Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 4-B, pp. 1291–1300
DOI : 10.47974/JDMSC-2267

A novel improvement of skew tent map for generating Pseudo random numbers

Raghad Kadhim Salih †
Ali Abd Aubad *
Department of Mathematics
College of Science
University of Baghdad
Baghdad
Iraq

Abstract

An encryption system needs unpredictability and randomness property to maintain information security during transmission and storage. Although chaotic maps have this property, they have limitations such as low Lyapunov exponents, low sensitivity and limited chaotic regions. The paper presents a new improved skewed tent map to address these problems. The improved skew tent map (ISTM) increases the sensitivity to initial conditions and control parameters. It has uniform distribution of output sequences. The programs for ISTM chaotic behavior were implemented in MATLAB R2023b. The novel ISTM produces a binary sequence, with high degree of complexity and good randomness properties. The performance of the ISTM generator shows effective statistical tests and correlation values near to zero, meaning no repeatability, and more random-like behavior. A comparison of ISTM and other chaotic maps was presented which shows the proposed map has greater Shannon entropy, wider chaotic area, higher Lyapunov exponents and it is appropriate for encryption algorithms and hash functions based on chaos.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Skew tent map, Chaotic behavior, PRNG, Lyapunov exponent, NIST statistical tests.*

1. Introduction

Many recent studies have focused on creating hash functions and cryptographic algorithms based on digital chaos as a result of their close relationship with these techniques [1] and [2]. In security applications, chaotic

† *E-mail:* **raghad.saleh2203p@sc.uobaghdad.edu.iq**
* *E-mail:* **ali.Abd@sc.uobaghdad.edu.iq (corresponding Author)**

trajectories are frequently used by algorithms as pseudo random number generators (PRNGs) [3] and [4]. However, due to their finite precision calculation, the chaotic one-dimensional maps do not exhibit ideal chaotic behavior, so they exhibit degraded chaotic properties, including reduced complexity, greater correlation, short chaotic range, poor path distribution, and reduced computational randomness [5]. The skew tent map (STM) is regarded as one of the 1- dimensional piecewise chaotic map that demonstrate limited and weakness chaotic behavior [6].

In this paper, we introduce a new Improved Skew Tent Map (ISTM) that overcomes the limitations and weakness of the classical STM by enhancing sensitivity to initial conditions and parameters, expanding the chaotic range, achieving higher Lyapunov exponents, stronger bifurcation properties, and near-maximum Shannon entropy (≈8). The pseudorandom numbers generated by ISTM were evaluated using linear complexity, NIST randomness tests, and correlation analysis. Comparative studies show that ISTM exhibits superior randomness and robustness against brute-force attacks, making it highly suitable for cryptographic applications and hash functions-based chaos.

This work is ordered as: Section 2 offers on some previous works. Section3 describes the STM while the novel proposed ISTM is presented in section 4. Section 5 covers the chaotic behavior of ISTM. Section 6 discusses ISTM design as PRNG and presented the security analysis of the suggested map. Finally, Section 7 provides the concluding remarks of the paper.

2. Related Work

Hua et al. [7] presented a simple structure to generate many novel 1D chaotic maps which construct of two maps: the first is utilized as a primary map, while the second works as control functions map. It has more intricate structures. Alawida, Samsudin, and Teh [8] created a hybrid chaotic system (HCS) by utilizing combination and cascade methods as a nonlinear chaotic function. Aouissaoui et al. [9] introduced two new 1-dimensional chaotic systems: cubic-tent map (CT) and altered sine logistic tent map (ASLT) by combining simple classical chaotic maps to achieve a wider range of chaotic behaviour. Lawnik and Berezowski [10] presented the dynamical map M-map with a chaotic area ranging from [0.25,0.5]. Umar, Nadeem, and Anwer [6] presented a novel chaotic system depending on the STM utilizing the sine function, with chaotic area [-1, +1)- {0}. In our work, ISTM achieves a balance of complexity and efficiency, as shown in Sections (5) and (6), where it exhibits a significantly wider chaotic range and outperforms existing chaotic maps.

3. Skew Tent Map

The skew tent map (STM) described by equation (1) is a piecewise one-dimensional linear function which generates real numbers within [0,1]. The main problem with STM is that the chaotic region (0,1) is small in size, if the parameters or initial values are not chosen carefully, this causes chaos cancellation [6].

$$x_{n+1} = \begin{cases} \frac{x_n}{r} & if \ \ 0 \leq x_n \leq r \\ \frac{1-x_n}{1-r} & if \ \ r < x_n \leq 1 \end{cases} \quad \text{where} \quad r \in (0,1)\,, n = 0,1,2,\dots \tag{1}$$

4. The Novel Improved Skew Tent Map (ISTM)

This section offers a novel 1D piecewise complicated map based on STM to overcome the clutter limitation of STM. The mathematical representation of improved skew tent map (ISTM) is illustrated in equation (2).

$$f(x_{n+1}) = x_{n+1} = \begin{cases} mod\left(\frac{x_n}{r} + r\,(x_n - 1)\,, 1\right) & if \ \ 0 \leq x_n \leq r \\ mod\left(r x_n + \frac{1-x_n}{1-r}, 1\right) & if \ \ r < x_n \leq 1 \end{cases}, \tag{2}$$

where x_0 is the initial value. In ISTM the control parameter r is expanded from (0,1) to $r \in (-\infty, 0) \cup (0,1) \cup (1, \infty)$ .The suggested function $f\colon [0,1] \to [0,1]$ maintains chaotic behavior, avoiding convergence to periodic or non-chaotic states. Figure 1 depicts the ISTM dynamics with 10^5 iterations.

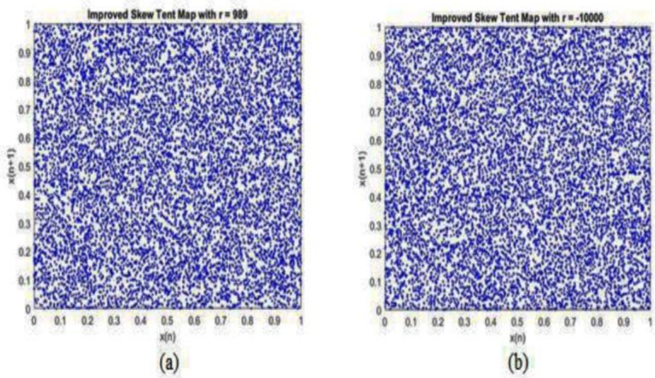

Figure 1
Phase plot of ISTM with $x_0 = 0.1$ when (a) r = 999 and (b) r = -10000

5. Analysis of Chaotic Behaviour

To evaluate the chaotic features of the ISTM, its performance and behavior were analyzed and compared with the classical STM as shown in Figure 2, and with other currently 1D chaotic maps as shown in Table 1, highlighting its effectiveness.

5.1 *Bifurcation Diagram*

The control parameters in chaotic systems define the chaotic behaviour. The STM has a small range of control parameters [6] as illustrated in Figure 2(a). The bifurcation figure of the newly suggested ISTM, offered in Figure 2(b), reveals that the ISTM exhibits chaotic behaviour over a much wider range of control parameters, specifically $r \in (-\infty, 0) \cup (0,1) \cup (1, \infty)$. Additionally, the ISTM uniformly covers the full phase space of its state variables, meaning it has a consistent data distribution along (0, 1). In PRNGs, a wide area of chaotic parameters supplies strong protection and resistance against brute-force attacks.

5.2 *Lyapunov Exponent (LE)*

The classical STM shows a narrow range of positive Lyapunov Exponent (LE) values (Figure 2(c)). In the proposed system, the LE was computed using equation (3) [7] with the results presented in Figure 2(d). The LE remains consistently positive and high across the entire parameter range $r \in (-\infty, 0) \cup (0,1) \cup (1, \infty)$. In contrast, the classical STM and other chaotic maps exhibit a narrow range of positive LE values and chaotic region than ISTM as seen in Table1, where the LE of ISTM increases as the control parameter r increases.

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{j=0}^{n-1} \ln\left(\left|\acute{f}(x_j)\right|\right) \quad (3)$$

where λ is the LE, n is the total number of iterations and $\acute{f}(x_j)$ is the derivative of the map function $f(x)$ in equation (2).

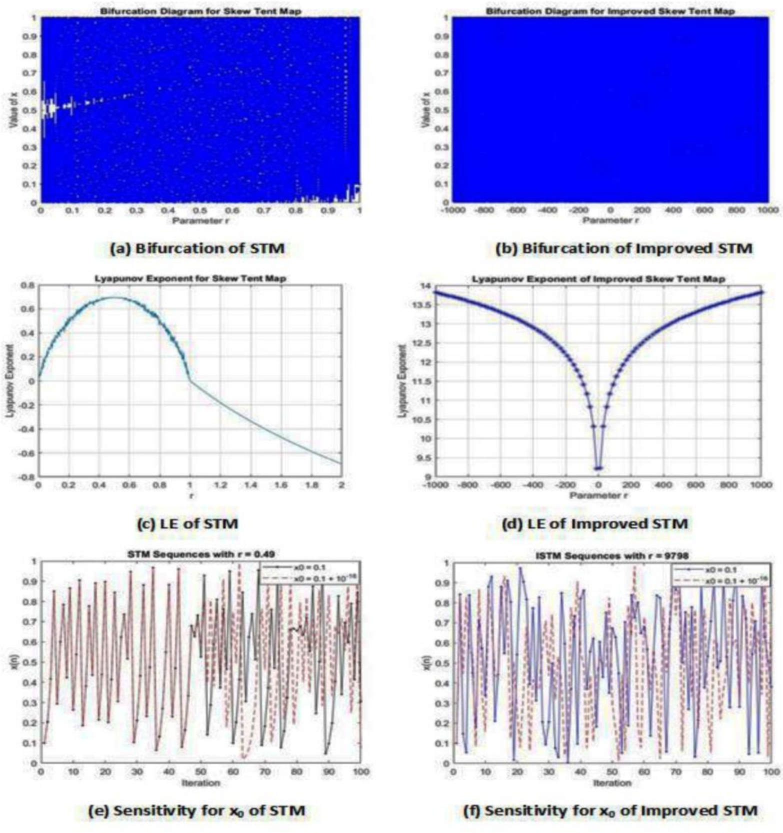

Figure 2 (a-f)
Chaotic Behavior Comparison of STM and Improved STM

5.3 *Sensitivity of ISTM to Initial Values and Parameters*

An ideal chaotic map ensures that even small changes in initial values cause a significant variance in the outcome sequence [6]. To scale the sensitivity of the new ISTM, small change was applied to the initial value, resulting in two distinct trajectories for each them. Figure 2(e) shows the trajectories created by both initial values $x_0 = 0.1$ and $x_0 = 0.1 + 10^{-16}$ with a fixed control parameter r =9798 for ISTM. The ISTM trajectories in Figure 2(f) start to diverge from the beginning while the trajectories of the STM in Figure 2(e) do not start to diverge until iterations 50. In ISTM even teeny changes in the initial values cause noticeable differences in the generated sequences, underscoring the chaotic nature of this map.

5.4 *Cobweb Diagram*

A cobweb diagram is a graphical tool utilized to analyze the qualitative behavior of one-dimensional iterated functions [6]. Figure 3(a) presents cobweb plots of ISTM for x_0 = 0.1and r = 999 which indicates that the trajectories do not coincide, reflecting the high performance of it.

5.5 *Sequence Distribution Analysis*

A histogram represents how often each element occurs within a sequence of numbers. To assess our PRNG, we generated a sequence of 10^6 numbers using ISTM in equation (2) and evaluated its uniformity through the histogram shown in figure 3(b). By dividing the interval [0,1] into 256 bins, the ideal probability per bin was approximately 3906.25. The histogram's average expected count of 3096.2 is close to the ideal, indicating the ISTM generates a uniform distribution, providing strong resistance to statistical attacks.

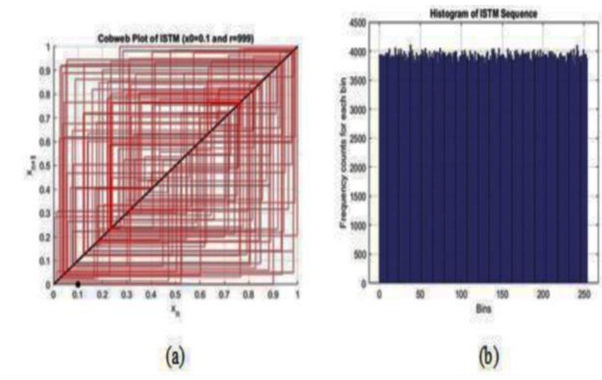

Figure 3
(a) Cobweb diagram of ISTM and (b) The ISTM histogram for r = 999 and x_0=0.1

6. ISTM Design for Pseudo Random Number Generation

Chaotic maps show strong potential for PRNG design as many chaos-based cryptosystems and hash functions use chaotic systems for key generation and boosting randomness. Although directly using chaotic maps as a PRNG may not be the optimal design approach, this work aims to demonstrate the ability of the ISTM when used directly to generate pseudorandom numbers. For this purpose, the threshold function $T(x_n)$ shown in Equation (4) was used to generate binary sequences from ISTM and the security analysis was performed to ensure its robust effectiveness in generating pseudo-random sequences as illustrated below.

$$T(x_n) = \begin{cases} 0 & if\ x_n < 0.5 \\ 1 & if\ x_n \geq 0.5 \end{cases} \tag{4}$$

6.1 *Shannon Entropy*

Shannon Entropy (SE) is a metric utilized to evaluate the randomness of a sequence. A good PRNG should generate sequences that are highly unpredictable, but still deterministic. We calculated the SE by using equation (5), for different control parameters $r \in (-\infty, 0) \cup (0,1) \cup (1, \infty)$ and 10^4 time series. Figure 4(a) illustrates the SE values for ISTM, showing that the proposed map exhibit significantly higher entropy values compared to other maps. The comparison of the ISTM with other existing chaotic maps is presented in Table 1 highlighting the proposed map's effectiveness in terms of LE, chaotic regions, and the mean SE values. Notably, the SE values for the ISTM are approximately equal to ideal value 8.

$$\mathrm{SE} = -\sum_{i=1}^{n} p_i \, log_2\,(p_i) \,, \tag{5}$$

where p_i is the probability with which the trajectory visits the i^{th} subinterval and n is the total number of subintervals.

Table 1
The comparison of ISTM and other chaotic maps with respect to their maximal LE and chaotic regions.

Reference	**Chaotic Map**	**Chaotic Region**	**Max. LE**	**Mean SE**
[9]	Logistic	[3.57, 4]	0.6930	0.9222
[7]	Tent map	(1,2]	0.6931	2.8827
[7]	Sine map	[0.867,1]	0.6850	5.0725
[7]	TCT	[0,2]	0.6504	7.8044
[9]	ASLT map	[0,4]	0.6995	7.9158
[9]	Cubic-Tent	[0,4]	1.0373	7.7239
[10]	M-map	[0.25,0.5]	ln (2)	-
[6]	M-STM	[-1, +1)- {0}	15.98	-
[6]	STM	(0, 1)	0.6951	7.8162
Our work	**ISTM**	$(-\infty, \mathbf{0}) \cup (\mathbf{0}, \mathbf{1}) \cup (\mathbf{1}, \infty)$	$\boldsymbol{\lambda} \to \infty$ $\boldsymbol{as\ r} \to \pm\infty$	**7.9769**

6.2 *Linear Complexity (LC)*

A sequence of length (n) should have a linear complexity that is nearly equal to half its length ($n/2$) in order to be as random as possible. We measured the LC of many PRNGs with varying sequence lengths using the Berlekamp–Massey method [11]. Figure 4(b) offers the LC of binary sequences generated by the proposed ISTM using equation (4) for different lengths. Hence, the results indicate that the LC is too close to *n/2* and it increases steadily.

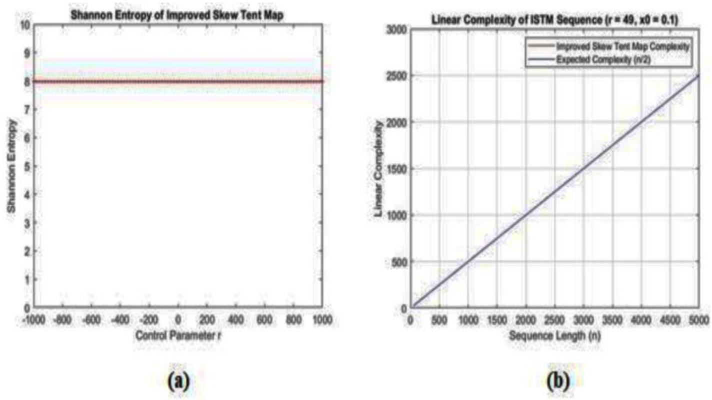

Figure 4
(a) Entropy analysis of ISTM and (b) Linear complexity of ISTM

6.3 *NIST Statistical Suite Tests*

The NIST suite includes 15 tests designed for assessing the randomness for binary sequences [12]. For the NIST tests, the input sequences were derived from 100 different ISTM binary sequences, each with a length of 10^6 bits. All tests produced P-values greater than 0.01, indicating that all 15 NIST randomness tests were successfully passed.

6.4 *Correlation Test*

To quantify the relationship between two chaotic paths, the correlation value is calculated as described in equation (6). In our tests, the correlation values were generated by introducing tiny changes in initial values x_0 and parameters r with 1000 iterations and 500 number sequences is shown in Figures 5 (a) and (b), respectively. It is clear from both figures and Table 2 that the correlation values of the ISTM are very nearly to zero which means there is no relationship between two trajectories. Table 2 compares the average correlation values with those from other chaotic maps.

$$Correlation\ value = \frac{N\sum_{i=0}^{N} xy - \sum_{i=0}^{N} x \sum_{i=0}^{N} y}{\sqrt{\left(N\sum_{i=0}^{N} x^2 - \left(\sum_{i=0}^{N} x\right)^2\right) - \left(N\sum_{i=0}^{N} y^2 - \left(\sum_{i=0}^{N} y\right)^2\right)}} \tag{6}$$

where N is the length of each sequence, x and y are the elements of the two sequences.

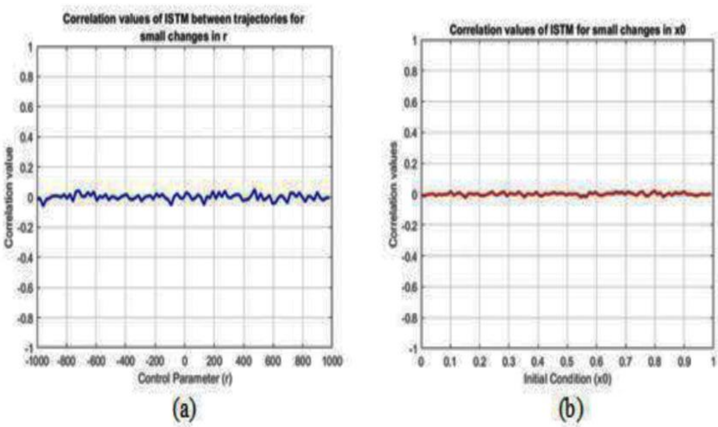

Figure 5
Correlation values of ISTM (a) For teeny changes in parameters *r* where x_0=0.1 and (b) From small changes of initial conditions x_0 where *r* = 999.

Table 2
Correlation values comparisons for different chaotic maps

Reference	**Chaotic Map**	**Mean correlation for small change in x_0. Ideal value (0)**	**Mean correlation for small change in *r*. Ideal value (0)**
[7]	Logistic map	0.07735	0.04012
[7]	Sine map	0.1192	0.01236
[7]	Tent map	0.04755	0.11597
[8]	Logistic-G	0.000429	-
[7]	TCT map	-0.015292	-0.008228
[8]	Sine-G	0.000510	-
	STM	0.000975	0.015677
Our work	ISTM	0.000286	0.000327

7. Conclusions

This work presented a new improved of the skew tent map (STM), called (ISTM). The proposed map overcomes the limitations of the classical STM, as demonstrated in Section 5. The STM exhibits better randomness and higher sensitivity to initial conditions. Furthermore, it has wider chaotic range, higher Lyapunov exponent and greater Shannon entropy compared to STM and other chaotic maps, as seen in Table 1. Statistical tests confirm strong randomness when using the ISTM as a PRNG where bits are directly extracted from its chaotic path to generate sequences. Experimental results from Table 1, Table 2, Figure 3, Figure 5 and correlation analysis show that the ISTM-based PRNG has superior statistical properties and produces independent sequences.

References

[1] A. A. Salih, Z. A. Abdulrazaq, and H. G. Ayoub, "Design and enhancing security performance of image cryptography system based on fixed point chaotic maps stream ciphers in FPGA," *Baghdad Science Journal*, vol. 21, no. 5 (SI), pp. 1754–1764 (2024).

[2] I. A. Taqi and S. M. Hameed, "A new color image encryption based on multi chaotic maps," *Iraqi Journal of Science*, vol. 59, no. 4B, pp. 2117–2127 (2018).

[3] F. F. Saleh and N. H. M. Ali, "Generating streams of random key based on image chaos and genetic algorithm," *Iraqi Journal of Science*, vol. 63, no. 8, pp. 652–3661 (2022).

[4] A. J. Oudah and A. A. Aubad, "Analysing the structure of A4-graphs for Mathieu groups," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 7, pp. 1907–1913 (2021).

[5] L. Liu and S. Miao, "Delay-introducing method to improve the dynamical degradation of a digital chaotic map," *Information Sciences*, vol. 396, pp. 1–13 (2017).

[6] T. Umar, M. Nadeem, and F. Anwer, "A new modified skew tent map and its application in pseudo-random number generator," *Computer Standards & Interfaces*, vol. 89, p. 103826 (2024).

[7] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "A new 1D parameter-control chaotic framework," in Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications, vol. 9030, pp. 180–189, SPIE (2014).

[8] M. Alawida, A. Samsudin, and J. S. The, "Enhancing unimodal digital chaotic maps through hybridization," *Nonlinear Dynamics*, vol. 96, pp. 601–613 (2019).

[9] I. Aouissaoui, T. Bakir, A. Sakly, and S. Femmam, "Improved one-dimensional piecewise chaotic maps for information security," *Journal of Communications*, vol. 17, no. 1, pp. 11–16 (2022).

[10] M. Lawnik and M. Berezowski, "New chaotic system: M-map and its application in chaos-based cryptography," *Symmetry*, vol. 14, no. 5, p. 895 (2022).

[11] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Transactions on Information Theory*, vol. 15, no. 1, pp. 122–127 (1969).

[12] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. Smid, S. D. Leigh, M. Levenson, M. Vangel, N. A. Heckert, and D. L. Banks, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Special Publication 800-22rev1a (2010).

Received February, 2025