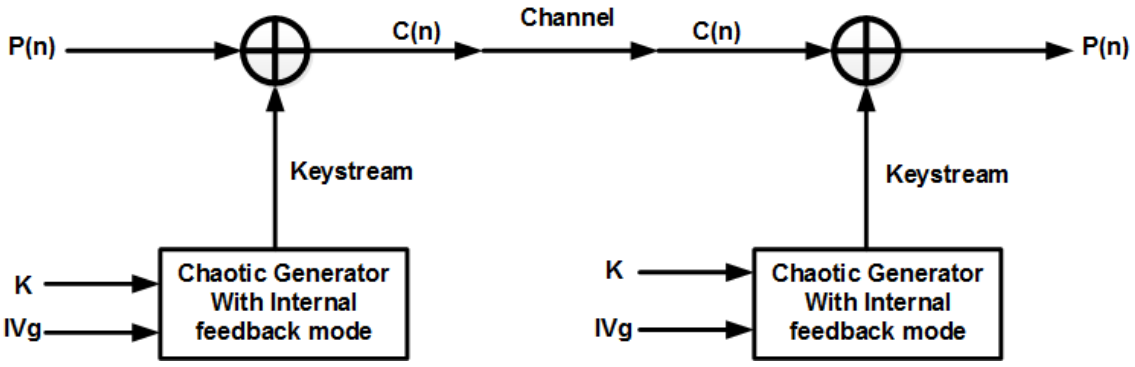


Figure 1: Stream cipher encryption/decryption structure

In the equations above, $P1$ and $P2$ are control parameters in the range $[1, 2^N - 1]$ and $[1, 2^{N-1} - 1]$ respectively. $Q1$ and $Q2$ are perturbing signals produced by the linear feedback shift registers (LFSRs). $K1\_s$, $K2\_s$, $K3\_s$, $K1\_p$, $K2\_p$, $K3\_p$ are the coefficients of the recursive cells in the interval $[1;\ 2^N - 1\ ]$. U_s and U_p, each of 32 bits, represent IVg of 64 bits.
The equations of the *Discrete* Skew Tent and *Discrete* PWLCM maps are respectively given by (Masuda and Aihara (2002)), (Lian et al. (2007)), (El Assad (2012)), (Desnos et al. (2014)): *Discrete* Skew Tent Map:

$$X_s[n] = \begin{cases} \left\lceil 2^N \times \frac{X_s[n-1]}{P1} \right\rceil & \text{if } 0 < X_s[n-1] < P1 \\ 2^N - 1 & \text{if } X_s[n-1] = P1 \\ \left\lceil 2^N \times \frac{2^N - X_s[n-1]}{2^N - P1} \right\rceil & \text{if } P1 < X_s[n-1] < 2^N \end{cases} \quad (5)$$

Discrete PWLCM map:

$$X_p[n] = \begin{cases} \left\lceil 2^N \times \frac{X_p[n-1]}{P2} \right\rceil & \text{if } 0 < X_p[n-1] \leq P2 \\ \left\lceil 2^N \times \frac{X_p[n-1] - P2}{2^{N-1} - P2} \right\rceil & \text{if } P2 < X_p[n-1] \leq 2^{N-1} \\ \left\lceil 2^N \times \frac{2^N - P2 - X_p[n-1]}{2^{N-1} - P2} \right\rceil & \text{if } 2^{N-1} < X_p[n-1] \leq 2^N - P2 \\ \left\lceil 2^N \times \frac{2^N - X_p[n-1]}{P2} \right\rceil & \text{if } 2^N - P2 < X_p[n-1] \leq 2^N - 1 \\ 2^N - 1 - P2 & otherwise \end{cases} \quad (6)$$

The values produced $X_s[n], X_p[n]$ by the recursive cells in `the internal state` are entered to `the output function`. Then, the output sequence $Xg(n)$ is obtained using a chaotic multiplexing controlled by the chaotic sequence $X1_s(n-1) \oplus X1_p(n-1)$ and by a threshold $Th = 2^{N-1}$, as shown in Figure 3. The output sequence is defined as follows:

$$Xg(n) = \begin{cases} Xs[n], \text{ if } 0 < X\_s[n-1] \oplus X\_p[n-1] <= Th \\ Xp[n], \text{ otherwise} \end{cases} \quad (7)$$

4.2 Parallel implementation of the chaotic generator using Pthread

Usually a multi thread process launches several threads that run concurrently. In our implementation, we parallelized the sequential version of our chaotic generator using the standard API used for implementing multithreaded applications, namely *POSIX Threads* or *pthread* (Pacheco (2011)). *pthread* is a library of functions that programmers can use to implement parallel programs. Unlike MPI, *pthread* is used to implement shared-memory parallelism. It is not a programming language (such as C or Java). It is a library that can be linked with C programs. The source code is compiled with *gcc* and using the *-lpthread* option. In our multithreaded approach, data sequences are partitioned among several threads. Threads execute the same instructions on different data sets. The number of samples to be processed and the starting point of the samples' subset data are different for each thread. The different threads are created and launched via a call to *pthread_create()*. In our case, we create a number of threads equals to the number of cores chosen in our system. The function *pthread_create()* takes the thread as parameter. Each thread will call the *computation* function. This function ensures the generation of the samples and the conversion to bytes. Then the computed sequences from threads will be stored in a buffer in a systematic manner to gain a maximum performance. Each sequence from each thread is then stored consecutively as illustrated in Figure 4. In the *main()* function, we wait for the termination of all threads by calling the *pthread_join()* function. To describe the decomposition of the sequences among the threads, we give the following example: consider that 4 cores are available on the platform and that the sequence length is *seq_length*=3125000 samples. 4 threads will then be created. The first thread computes samples from index $imin = 0 * 3125000/4 = 0$ to index $imax = (0+1) * (3125000/4) - 1 = 781249$. The second thread computes samples from index $imin = 1 * 3125000/4 = 781250$ to index $imax = (1+1) * (3125000/4) - 1 = 1562499$ and so on until the last

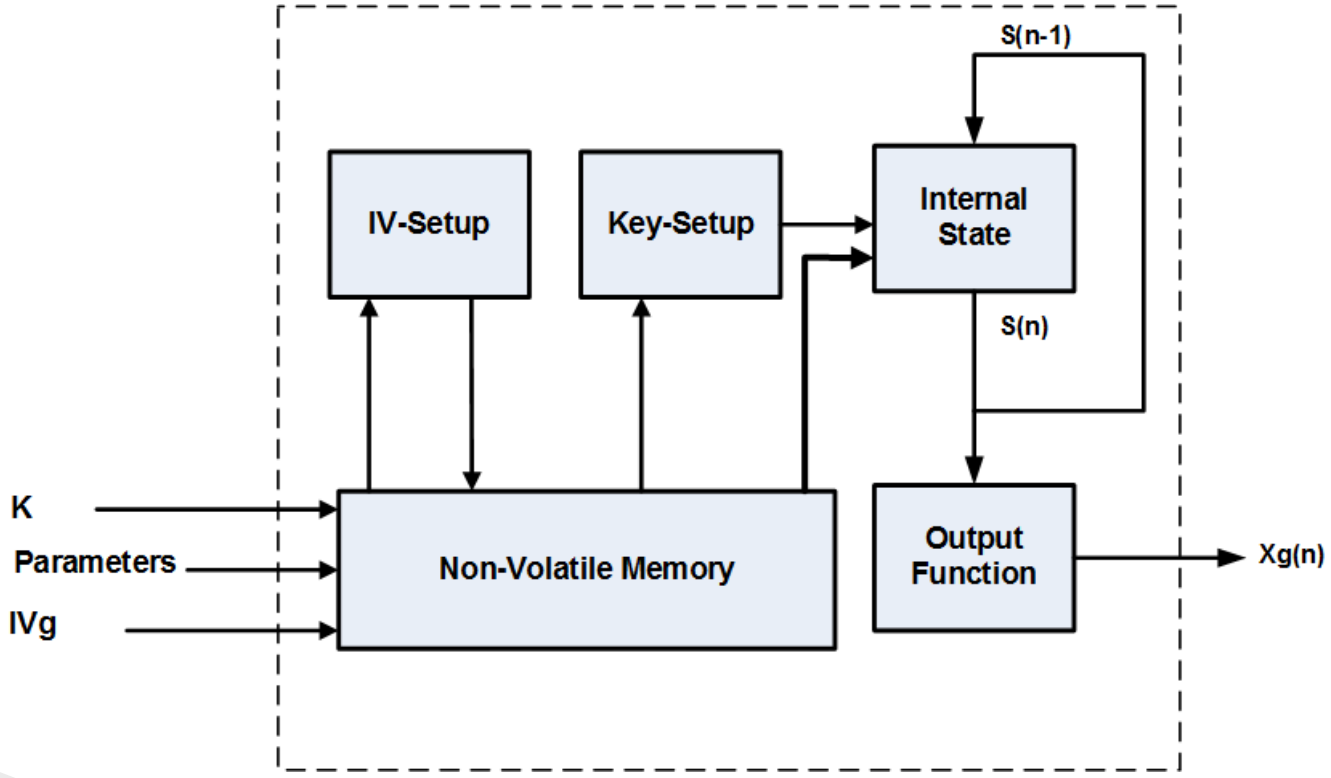


Figure 2: Architecture of the proposed generator with internal feedback mode

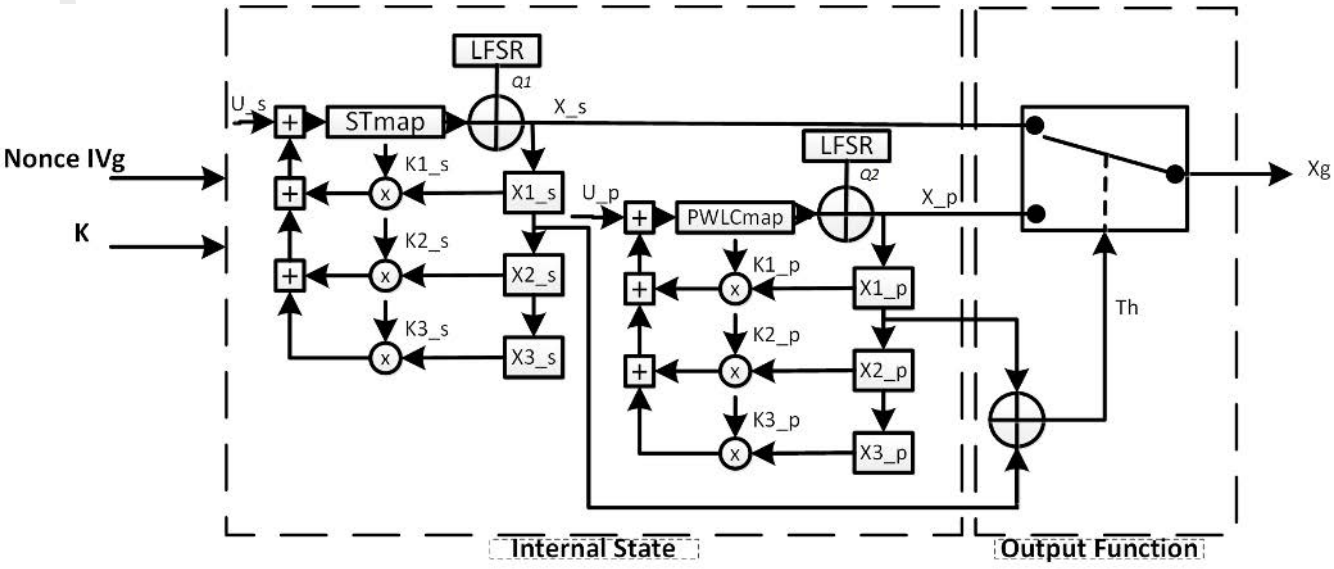


Figure 3: Detailed description of the internal state and the output function

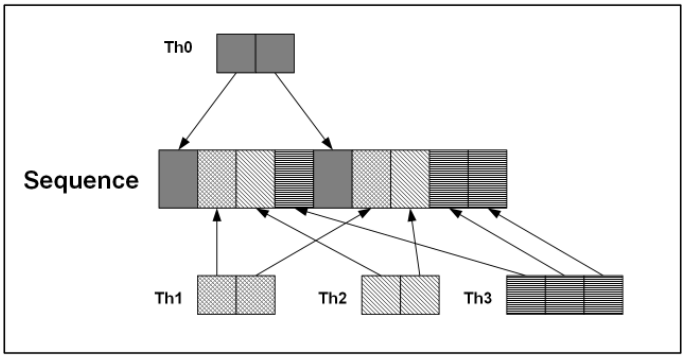


Figure 4: Storing of samples that generated by different threads.

Table 1 Generation time for sequential and parallel generators

Data (Bytes)	GT/Seq (μs)	GT/Parl (μs)
64	6	705
128	8	726
256	11	743
512	19	753
1024	32	763
2048	57	801
4096	109	810
16384	332	835
32768	520	847
65536	712	764
125000	1282	1325
196608	1830	1869
393216	2902	2436
786432	5502	4835
3145728	21723	19539
12582912	85009	49154

Table 2 NCpB performance of some PRNG

PRNG	NCpB (Cycles/B)
Wang et al. (2016)	160
Akhshani et al. (2014)	45
Ons et al.[conf icacci 2016]	24.68
Proposed algorithm	17.3

thread that will compute the rest of samples. The remainder of samples that resulted from the division of the number of sequences to the number of threads, if it exist, will also be computed by the last thread. Samples from each thread are stored in a shared result array, each thread filling specific index values.

4.3 Computing performance of the chaotic generator

To evaluate the computing performance of the proposed chaotic generator we performed some experiments using a two 32-bit multi-core Intel Core (TM) i5 processors running at 2.60 GHz with 16 G of memory. This

Table 3 Bit rate for sequential and parallel generators

Data (Bytes)	BR/Seq (Mbit/s)	BR/Parl (Mbit/s)
64	85.33	0.73
128	128	1.41
256	186.18	2.76
512	215.58	5.44
1024	256	10.74
2048	287.44	20.45
4096	300.62	40.45
16384	394.8	156.97
32768	504.12	309.5
65536	736.36	686.24
125000	780.03	754.72
196608	859.49	841.55
393216	1083.99	1291.35
786432	1143.49	1301.23
3145728	1158.49	1287.98
12582912	1184.15	2047.92

hardware platform was used on top of an Ubuntu 14.04 Trusty Linux distribution. Here after, for different sizes of data bytes, we give the average generation time in micro second GT(μs), the average bit rate en Mega bit par second BR(Mbit/s), and the average of the required number of cycles to generate one byte, NCpB(Cycles/B). The average is determined by using 100 different secret keys for each data size. For parallel implementation we choose 4 threads in parallel running on a 4-cores platform. The results obtained for GT(μs), BR(Mbit/s) and NCpB(Cycles/B) are given in Tables 1, 3 and 4 and are depicted in Figures 5, 6 and 7 for sequential and parallel implementation. The number of cycles required to generate one byte *NCpB* is given by:

$$\text{NCpB} = \frac{\text{CPU Speed}_{(Hertz)}}{Db_{(Byte/s)}} \tag{8}$$

As we can see from these results, the parallel implementation is only better for data size equal to or bigger than 393216 bytes. This is due to the overhead time caused by the synchronisation between threads. In Table 2 we compare our obtained results in terms of NCpB with some known chaos-based generators, for data

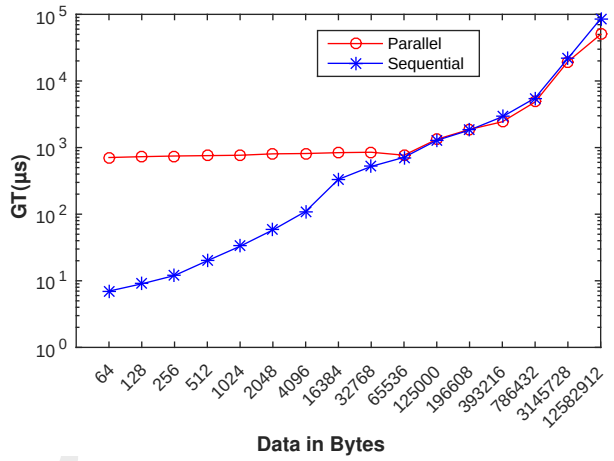


Figure 5: Generation time for parallel and sequential generators.

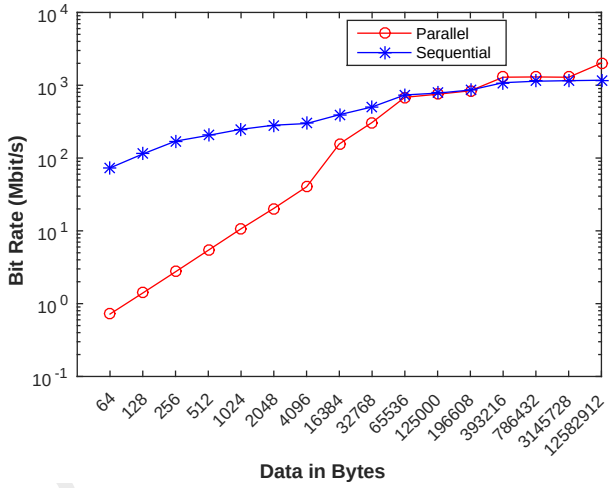


Figure 6: Bit Rate for parallel and sequential generators.

size equal to 786432 bytes that correspond to a image size of $512 * 512 * 3$. As we can see, the obtained performance is good.

5 Encryption speed and security analysis of the proposed stream cipher

5.1 Time performance

The computation performance is determined by: the average encryption time $Enc\_T(\mu s)$, the average encryption throughput ET(Mbit/s) defined in Equation 9, and the average number of cycles to encrypt one byte NCpB(Cycles/B) defined previously in Equation 8.

$$ET = \frac{Image_{Size}(Mbit)}{Encryption_{Time}(s)} \quad (9)$$

Table 4 NCpB for sequential and parallel generators

Data (Bytes)	NCpB-S (Cycles/B)	NCpB-P (Cycles/B)
64	232.5	27173.2
128	155	14068.4
256	106.5	7187.1
512	92	3646.4
1024	77.5	1847
2048	69	970
4096	66	490.4
16384	50.2	126.4
32768	39.3	64.1
65536	26.9	28.9
125000	25.4	26.3
196608	23.1	23.6
393216	18.3	15.4
786432	17.3	15.2
3145728	17.1	15.4
12582912	16.8	9.7

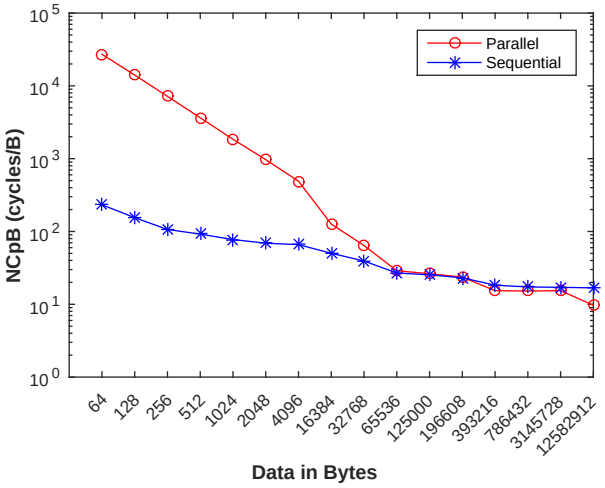


Figure 7: NCpB for parallel and sequential generators.

We report in Table 5 and in Figures 8, 9, 10 the obtained results of the computation performance for sequential and parallel implementation of the proposed stream cipher. The decryption time is approximatively equal to the encryption time.

For big data size, from 196608 bytes upwards, the parallel implementation is better than the sequential one and on average the NCpB of the stream cipher takes approximatively 8 cycles more compared to the NCpB of the chaotic generator.

In Table 6, we report a comparison of time computation for the proposed algorithm (for different data size images of Lena) with three chaos-based algorithms and the most Known stream ciphers of eStream project (Maxime (2016)). For big data, the proposed algorithm has better results than (Abderrahim et al. (2014)), (Lü et al. (2004)). We also observed that the time computation of eStream's algorithms is better than the proposed system until we reach the big data size, for which, our system will be faster. For very big data size (201326592) such

Table 5 Performance results of proposed sequential Stream Cipher with different data bytes

Data in Bytes	Enc-T(μs) Seq/Parl	ET (Mbit/s) Seq/Parl	NCpB (Cycles/B) Seq/ Parl
512	21/ 778	213.01/ 5.31	92.9/ 3650.7
1024	33/ 792	259.1/ 11.1	78.2/ 1889
2048	60/ 806	286.5/ 19.9	70.2/ 973
4096	116/ 822	299.3/ 39.3	67.0/ 491.3
49152	659/ 1619	569.0/ 231.6	34.8/ 85.6
196608	2455/ 2419	610.9/ 620.0	31.9/ 31.2
786432	9088/ 8099	660.2/ 740.8	30.0/ 26.7
3145728	35560/ 24190	674.9/ 978.8	29.3/ 20.2
12582912	121899/ 88597	787.5/ 1083.5	25.1/ 18.3
50331648	398089/ 319785	964.6/ 1200.8	20.5/ 16.5

Table 6 Performance results comparison of some stream ciphers

Stream cipher-Alg	Image size(B)	Enc-Time(μs)	ET(Mbit/s)	NCpB(cycles/B)
Abderrahim et al.	-	-	10	2800
Hauping et al.	-	-	914	17
Ping et al.	-	-	700	20
Rappit	256x256x3	811.3	1848.8	9.5
	512x512x3	3256	1842.6	9.5
	1024x1024x3	12950	1853.9	9.5
HC-128	256x256x3	1221	1228.1	14.4
	512x512x3	4895	1225.6	14.4
	1024x1024x3	19647	1221.5	14.4
Salsa20/12	256x256x3	836.4	1793.4	9.8
	512x512x3	3389	1770	9.9
	1024x1024x3	13483	1779.9	9.9
SOSEMANUK	256x256x3	880.3	1704	10.3
	512x512x3	3570	1680	10.5
	1024x1024x3	14134	1698	10.4
AES-CTR	-	-	-	21.2
Proposed chaos stream cipher (Seq)	256x256x3	2455	610.9	31.9
	512x512x3	9088	660.2	30.0
	1024x1024x3	35560	674.9	29.3
Proposed chaos stream cipher (Parl)	256x256x3	2419	620	31.2
	512x512x3	8099	740.8	26.7
	1024x1024x3	24190	978.8	20.2
	201326592	1200178	1881	8.8

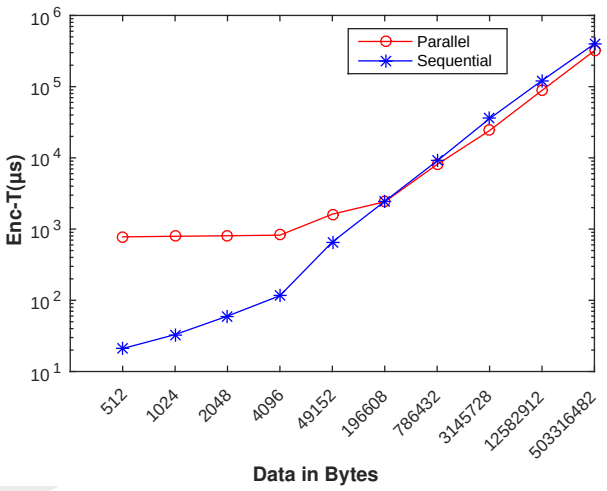


Figure 8: Encryption time for parallel and sequential cryptosystem.

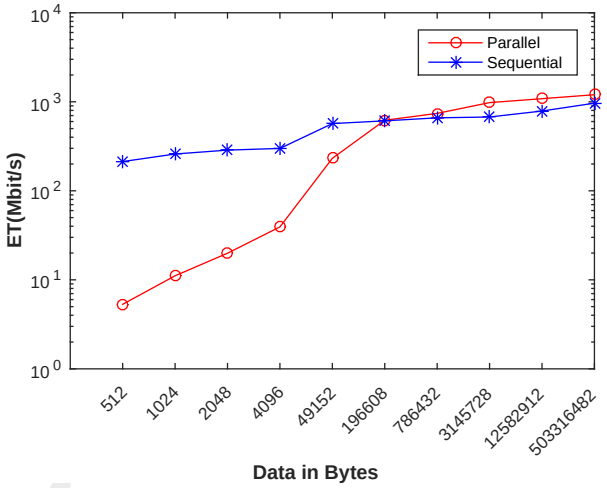


Figure 9: Encryption throughput for parallel and sequential cryptosystem.

as videos, the obtained NCpB is around 9. In addition, the proposed chaotic system has a strong non-linearity compared to the other systems thus, its robustness against cryptographic attacks is higher.

5.2 Security analysis

In this section we evaluated the software security implementation and the security of the proposed chaotic system against cryptanalytic and statistic attacks.

5.2.1 Software security implementation

Software security analysis is another crucial factor to ensure the quality of the source code and to restrict all security threats. Because it is still possible to read data out of memory even if the application no

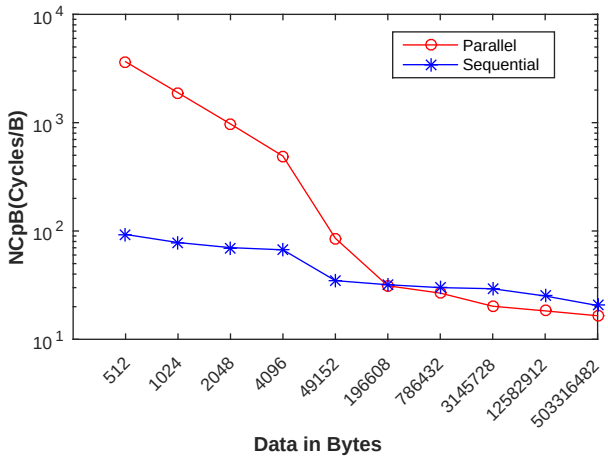


Figure 10: NCpB for parallel and sequential cryptosystem.

longer has pointers to it, it is necessary to incorporate data security within the source code. In cryptographic applications, sensitive information (e.g., secret keys) must be kept in memory for the minimum amount of time possible and should be written over/deleted, not just released, when no longer needed. One first step consists in erasing such sensitive data from memory once it is no longer needed in order to prevent any security attacks. The idea is to zero-fill buffers which contained sensitive information. In practice, we used the following functions to decontaminate (i.e., zero) a buffer and guarantee that the compiler will not optimize it away: The `secure_memzero()` function depends on a function pointer `memset_ptr` that itself points to the `memset()` `function`. It uses the key and the key size and will put zero value on the allocated memory related to the key by call `memset()`. The function `memset()` is invoked to write a specific value in a buffer that was allocated previously. We used this function to write a zero value in the buffer. While Some compilers optimize away the call to `memset()` function. To overcomes this , we declared `memset_ptr` as a *volatile* pointer. Since a *volatile* pointer can be manipulated outside the scope of the application, the code is not optimized by the compiler, thus keeping the program unchanged. Furthermore, the data in main memory may leak to the disk through virtual memory, thus representing another source of the most serious leaks (leaks to physical mediums). One solution, which is sufficient to include, is to deactivate the swap space altogether, thus preventing data from being written to the page file by locking it in memory. In our code, we used the `mlock()` function that locks pages in the address range starting at the address and continuing for byte lengths. All pages that contain a part of the specified address range are secured to be resident in the main memory when the call returns successfully. Then, the pages are guaranteed to stay in the main memory until later unlocked.

In order to guarantee the validity of our solution, we

carried out a security code review using several static and dynamic techniques: Clang, Gdb, Valgrind, DRD, Callgrind and Leak-analysis tools. Results match up well with the security level requested by our chaos-based stream cipher (Taha et al. (2016)).

5.2.2 Cryptanalytic attacks

The proposed system has the ability to resist common attacks such as ciphertext only (Siegenthaler (1985)), chosen plaintext attack, brute force attack, and key sensitivity attack. Indeed, encrypting an image several times using the same secrete key, produces totally different ciphered images. This is due to the IV-setup block.

Key Space

The size of the secret key, formed by all the initial conditions and by all the parameters of the system, varies from 299 bits, with delay = 1, to 555 bits, with delay =3. This means that the brute force attack is impracticable.

Key security and sensitivity attack

From the generated sequences it is impossible to find the secret key and this is because of the structure of the chaotic generator which in addition includes a chaotic switching. The knowledge of part of the secret key is not very useful for an attacker because of the intrinsic property of chaotic signal, which is extremely sensitive to the secret key. Besides, we computed the average Hamming distance (of 100 secret keys) of two Keystreams generated each time with two secret keys that differ only by one bit and the result obtained is equal to 0.499993, therefore very close to 50%. In conclusion, the produced keystreams are highly secure. A cryptosystem must be sensitive to one bit change per key used. This property is important in order to resist many attacks (Lian et al. (2005)). To test the key sensitivity of the proposed chaos stream cipher, we encrypted "Lena" image 100 times using 100 secrete keys that differ only by the LSB bit. Then we computed the following parameters: the Number of Pixel Change Rate (NPCR), the Unified Average Changing Intensity (UACI) and the Hamming Distance (HD). The parameters (NPCR, UACI) are necessary but not sufficient to ensure that the proposed cryptosystem is resistant against the key sensitivity attack. For this reason, we add the Hamming Distance measurement (Mar and Latt (2008)).

The NPCR and UACI, introduced by Eli Biham and Adi Shamir (Biham and Shamir (1991)) are given by the following equations:

$$NPCR = \frac{1}{L \times C \times P} \times \sum_{p=1}^{P} \sum_{i=1}^{L} \sum_{j=1}^{C} D(i,j,p) \times 100\% \quad (10)$$

where

$$D(i,j,p) = \begin{cases} 0, & \text{if} \quad C_1(i,j,p) = C_2(i,j,p) \\ 1, & \text{if} \quad C_1(i,j,p) \neq C_2(i,j,p) \end{cases} \quad (11)$$

$$UACI = \frac{1}{L \times C \times P \times 255} \times \sum_{p=1}^{P} \sum_{i=1}^{L} \sum_{j=1}^{C} |C_1(i,j,p) - C_2(i,j,p)| \times 100\% \quad (12)$$

Table 7 The NPCR, UACI and HD

Cryptosystem	NPCR	UACI	HD
Proposed Cipher Cryptosystem	99.665	33.459	0.499999

In the previous equations, i, j and p are the row, column, and plane indexes of the image, respectively. L, C and P are, the length, width, and plane sizes of the image respectively. The optimal NPCR and UACI values are 99.61% and 33.46% respectively (Wu et al. (2011)).

The HD is defined by:

$$HD(C_1, C_2) = \frac{1}{|Ib|} \sum_{K=1}^{|Ib|} (C_1(K) \oplus C_2(K)) \quad (13)$$

where $|Ib| = LxCxPx8$, is the size of the image in bits. The optimum HD value is 50%. A good stream cipher should produce an HD close to 50% (Wang et al. (2014)). Table 7 indicates that the NPCR, UACI and HD values of the proposed stream cipher are very close to Optimal values. Consequently a high resistance to differential attack is achieved.

5.3 Statistical analysis

5.3.1 NIST Test

To evaluate the statistical performances of the Key stream produced, we also used one of the most popular standards for investigating the randomness of binary data, namely the NIST statistical test (Elaine and John (2012)). This test is a statistical package that consists of 188 tests that were proposed to assess the randomness of arbitrarily long binary sequences. We applied the NIST test to many ciphered texts, and all the NIST results obtained, are as expected (good NIST values). In Figure 11 we present one of the NIST result obtained. This means that the ciphered texts have a high randomness.

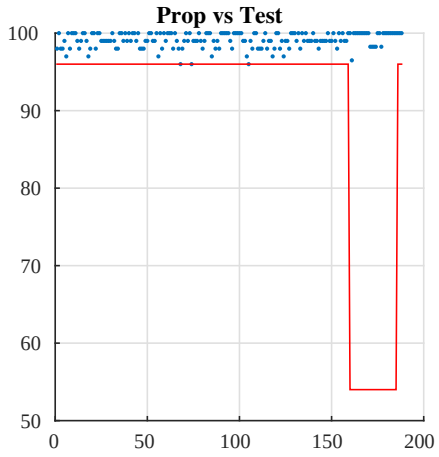
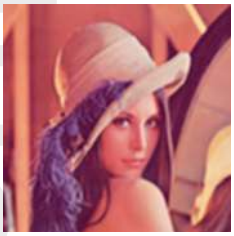
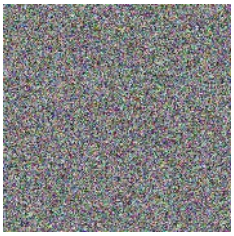


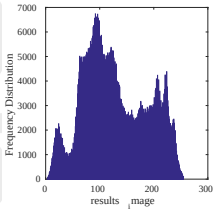
Figure 11: NIST test key stream results.



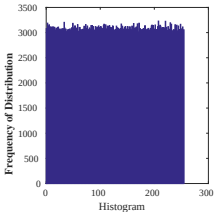
(a) Lena plain image



(b) Lena cipher image



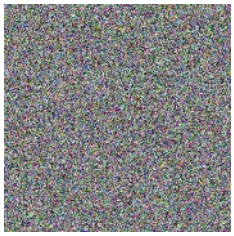
(c) Histogram for plain Image



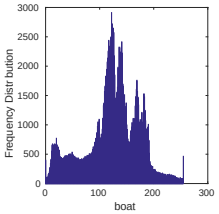
(d) Histogram for the cipher image

Figure 12: Histogram of the lena plain image and its ciphered image

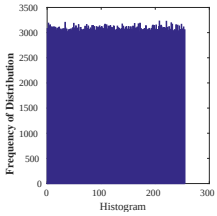
(a) Boat plain image



(b) Boat cipher image



(c) Histogram for plain Image



(d) Histogram for the cipher image

Figure 13: Histogram of the Boat plain image and its ciphered image

5.3.2 Histogram and Chi-square test

A cryptosystem is considered to be strong against statistical attacks, if the histogram of the ciphered text is uniformly distributed. Visually, the uniformity test is necessary, but it is not sufficient. The chi-square test is applied to statistically confirm the uniformity of the histogram:

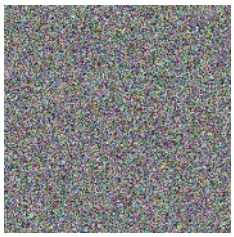
$$\chi^2_{exp} = \sum_{i=0}^{Q-1} \frac{(o_i - e_i)^2}{e_i} \tag{14}$$

Table 8 Chi-square value for ciphered Lena, Boat and C-man with different sizes

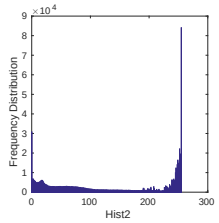
Image	Experimental value	Theoretical value
lena 256x256x3	261.085938	293.247835
lena 512x512x3	263.013852	293.247835
lena 1024x1024x3	270.300127	293.247835
boat 256x256x3	260.186354	293.247835
boat 512x512x3	266.465369	293.247835
boat 1024x1024x3	272.669811	293.247835
C-man 256x256x3	261.339680	293.247835
C-man 512x512x3	267.317852	293.247835
C-man 1024x1024x3	274.397541	293.247835

In equation (14), Q is the number of levels (here $Q = 256$), o_i is the observed occurrence frequency of each color level (0-255) on the histogram of the ciphered image, and e_i is the expected occurrence frequency of the uniform distribution, given here by $e_i = \frac{L \times C \times P}{Q}$. For a secure cryptosystem, the experimental chi-square value must be less than the theoretical chi-square one, which is 293 in case of $\alpha = 0.05$ and $Q = 256$. In Figures 12, 13 and 14 we give the histograms for the plain/cipher images for lena, Boat and Camera man images on size 512*512*3 . As we can see the histogram of the ciphered image seems to be uniform. To assess the uniformity, we performed the chi square test with the following parameters: alpha=0.05, and number of classes equal to 256. Experimental value obtained is less than the theoretical one that equal 293. This means that the histogram is uniform (see Table 8).

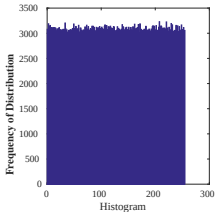
(a) Camera man plain image



(b) Camera man cipher image



(c) Histogram for plain Image



(d) Histogram for the cipher image

Figure 14: Histogram of the Camera man plain image and its ciphered image

5.3.3 Correlation analysis

Correlation analysis is also one of the statistical attacks that are used to cryptanalyze the cryptosystem. The attacker should not have any information of the used secret key or any partial information on the original plain image. This means that the encrypted image should be extremely different from its original version. Correlation analysis is one of the regular and standard methods to measure this property. Indeed, it is well-known that adjacent pixels in the plain images are very redundant and correlated. Thus, in the encrypted images, adjacent pixels should have a redundancy and a correlation as low as possible. The following mathematical equations are used to calculate the correlation coefficient (Song et al. (2013)):

$$\rho_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{15}$$

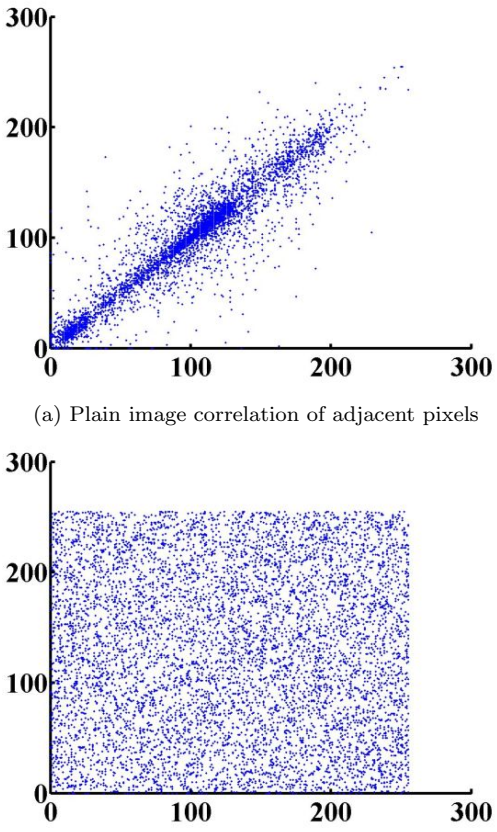
where

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}([x_i - E(x)][y_i - E(y)]) \tag{16}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{17}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i) \tag{18}$$

In the previous equations, x_i and y_i are the values of the two adjacent pixels in the plain image or the corresponding ciphered image.
To test the security of our proposed stream cipher algorithm, regarding to this type of attack, first N pairs of adjacent pixels in vertical, horizontal, and diagonal directions are selected from the plain image and its ciphered version. Figure 15 shows the correlation curves of the adjacent pixels in the horizontal direction for the plain image and its ciphered one. The values of their corresponding correlation coefficient are 0.96606 and 0.0035. Similar results are obtained for the correlation in vertical and diagonal directions.



(a) Plain image correlation of adjacent pixels

(b) ciphered image correlation of adjacent pixels

Figure 15: correlation of the boat plain image and its ciphered image

6 Conclusion

We proposed a new chaos-based stream cipher, useful for continuous communication as used in network communications. The heart of the system relies on a proposed chaotic generator that is designed and implemented in a secure and efficient manner with a sequential and parallel version. Its structure is modular, generic, and allow the production of high secure sequences. The performance in time for the proposed generator is better than other known PRNG. Also, For very big data size, the obtained performance results are better than other known stream ciphers. The proposed chaotic system is robust against cryptographic attacks. Furthermore, it has strong non-linearity compared to the other systems. Indeed, the results obtained from the cryptographic analysis and of common statistical tests indicate the robustness of the proposed stream cipher. Our future work will focus on the design of chaos-based joint crypto-compression systems to secure videos: HEVC bitstream and MPEG-4.

References

L. Kocarev, "Chaos-based cryptography: a brief overview," *Circuits and Systems Magazine, IEEE*, vol. 1, no. 3, pp. 6–21, 2001.

S. El Assad and M. Farajallah, "A new chaos-based image encryption system," *Signal Processing: Image Communication*, vol. 41, pp. 144–157, 2016.

M. Farajallah, S. El Assad, and O. Deforges, "Fast and secure chaos-based cryptosystem for images," *International Journal of Bifurcation and Chaos*, vol. 26, no. 2, pp. 1 650 021–1–1 650 021–21, 2016.

G. Setti, R. Rovatti, and G. Mazzini, "Chaos-based generation of arti. cial self-similar traffic," in *Complex*

Dynamics in Communication Networks. Springer, 2005, pp. 159–190.

G. Cimatti, R. Rovatti, and G. Setti, "Chaos-based spreading in ds-uwb sensor networks increases available bit rate," *Circuits and Systems I: Regular Papers, IEEE Transactions on*, vol. 54, no. 6, pp. 1327–1339, 2007.

M. AbuTaha, S. El Assad, M. Farajallah, A. Queudet, and O. Deforge, "Chaos-based cryptosystems using dependent diffusion: An overview," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 2015, pp. 44–49.

A. Arlicot, "Sequences generator based chaotic maps," Université de Nantes, Tech. Rep., FEB 2014.

D. Caragata, S. El Assad, H. Noura, and I. Tutanescu, "Secure unicast and multicast over satellite dvb using chaotic generators," *International Journal of Internet Technology and Secured Transactions*, vol. 2, no. 3-4, pp. 357–379, 2010.

M. Chetto, S. El Assad, and M. Farajallah, "A lightweight chaos-based cryptosystem for dynamic security management in real-time overloaded applications," *International Journal of Internet Technology and Secured Transactions 7*, vol. 5, no. 3, pp. 262–274, 2014.

S. Smale, "Differentiable dynamical systems," *Bulletin of the American mathematical Society*, vol. 73, no. 6, pp. 747–817, 1967.

L. Li and J.-H. Lee, "On the security of a strong provably secure identity-based encryption scheme without bilinear pairing," *International Journal of Internet Technology and Secured Transactions*, vol. 6, no. 3, pp. 178–185, 2016.

M. Masoumi, P. Habibi, A. Dehghan, M. Jadidi, and L. Yousefi, "Efficient implementation of power analysis attack resistant advanced encryption standard algorithm on side-channel attack standard evaluation board," *International Journal of Internet Technology and Secured Transactions*, vol. 6, no. 3, pp. 203–218, 2016.

I.-H. Jo and B.-S. Koh, "Building a common encryption scrambler to protect paid broadcast services," *International Journal of Internet Technology and Secured Transactions*, vol. 6, no. 3, pp. 167–177, 2016.

S. S. Gupta, A. Chattopadhyay, K. Sinha, S. Maitra, and B. P. Sinha, "High-performance hardware implementation for rc4 stream cipher," *IEEE Transactions on Computers*, vol. 62, no. 4, pp. 730–743, 2013.

eSTREAM, *eSTREAM: the ECRYPT Stream Cipher Project*, 2008. [Online]. Available: http://www.ecrypt.eu.org/stream/

C. Manifavas, G. Hatzivasilis, K. Fysarakis, and Y. Papaefstathiou, "A survey of lightweight stream ciphers for embedded systems," *Security and Communication Networks*, vol. 9, pp. 1227–1246, 2015.

J. Machicao, A. G. Marco, and O. M. Bruno, "Chaotic encryption method based on life-like cellular automata," *Expert Systems with Applications*, vol. 39, no. 16, pp. 12 626–12 635, 2012.

H. Lipmaa, D. Wagner, and P. Rogaway, "Comments to nist concerning aes modes of operation: Ctr-mode encryption," vol. 1, pp. 1– 4, 2000.

M. Boesgaard, M. Vesterager, T. Christensen, and E. Zenner, "The stream cipher rabbit," *ECRYPT Stream Cipher Project Report*, vol. 6, 2005.

A. Kircanski and A. M. Youssef, "Differential fault analysis of rabbit," in *International Workshop on Selected Areas in Cryptography*. Springer, 2009, pp. 197–214.

D. J. Bernstein, "The salsa20 family of stream ciphers," in *New stream cipher designs*. Springer, 2008, pp. 84–97.

Y. Tsunoo, T. Saito, H. Kubo, T. Suzaki, and H. Nakashima, "Differential cryptanalysis of salsa20/8," in *Workshop Record of SASC*, 2007.

H. Wu, "The stream cipher hc-128," in *New stream cipher designs*. Springer, 2008, pp. 39–47.

——, "A new stream cipher hc-256," in *International Workshop on Fast Software Encryption*. Springer, 2004, pp. 226–244.

A. Kircanski and A. M. Youssef, "Differential fault analysis of hc-128," in *International Conference on Cryptology in Africa*. Springer, 2010, pp. 261–278.

C. Berbain, O. Billet, A. Canteaut, N. Courtois, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier *et al.*, "Sosemanuk, a fast software-oriented stream cipher," in *New stream cipher designs*. Springer, 2008, pp. 98–118.

Y. E. Salehani, A. Kircanski, and A. Youssef, "Differential fault analysis of sosemanuk," in *International Conference on Cryptology in Africa*. Springer, 2011, pp. 316–331.

N. Abderrahim, F. Benmansour, and O. Seddiki, "A chaotic stream cipher based on symbolic dynamic description and synchronization," *Nonlinear Dynamics*, vol. 78, no. 1, pp. 197–207, 2014.

H. Lü, S. Wang, X. Li, G. Tang, J. Kuang, W. Ye, and G. Hu, "A new spatiotemporally chaotic cryptosystem and its security and performance analyses," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 14, no. 3, pp. 617–629, 2004.

P. Li, Z. Li, W. A. Halang, and G. Chen, "A stream cipher based on a spatiotemporal chaotic system," *Chaos, Solitons & Fractals*, vol. 32, no. 5, pp. 1867–1876, 2007.

M. S. Rani, "An efficient and scalable core allocation strategy for multicore systems," Ph.D. dissertation, Florida Atlantic University Boca Raton, FL, 2011.

O. Sinnen, *Task scheduling for parallel systems*. John Wiley & Sons, 2007, vol. 60.

J.-P. Lozi, F. David, G. Thomas, J. Lawall, and G. Muller, "Fast and portable locking for multicore architectures," *ACM Transactions on Computer Systems (TOCS)*, vol. 33, no. 4, p. 13, 2016.

U. Banerjee, R. Eigenmann, A. Nicolau, D. A. Padua *et al.*, "Automatic program parallelization," *Proceedings of the IEEE*, vol. 81, no. 2, pp. 211–243, 1993.

D. R. Butenhof, *Programming with POSIX threads*. Addison-Wesley Professional, 1997.

L. Dagum and R. Enon, "Openmp: an industry standard api for shared-memory programming," *Computational Science & Engineering, IEEE*, vol. 5, no. 1, pp. 46–55, 1998.

W. Gropp, E. Lusk, N. Doss, and A. Skjellum, "A high-performance, portable implementation of the mpi message passing interface standard," *Parallel computing*, vol. 22, no. 6, pp. 789–828, 1996.

W. Stallings, *Cryptography and network security: principles and practices*. Pearson Education India, 2006.

Z. Gutterman, B. Pinkas, and T. Reinman, "Analysis of the linux random number generator," in *Security and Privacy, 2006 IEEE Symposium on*. IEEE, 2006, pp. 2 – 16.

N. Masuda and K. Aihara, "Cryptosystems with discretized chaotic maps," *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on*, vol. 49, no. 1, pp. 28–40, 2002.

S. Lian, J. Sun, J. Wang, and Z. Wang, "A chaotic stream cipher and the usage in video protection," *Chaos, Solitons & Fractals*, vol. 34, no. 3, pp. 851–859, 2007.

S. El Assad, "Chaos based information hiding and security," in *Internet Technology And Secured Transactions, 2012 International Conference for*. IEEE, 2012, pp. 67–72.

K. Desnos, S. El Assad, A. Arlicot, M. Pelcat, and D. Menard, "Efficient multicore implementation of an advanced generator of discrete chaotic sequences," in *Chaos-Information Hiding and Security (CIHS), International Workshop on*, 2014.

P. Pacheco, *An Introduction to Parallel Programming*, 1st ed. Morgan Kaufmann, 1 2011. [Online]. Available: http://amazon.com/o/ASIN/0123742609/

Y. Wang, Z. Liu, J. Ma, and H. He, "A pseudorandom number generator based on piecewise logistic map," *Nonlinear Dynamics*, vol. 83, no. 4, pp. 2373–2391, 2016.

A. Akhshani, A. Akhavan, A. Mobaraki, S.-C. Lim, and Z. Hassan, "Pseudo random number generator based on quantum chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 101–111, 2014.

B. Maxime, "Comparative analysis of estream ciphers," Université de Nantes, Tech. Rep., March 2016.

M. A. Taha, S. El Assad, O. Jallouli, A. Queudet, and O. Déforges, "Design of a pseudo-chaotic number generator as a random number generator," in *The 11th International Conference on Communications*, 2016, pp. 401 – 404.

T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," *IEEE Transactions on computers*, vol. 100, no. 1, pp. 81–85, 1985.

S. Lian, J. Sun, and Z. Wang, "Security analysis of a chaos-based image encryption algorithm," *Physica A: Statistical Mechanics and its Applications*, vol. 351, no. 2, pp. 645–661, 2005.

P. P. Mar and K. M. Latt, "New analysis methods on strict avalanche criterion of s-boxes," *World Academy of Science, Engineering and Technology*, vol. 48, pp. 150–154, 2008.

E. Biham and A. Shamir, "Differential cryptanalysis of des-like cryptosystems," *Journal of CRYPTOLOGY*, vol. 4, no. 1, pp. 3–72, 1991.

Y. Wu, J. P. Noonan, and S. Agaian, "Npcr and uaci randomness tests for image encryption," *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, pp. 31–38, 2011.

X. Wang, D. Luan, and X. Bao, "Cryptanalysis of an image encryption algorithm using chebyshev generator," *Digital Signal Processing*, vol. 25, pp. 244–247, 2014.

B. Elaine and K. John, "Recommendation for random number generation using deterministic random bit generators," NIST SP 800-90 Rev A, Tech. Rep., 2012.

C.-Y. Song, Y.-L. Qiao, and X.-Z. Zhang, "An image encryption scheme based on new spatiotemporal chaos," *Optik-International Journal for Light and Electron Optics*, vol. 124, no. 18, pp. 3329–3334, 2013.