Microelectronic Engineering 90 (2012) 168–172

Contents lists available at ScienceDirect

Microelectronic Engineering

journal homepage: www.elsevier.com/locate/mee

Chaotic block cryptosystem using high precision approaches to tent map

J.A. Martínez-Ñonthe [a], A. Castañeda-Solís [a], A. Díaz-Méndez [b], M. Cruz-Irisson [a], R. Vázquez-Medina [a,*]

[a] *Instituto Politécnico Nacional, ESIME-Culhuacan, Santa Ana 1000, 04430 México, D.F., Mexico*
[b] *Instituto Nacional de Astrofísica, Óptica y Electrónica, Luis Enrique Erro 1, Tonantzintla, Puebla, Mexico*

ARTICLE INFO

Article history:
Available online 19 April 2011

Keywords:
Chaotic cryptosystem
Block cryptosystem
Chaotic maps

ABSTRACT

This paper presents the implementation and evaluation of a block cryptosystem based in chaotic maps. The noise function used in this cryptosystem is an approximation to the chaotic tent map, and for this reason, it is named pseudo chaotic tent map (PCT map). PCT map has been analyzed and evaluated using the statistical mechanic tools such as: bifurcation diagram, Lyapunov exponent and invariant distribution. In order to determine the influence of PCT map in the syntactic, semantic and statistic of a message, this map has been used on the non-balanced and dynamic network proposed by Kocarev. Cryptosystem has been evaluated using concepts of the information theory, such as: entropy and mutual information. The randomness of the produced cryptograms has been evaluated using the statistical tests suite of NIST.

1. Introduction

Chaotic systems have interesting features, which have a strong tight relationship with cryptography requirements. Thus, it is a natural idea to use chaos to construct cryptosystems. Although a general definition for chaos does not exist applicable to many of the cases of interest, the mathematicians agree that for the special case of iterated transformations, according to Devaney [1] there are three common characteristics of chaos: (a) sensitive dependence on initial conditions, (b) mixing and (c) dense periodic points. The chaos term was coined in 1975 by Li and Yorke [2], but mathematical research in chaos can be traced back at least to 1890 with some great initial ideas, concepts and results of Poincaré [3] when he studied the stability of solar system. Other pioneers followed the trail of Poincaré. In 1960s, Smale formulated a plan to classify all typical types of dynamic behavior. In 1961, Lorenz [4] working on weather simulation models found that simulations results were dramatically different when very small numerical changes were made in initial conditions, which were not expected to affect measurably the behavior of his model. Lorenz [4] used the quadratic equation $y = \alpha x - \beta x^2$ and his description of deterministic chaos goes like this: Chaos occurs when the error propagation grows the same size or scale as the original signal [5].

Another quadratic equation was used in 1947 by Ulam and von Neumann [6] as a source of pseudorandom numbers. This equation is $x_{n+1} = \mu x_n(1 - x_n)$ and was called logistic equation, which was applied in population studies in 1976 by May [7]. Logistic equation was studied by Feigenbaum [8] in 1978 to understand the bifurcation behavior and period doubling regime in a dynamic system. Feigenbaum [8] found that the point which marks the end of the process of bifurcation is the point $\mu_c = 3.5699456\ldots$ and it is known as Feigenbaum constant.

Using the bifurcations diagram and Lyapunov exponent, the disadvantage of logistic equation can be shown when it is used in the pseudorandom numbers generation. This disadvantage is the presence of stability islands, in which the logistic equation produces periodic signals. These stability islands appear according to Charkovsky sequence [9].

There are other equations that can be used to produce pseudorandom numbers which do not have stability islands. These equations are known as piecewise linear maps such as Bernoulli [10] and tent maps [11], which exhibit a reproducible chaotic behavior. Nevertheless, when these chaotic maps are used in a computer, there are other problems that are due to consider. There is at least one initial condition for which chaos is not only sustained but also collapsed; this condition is called "*chaos annulling trap*" (CAT). CAT condition can be achieved as a result of the rounding off done by the computer; due to it, IEEE recommends calculations in double precision. Therefore in this work a map with 16-bits words is used instead of a map with 8-bits words. Similarly, there are other x_0 values that produce a similar condition, which is called "chaos fixed trap" or CFT [12].

2. Model and calculation scheme

The chaotic map considered in this work is the tent map, and it is used to build a pseudorandom noise generator, which is included in a block cryptosystem. The tent map is defined by Eq. (1), where, μ is the control parameter, j is the iteration number of the function f, x_j [0,1] in $\Re$, $0 \leqslant \mu \leqslant 1$ and f:[0,1] → [$(1 - \mu)/2$, $(1 + \mu)/2$].

[*] Corresponding author. Tel./fax: +52 55 5656 2058.
E-mail address: ruvazquez@ipn.mx (R. Vázquez-Medina).

0167-9317/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.mee.2011.04.005

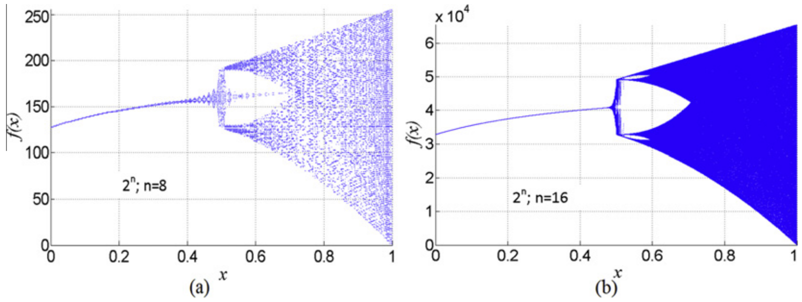


Fig. 1. Comparison of PCT map and its bifurcation diagram when $n = 8$ and 16.

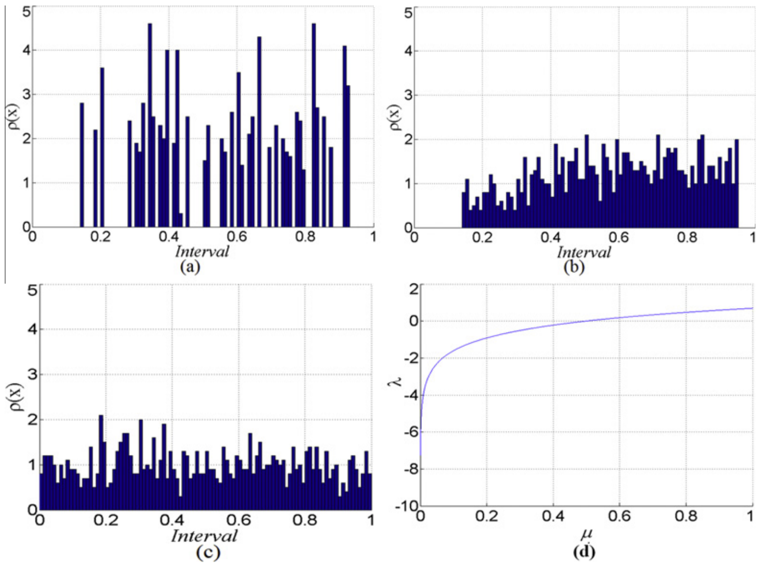


Fig. 2. Statistical distribution of a PCT map, (a) $n = 8$ and (b) $n = 16$ using $\mu = 0.9$ and (c) $n = 16$ using $\mu = 1.0$, and (d) Lyapunov exponent of a PCT map.

$$X_{j+1} = f(x_j) = \mu\left(1 - 2\left|x_j - \frac{1}{2}\right|\right) \tag{1}$$

In order to implement this chaotic map in a computer, this must be scaled and discretized to $[0, 2^n]$, with $n = 8$ or $n = 16$, and it is the precision in each number that uses function f. Thus, a new function must be created, like f': $[0,2^n] \rightarrow [2^n(1-\mu)/2, 2^n(1+\mu)/2]$ in $\Re$, which can be expressed by Eq. (2), where $\lfloor\ \rfloor$ represents the floor or rounding function.

$$F(x) = \begin{cases} \left\lfloor 2\mu x_j + 2^n\left(\frac{1-\mu}{2}\right)\right\rfloor; & 0 \leq_{xj} \leq 2^{n-1} \\ \left\lfloor \mu(2(2^n - x_j) + 2^n\left(\frac{1-\mu}{2}\right))\right\rfloor; & 2^{n-1} \leq x_j \leq 2^n \end{cases} \tag{2}$$

The noise function used in the proposed cryptosystem is an approximation to the chaotic tent map, and it is called pseudo chaotic tent map (PCT map). PCT map has been evaluated using the bifurcation diagram, Lyapunov exponent and invariant distribution. Fig. 1a and b shows that the density of bifurcation diagram is a function of n. Notice that as the value of n increases, a better approach to the chaotic map of tent is obtained.

In order to determine the influence of a PCT map in a plaintext, this PCT map is used on the non-balanced and dynamic network proposed by Kocarev et al. [13] in 2001. The proposed cryptosystem uses blocks with a size of 64 bits, considering 4 sub-blocks with a size of 16 bits each one and a PCT map of 16 bits (PCT-16 map). 16 bits are used in each block because the bifurcation diagram of PCT-16 map is denser than the one generated by a PCT map that uses sub-blocks with a size of 8 bits (PCT-8 map). In this way, a PCT-16 map is a better approach to chaotic tent map than a PCT-8 map. Therefore the statistical distribution of the cryptogram produced with a cryptosystem that uses a PCT-16 map (see Fig. 2b and c) must be a better approach to uniform statistical distribution than the statistical distribution of the cryp-

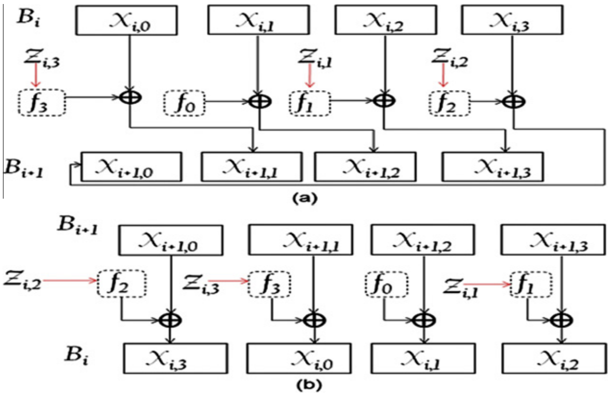
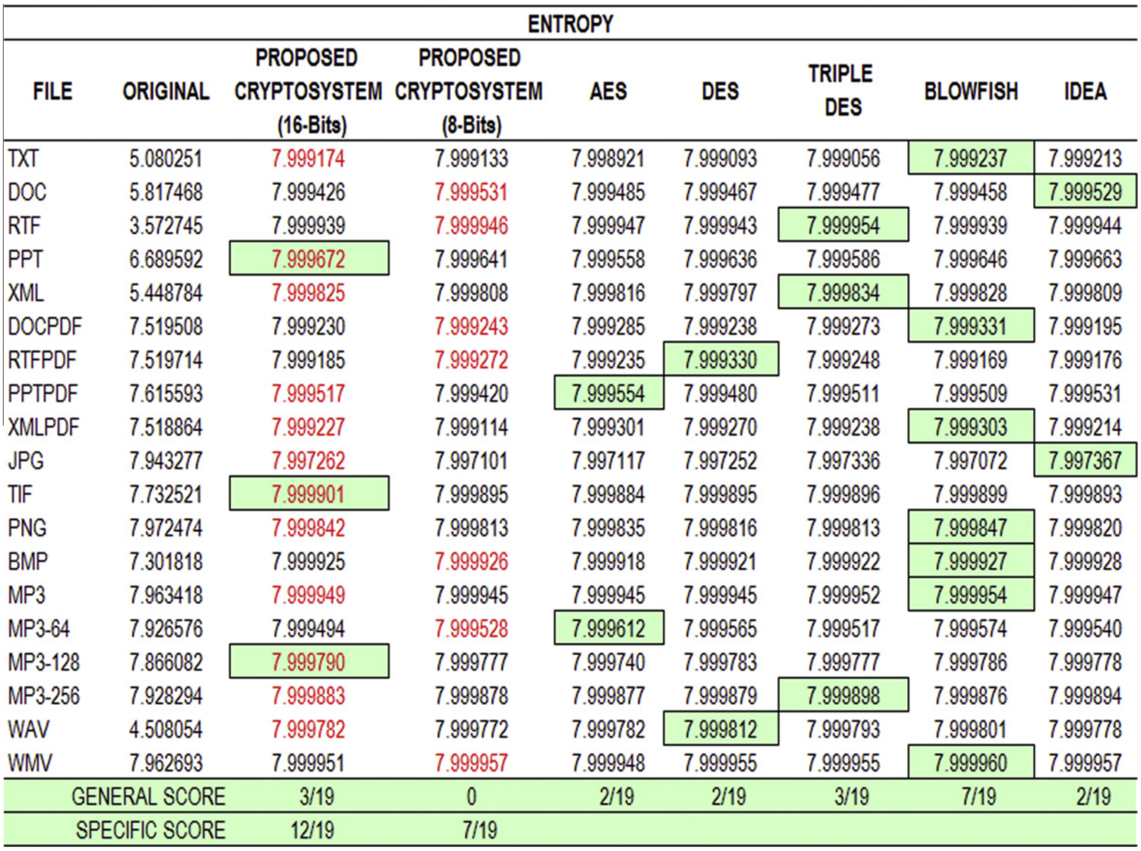


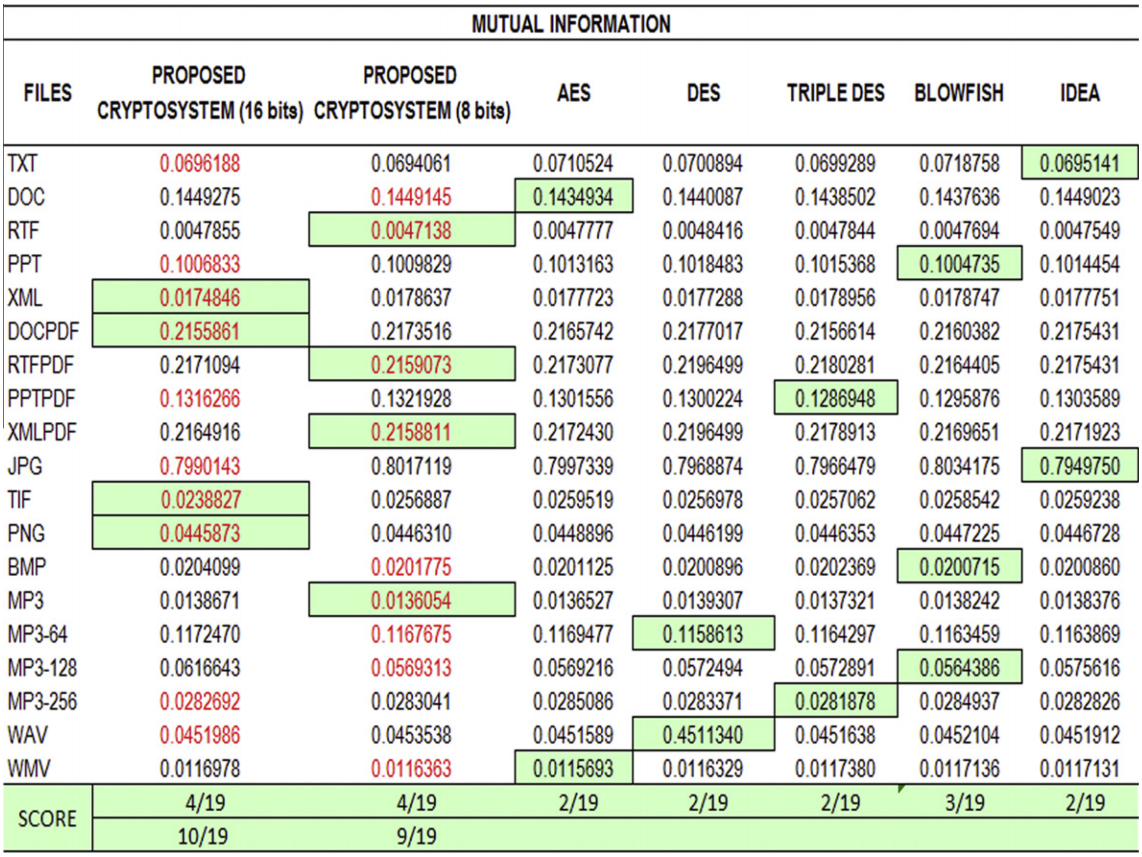
Fig. 3. Block chaotic cryptosystem using PCT-16 map, (a) encryption process, and (b) decryption process.

Table 1
Cryptograms entropy using the proposed cryptosystem (PCT-16 and PCT-8, with $\mu = 1.0$) and the AES, DES, 3DES, BLOWFISH, and IDEA cryptosystems.



ENTROPY								
FILE	ORIGINAL	PROPOSED CRYPTOSYSTEM (16-Bits)	PROPOSED CRYPTOSYSTEM (8-Bits)	AES	DES	TRIPLE DES	BLOWFISH	IDEA
TXT	5.080251	7.999174	7.999133	7.998921	7.999093	7.999056	7.999237	7.999213
DOC	5.817468	7.999426	7.999531	7.999485	7.999467	7.999477	7.999458	7.999529
RTF	3.572745	7.999939	7.999946	7.999947	7.999943	7.999954	7.999939	7.999944
PPT	6.689592	7.999672	7.999641	7.999558	7.999636	7.999586	7.999646	7.999663
XML	5.448784	7.999825	7.999808	7.999816	7.999797	7.999834	7.999828	7.999809
DOCPDF	7.519508	7.999230	7.999243	7.999285	7.999238	7.999273	7.999331	7.999195
RTFPDF	7.519714	7.999185	7.999272	7.999235	7.999330	7.999248	7.999169	7.999176
PPTPDF	7.615593	7.999517	7.999420	7.999554	7.999480	7.999511	7.999509	7.999531
XMLPDF	7.518864	7.999227	7.999114	7.999301	7.999270	7.999238	7.999303	7.999214
JPG	7.943277	7.997262	7.997101	7.997117	7.997252	7.997336	7.997072	7.997367
TIF	7.732521	7.999901	7.999895	7.999884	7.999895	7.999896	7.999899	7.999893
PNG	7.972474	7.999842	7.999813	7.999835	7.999816	7.999813	7.999847	7.999820
BMP	7.301818	7.999925	7.999926	7.999918	7.999921	7.999922	7.999927	7.999928
MP3	7.963418	7.999949	7.999945	7.999945	7.999945	7.999952	7.999954	7.999947
MP3-64	7.926576	7.999494	7.999528	7.999612	7.999565	7.999517	7.999574	7.999540
MP3-128	7.866082	7.999790	7.999777	7.999740	7.999783	7.999777	7.999786	7.999778
MP3-256	7.928294	7.999883	7.999878	7.999877	7.999879	7.999898	7.999876	7.999894
WAV	4.508054	7.999782	7.999772	7.999782	7.999812	7.999793	7.999801	7.999778
WMV	7.962693	7.999951	7.999957	7.999948	7.999955	7.999955	7.999960	7.999957
GENERAL SCORE		3/19	0	2/19	2/19	3/19	7/19	2/19
SPECIFIC SCORE		12/19	7/19					

Table 2
Mutual information of the proposed cryptosystem (PCT-16 and PCT-8, with $\mu = 1.0$) and the AES, DES, 3DES, BLOWFISH, and IDEA cryptosystems.



MUTUAL INFORMATION							
FILES	PROPOSED CRYPTOSYSTEM (16 bits)	PROPOSED CRYPTOSYSTEM (8 bits)	AES	DES	TRIPLE DES	BLOWFISH	IDEA
TXT	0.0696188	0.0694061	0.0710524	0.0700894	0.0699289	0.0718758	0.0695141
DOC	0.1449275	0.1449145	0.1434934	0.1440087	0.1438502	0.1437636	0.1449023
RTF	0.0047855	0.0047138	0.0047777	0.0048416	0.0047844	0.0047694	0.0047549
PPT	0.1006833	0.1009829	0.1013163	0.1018483	0.1015368	0.1004735	0.1014454
XML	0.0174846	0.0178637	0.0177723	0.0177288	0.0178956	0.0178747	0.0177751
DOCPDF	0.2155861	0.2173516	0.2165742	0.2177017	0.2156614	0.2160382	0.2175431
RTFPDF	0.2171094	0.2159073	0.2173077	0.2196499	0.2180281	0.2164405	0.2175431
PPTPDF	0.1316266	0.1321928	0.1301556	0.1300224	0.1286948	0.1295876	0.1303589
XMLPDF	0.2164916	0.2158811	0.2172430	0.2196499	0.2178913	0.2169651	0.2171923
JPG	0.7990143	0.8017119	0.7997339	0.7968874	0.7966479	0.8034175	0.7949750
TIF	0.0238827	0.0256887	0.0259519	0.0256978	0.0257062	0.0258542	0.0259238
PNG	0.0445873	0.0446310	0.0448896	0.0446199	0.0446353	0.0447225	0.0446728
BMP	0.0204099	0.0201775	0.0201125	0.0200896	0.0202369	0.0200715	0.0200860
MP3	0.0138671	0.0136054	0.0136527	0.0139307	0.0137321	0.0138242	0.0138376
MP3-64	0.1172470	0.1167675	0.1169477	0.1158613	0.1164297	0.1163459	0.1163869
MP3-128	0.0616643	0.0569313	0.0569216	0.0572494	0.0572891	0.0564386	0.0575616
MP3-256	0.0282692	0.0283041	0.0285086	0.0283371	0.0281878	0.0284937	0.0282826
WAV	0.0451986	0.0453538	0.0451589	0.4511340	0.0451638	0.0452104	0.0451912
WMV	0.0116978	0.0116363	0.0115693	0.0116329	0.0117380	0.0117136	0.0117131
SCORE	4/19	4/19	2/19	2/19	2/19	3/19	2/19
	10/19	9/19					

Table 3
NIST Statistical test suite.

No.	Test	Proposed cryptosystem pct-16 (p-value)	Conclusion
1	Frequency	0.5955	Random
2	Block-frequency	0.3669	Random
	Cumulative-sums forward	0.9357	Random
3	Cumulative-sums reverse	0.7197	Random
4	Runs	0.9357	Random
5	Longest-runs of ones	0.6579	Random
	Rank	0.3505	Random
7	Spectral fit	0.0428	Random
8	Overlapping-templates	0.7792	Random
9	Non-overlapping-templates	0.4461	Random
10	Universal	0.3345	Random
11	Approximate entropy	0.4012	Random
12	Random-excursions	0.5047	Random
13	Random-excursions-variant	0.3789	Random
14	S9-IJ	0.8669	Random
15	Linear-complexity	0.5955	Random

togram produced with a cryptosystem that uses a PCT-8 map (see Fig. 2a). Fig. 2d shows the Lyapunov exponent (λ) as a function of μ for a PCT with $n = 16$. Note that the map has no stability islands since the λ remains positive once it becomes greater than zero. This situation is desirable in cryptographic applications because $\lambda > 0$ suggests that the sequences produced by a PCT-16 will have a chaotic behavior.

In the proposed algorithm (see Fig. 3) data blocks are represented by $B_i = x_{i,0}, x_{i,1}, x_{i,2}, x_{i,3}$; with $i = 1, 2, 3, \ldots$, and the ciphering process consists of r rounds of the PCT map using the ciphering key applied to each plaintext block. The result of this process is the cryptogram block, $B_{i+1} = x_{i+1,0}$, $\mathrm{x}_{i+1,1}$, $x_{i+1,2}$, $x_{j+1,3}$ (see Fig. 3a). In a similar way, the deciphering process consists of the inverse application of r rounds of the PCT map using the respective deciphered sub key, $z_{i,k}$ and then B_i is obtained of B_{i+1} (see Fig. 3b).

Each round is made up of a non-balanced network that uses a 64-bits sub key. These rounds can be defined as the follow set of transformations:

$$\begin{aligned}
x_{i+1,2} &= x_{i,1} \oplus f_0 \\
x_{i+1,3} &= x_{i,2} \oplus f_1(x_{i,1} \oplus z_{i-1,1}) \\
x_{i+1,0} &= x_{i,3} \oplus f_2(x_{i,1} \oplus x_{i,2} \oplus z_{i-1,2}) \\
x_{i+1,1} &= x_{i,0} \oplus f_3(x_{i,1} \oplus x_{i,2} \oplus z_{i-1,3})
\end{aligned} \tag{3}$$

3. Results

Kocarev proposal uses the logistic map with 8-bits words. But, logistic map has stability islands and, therefore, the proposed cryptosystem uses the piecewise linear chaotic maps designed to process 16-bits words. The growth in the precision with which each symbol is processed in the noise generator tries to reduce the problems of chaos annulling that could occur when the cryptosystem is used in a computer.

The evaluation of the proposed cryptosystem was done using three measures: cryptograms entropy, cryptosystem mutual information and cryptograms randomness. The control parameter used in the PCT-16 map is $\mu = 1$. Nineteen files with different formats and sizes were used. With results shown in Tables 1 and 2, it is possible to quantify the quality of the proposed cryptosystem comparing it with other well-known cryptosystems (AES, DES, 3DES, BLOWFISH, and IDEA). Table 1 refers to the cryptograms entropy, which is used as diffusion measure in the cipher process; that is, it is used to determine the proximity of the cryptogram of being a system with uniform probability, whose entropy is $H_{\mathrm{MAX}} = 8$. This condition tries to reach a high diffusion and confusion in the message, and thus the system will tend to reach the greater uncertainty state. In Table 1, the general score row shows the number of cases in which each cryptosystem has the highest value of entropy. These results show that, without considering the Blowfish cryptosystem, the proposed cryptosystem (together with 3DES cryptosystem) is better in more cases (3/19) than other cryptosystems considered. Entropy behavior of the cryptograms produced by proposed cryptosystem was above the entropy behavior of the cryptograms produced by AES, DES, 3DES and IDEA cryptosystems. To indicate the best case of entropy the cell with the biggest value in each row has been shaded.

Additionally, as it can be seen in Table 1, the cryptosystem with PCT-16 maps is better in 12 of the 19 cases than the cryptosystem with PCT-8 map. To indicate the best case of entropy the biggest value in each column has been written using red text.

Table 2 shows the mutual information of each of the cryptosystems considering the cryptograms obtained from each file type. Mutual information measures the amount of information that contributes on a variable, the knowledge of another one and it is used as a measure of the relationship between plaintext and its respective cryptogram. A cryptosystem can be considered safe if the mutual dependence between cryptogram and plaintext is worth zero. Table 2 shows the number of cases in each cryptosystem that has the lowest value of mutual information. These results show that the proposed cryptosystem (PCT-8 and PCT-16) is better in more cases (4/19) than other cryptosystems considered. Mutual information of the proposed cryptosystem is below the mutual information of AES, DES, 3DES, Blowfish and IDEA cryptosystems. To indicate the best case of mutual information the cell with the shortest value in each row has been shaded. Also, Table 2 shows that the cryptosystem with PCT-16 map is better in 10 of the 19 cases that the cryptosystem with PCT-8 map. To indicate the best case of mutual information the shortest value in each column has been written using red text.

The randomness of the produced cryptograms has been evaluated using the statistical tests suite of NIST. Criteria for characterizing and selecting appropriate noise generators are discussed in [14]. Table 3 shows the results of applying the suite of NIST tests to a specific file, which was ciphered with each one of the different cryptosystems. In order to be able to apply the tests, the ciphered files were binarized in a stream of 100 million bits. In this paper the statistical tests suite of NIST is used to assess if the cryptograms produced by a cryptosystem are apparently random. It is intended that the cryptograms should be unpredictable in the absence of knowledge of the plaintext. Table 3 shows the fact that the proposed cryptosystem acts as a noise generator to the possibility that the plaintext is not known.

4. Conclusions

The proposed cryptosystem was made using tent map, which has not stability islands. 16-bits words are used because the bifurcation diagram of PCT-16 map is denser than the one generated by a PCT-8 map. The statistical distribution of the cryptogram produced with a cryptosystem that uses a PCT-16 map is a better approach to uniform statistical distribution than the statistical distribution of the cryptogram produced with a cryptosystem that uses a PCT-8 map. The proposed cryptosystem can be an alternative that is preferred because the results show that it is a better option than other cryptosystems. Entropy results indicate that the proposed cryptosystem has a comparable performance with 3DES cryptosystem, and is better than AES, DES and IDEA, but has a lower performance than the cryptosystem Blowfish. Mutual information results indicate that the proposed cryptosystem has a comparable performance with the Blowfish cryptosystem, and is better than the AES, DES, 3DES and IDEA cryptosystems. The benefit of using the proposed cryptosystem is to use noise generators with piecewise linear chaotic maps, which produce aperiodic sequences, which does not occur with noise generators built with LFSR or chaotic maps that have stability islands.

Acknowledgments

The authors are grateful to the financial support of the SIP-IPN 20110670 and ICYTDF 270/2010 projects. J.A. Martínez-Ñonthe appreciates the CONACYT scholarship (CVU209959, #202398).

References

[1] R.L. Devaney, An Introduction to Chaotic Dynamical Systems, second ed. Addison Wesley, California, USA, 1989.
[2] T.Y. Li, J.A. Yorke, Amer. Math. 82 (1975) 985–992.
[3] J.D. Biggins, N.H. Bingham, Math. Proc. Camb. Philos. Soc. 110 (1991) 545–558.
[4] E.N. Lorenz, J. Atmos. Sci. 26 (1969) 636–646.
[5] H.O. Peitgen, H. Jürgens, D. Saupe, Fractals For the Classroom Part II: Complex Systems and Mandelbrot Set, Springer Verlag, New York, USA, 1991. pp. 117–118.
[6] S.M. Ulam, J. von Neumann, Bull. Am. Math. Soc. 53 (1947) 1120.
[7] R.M. May, Nature 261 (1976) 459–467.
[8] M.J. Feigenbaum, J. Stat. Phys. 19 (1978) 25–52.
[9] H.O. Peitgen, H. Jürgens, D. Saupe, Fractals For the Classroom Part II: Complex Systems and Mandelbrot Set, Springer Verlag, New York, USA, 1991. pp. 593–594.
[10] D.J. Driebe, Fully Chaotic Maps and Broken Time Symmetry, Kluwer Academic, Dordrecht, Netherlands, 1999.
[11] P. Collett, J.P. Eckmann, Iterated Maps on the Interval as Dynamical Systems. Boston: Birkhauser, 1980.
[12] S.V. Kartalopoulos, Security of Information and Communication Networks, John Wiley & Sons, New Jersey, USA, 2009.
[13] L. Kocarev, G. Jakimoski, Phys. A 289 (2001) 199–206.
[14] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST: SP 800-22 Rev. 1a, Maryland, USA, 2010.