Application of high performance one-dimensional chaotic map in key expansion algorithm

Yuxuan Li (liyux2001@163.com)
University of Jinan

Research Article

Keywords: Chaotic map, Lyapunov Exponent, Key expansion algorithm

Posted Date: June 22nd, 2023

DOI: https://doi.org/10.21203/rs.3.rs-3091298/v1

Additional Declarations: No competing interests reported.

Application of high performance one-dimensional chaotic map in key expansion algorithm

Yuxuan Li[1]✉

[1] School of Mathematical Sciences, University of Jinan, Jinan, China

✉ Corresponding author liyux2001@163.com

Abstract

In this paper, we present a key expansion algorithm based on a high-performance one-dimensional chaotic map. Traditional one-dimensional chaotic maps exhibit several limitations, prompting us to construct a new map that overcomes these shortcomings. By analyzing the structural characteristics of classic 1D chaotic maps, we propose a high-performance 1D map that outperforms multidimensional maps introduced by numerous researchers in recent years.

In block cryptosystems, the security of round keys is of utmost importance. To ensure the generation of secure round keys, a sufficiently robust key expansion algorithm is required. The security of round keys is assessed based on statistical independence and sensitivity to the initial key. Leveraging the properties of our constructed high-performance chaotic map, we introduce a chaotic key expansion algorithm.

Our experimental results validate the robust security of our proposed key expansion algorithm, demonstrating its resilience against various attacks. The algorithm exhibits strong statistical independence and sensitivity to the initial key, further strengthening the security of the generated round keys.

Keywords Chaotic map · Lyapunov Exponent · Key expansion algorithm

1 Introduction

With the rapid advancement of information technology, the significance of information security has garnered increasing attention, consequently driving the progress of cryptography. Among various encryption techniques, block ciphers hold a crucial position. In 2000, the Advanced Encryption Standard (AES) emerged as a pivotal block cipher. The AES encryption algorithm consists of multiple encryption rounds, where each round involves XOR operations between round keys and encryption blocks [1].

Chaos is renowned for its sensitivity to initial values and the unpredictable nature of the sequences it generates [2,3]. In recent years, chaotic maps have found extensive applications in the realm of encryption [4-12]. However, traditional low-dimensional chaotic systems exhibit certain shortcomings in cryptographic applications, such as discontinuous chaotic intervals and predictable chaotic signals. To address these issues, researchers have proposed high-dimensional chaotic maps [13-16]. Although higher dimensions result in more complex mapping forms, they also increase computational requirements. Consequently, we draw inspiration from these developments and aim to design a high-performance one-dimensional chaotic map with a simple structure.

In a block cipher algorithm, apart from round key addition, all other steps do not utilize keys. This implies that an attacker could calculate the inverse without possessing the key, underscoring the pivotal role of the round key in ensuring the security of the block cipher. The round key is derived from a key expansion algorithm, thus emphasizing the significance of devising a secure key expansion algorithm. Upon analyzing the key expansion algorithm employed by AES, we observe that it undergoes a reversible serial transformation process. If the round key for any round is known, one can deduce the round key for other rounds or even the initial key. This substantially diminishes the security of block ciphers and exposes vulnerabilities to side-channel attacks and other forms of intrusion. Inspired by the successful applications of chaotic maps in various cryptographic domains, we propose leveraging chaotic maps to generate a more secure key expansion algorithm.

In this study, we introduce a high-performance 1D chaotic map tailored for our key expansion algorithm, drawing insights from the analysis of various classical 1D chaotic map structures. By examining the nonlinear dynamics inherent in our mapping, we showcase its superiority over alternative maps. Subsequently, we put forth a chaotic key expansion algorithm built upon this chaotic map, accompanied by a thorough security analysis.

The subsequent sections of this paper are organized as follows: Section 2 provides an analysis of several well-established classical 1D chaotic maps. In Section 3, we present our high-performance 1D chaotic map, along with an examination of its Lyapunov Exponent and K-Entropy. Section 4 introduces our chaotic key expansion algorithm, while addressing its security considerations. Finally, Section 5 concludes this paper, summarizing the key findings and contributions.

2 Classic 1D chaotic maps

2.1 Logistic map

The Logistic map represents a classical 1D chaotic map, which can be mathematically expressed by Eq. (1) [17].

$$x(i+1) = rx(i)(1-x(i)) \,, \tag{1}$$

where $x \in [0,1]$ is the state variable and $r \in [0,4]$ is the control parameter. Its bifurcation diagram is shown in Fig. 1. When $r \in [3.56995, 4]$, the system enters a chaotic state [17].

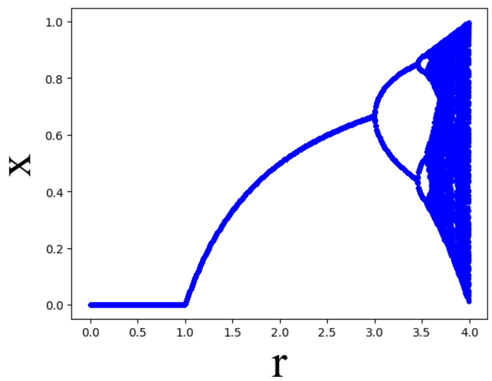

Fig. 1 Bifurcation diagram of the Logistic map

2.2 Quadratic map

The Quadratic map can be mathematically represented by Eq. (2) [18].

$$x(i+1) = r - x(i)^2 \,, \tag{2}$$

where $x \in [-2,2]$ is the state variable and $r \in [0,2]$ is the control parameter. The bifurcation diagram of the Quadratic map is depicted in Fig. 2.

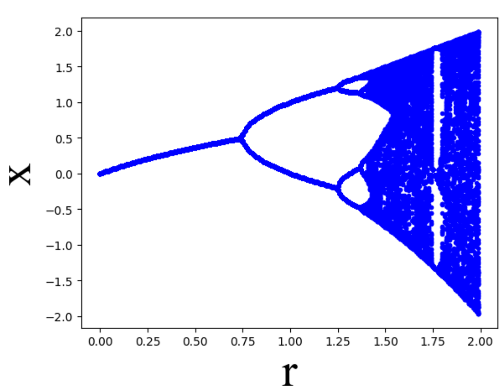

Fig. 2 Bifurcation diagram of the Quadratic map

2.3 Sine map

In addition, we introduce another classical one-dimensional map, known as the Sine map. The Sine map can be mathematically represented by Eq. (3) [19].

$$x(i+1) = r\sin(\pi x(i))\,, \tag{3}$$

where $x \in [-4,4]$ is the state variable and $r \in [0,4]$ is the control parameter. The bifurcation diagram of the Sine map is depicted in Fig. 3.

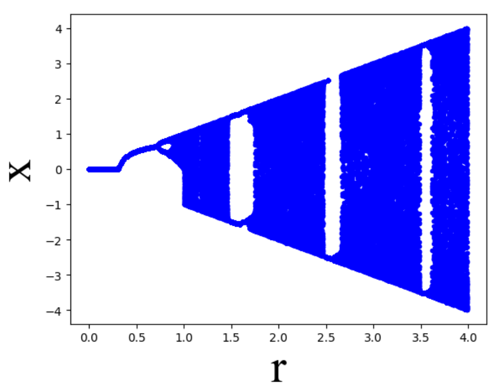

Fig. 3 Bifurcation diagram of the Sine map

3 The proposal of efficient 1D chaotic map and performance evaluations

Upon examining the limitations of the previously introduced classical 1D chaotic maps, it becomes evident that they share common weaknesses, such as discontinuities in the chaotic interval. These maps may exhibit non-chaotic phenomena, including fixed points, at certain control parameter values. Consequently, the predictability of chaotic signals restricts their applicability in cryptography. Our objective is to overcome these limitations without increasing the dimensionality of the map.

We embark on improving the structure of the existing 1D map by leveraging the inherent characteristics of nonlinear components. Chaos, as a typical nonlinear phenomenon in iterative maps, necessitates the presence of nonlinear components that eliminate the superposition effect. The sine map, a classical nonlinear component, effectively constrains the range of state variables. Additionally, the tangent map displays exceptional sensitivity to changes in initial values within specific ranges, making it an ideal candidate for constructing chaotic maps.

By amalgamating these existing structures and incorporating both the sine map and the tangent map, we propose a high-performance 1D chaotic map, mathematically expressed by Eq. (4).

$$x(i+1) = \sin(\tan(r^2(r - x(i)^2))) , \tag{4}$$

where $x \in [-1,1]$ is the state variable and $r \in [0, 3\times10^4]$ is the control parameter. We have named this new chaotic map the 1D-sin-tan-quadratic chaotic map (1D-STQCM). The bifurcation diagram of the 1D-STQCM is presented in Fig. 4, demonstrating its ability to exhibit chaos across a significantly wider parameter range. In the subsequent analysis, we delve into the dynamical performance of the 1D-STQCM, evaluating its key characteristics and properties.

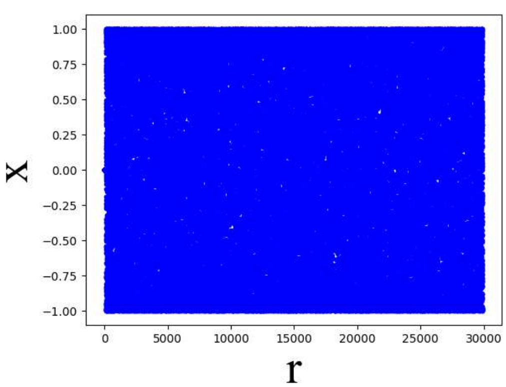

Fig. 4 Bifurcation diagram of 1D-STQCM

3.1 Lyapunov Exponent

The Lyapunov Exponent serves as a crucial index for describing the stability and chaotic properties of dynamical systems. It quantifies the rate at which adjacent orbits in phase space diverge, thus capturing the system's sensitive dependence. This measure is commonly employed to analyze nonlinear dynamical systems, particularly those exhibiting chaotic behavior [20]. Chaotic systems display a high degree of sensitivity to initial conditions, where small perturbations can lead to significant deviations in system behavior. The Lyapunov Exponent effectively captures this sensitive dependence and provides insights into the stability and chaotic nature of the system.

Typically, the Lyapunov Exponent is expressed as a real number or a set of real numbers. Each index corresponds to a specific direction within the system, describing the rate of separation along that particular direction. A positive Lyapunov Exponent indicates exponential divergence between adjacent orbits, indicating chaotic behavior. Conversely, a negative Lyapunov Exponent suggests exponential convergence between adjacent orbits, indicating stability. A Lyapunov Exponent of zero signifies linear separation or convergence, indicating bounded behavior within the system.

It is worth noting that the Lyapunov Exponent is a statistical measure that is not sensitive to the specific evolution path of the system. It is typically obtained by calculating an average value and can be estimated using numerical simulation or mathematical analysis methods. In other words, a larger positive Lyapunov Exponent indicates a more pronounced chaotic performance. Ref. [21] provides a method for computing the Lyapunov Exponent, expressed by Eq (5).

$$LE = \lim_{x \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left| f^{'}(x_i) \right|, \tag{5}$$

where LE denotes the Lyapunov Exponent and $f(x_i)$ is the time series of length n generated by the chaotic system. The curve illustrating the Lyapunov Exponent of the 1D-STQCM in relation to the control parameter is presented in Fig. 5. Furthermore, a comparison between the maximum Lyapunov Exponent of the 1D-STQCM and other chaotic maps is presented in Table 1. Notably, despite being one-dimensional, the dynamic performance of the 1D-STQCM surpasses that of more recent three-dimensional maps, as evident from the table.

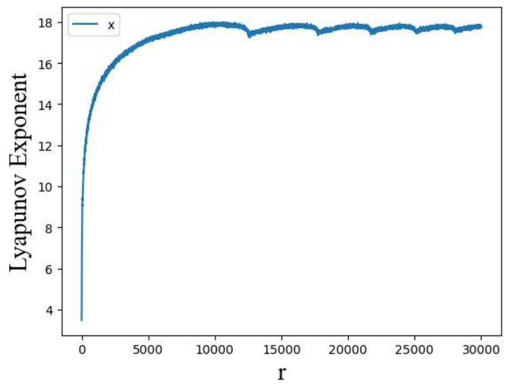

Fig. 5 Lyapunov Exponent of 1D-STQCM

Table 1 A comparison of the maximum K-Entropy and maximum Lyapunov Exponents of 1D-STQCM with other maps.

Map	Max Lyapunov Exponent	Max K-Entropy
Logistic map	0.6929	0.3456
Quadratic map	0.7025	0.2876
Sine map	0.6919	0.3791
ICQM [22]	15.2462	0.8862
EQM [23]	16.6540	1.4343
3D-ICQM [24]	17.1231	0.6893
3D-ECM [25]	16.9166	0.9238
1D-STQCM	17.9990	1.4440

3.2 K-Entropy

In discrete chaotic systems, K-Entropy serves as a vital concept for measuring the complexity and uncertainty inherent in the system. It stems from the notion of entropy, which is a fundamental concept in information theory used to quantify the uncertainty of random variables. In the context of discrete random variables, entropy describes the average amount of information present. In discrete chaotic systems, K-Entropy extends the concept of entropy to discrete variable sequences. It characterizes the rate at which information grows during the dynamic evolution of discrete chaotic systems.

The calculation method for K-Entropy involves dividing the state sequence of the system into different subsequences of length K. Subsequently, the entropy of each subsequence is computed, and the average of these entropies is determined. This average reflects the overall rate of information growth within the system. The value of K-Entropy is typically directly linked to the complexity and chaotic nature of the system. In a simple periodic system, the K-Entropy value may be low as the entropy of the sequence tends to remain stable. However, in a chaotic system, characterized by high sensitivity and uncertainty, the K-Entropy value tends to be higher due to the rapid increase in sequence entropy.

Ref. [26] provides a method for calculating K-Entropy, as expressed in Eq. (6).

$$KE = -\lim_{\tau\to 0}\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n\tau}\sum_{i_1,i_2,\ldots,i_n} p(i_1,i_2,\ldots,i_n)\ln(p(i_1,i_2,\ldots,i_n)), \tag{6}$$

where n is the embedding dimension, τ denotes the time delay, p is the joint probability.

The K-Entropy of the 1D-STQCM is illustrated in Fig. 6, revealing that with the appropriate selection of control parameters, our map exhibits a significantly high K-Entropy. This characteristic renders the generated chaotic sequence highly unpredictable. The superiority of the 1D-STQCM in terms of K-Entropy is also demonstrated in Table 1, further highlighting its advantages over other chaotic maps.

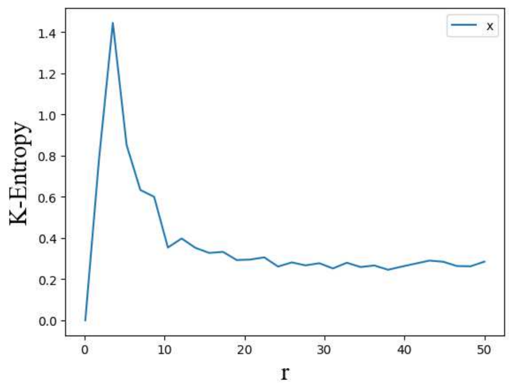

Fig. 6 K-Entropy of 1D-STQCM

4 Key expansion algorithm based on 1D-STQCM and its security analysis

4.1 Proposed key expansion algorithm

Our proposed key expansion algorithm targets the AES encryption algorithm structure with a key length of 128 bits, which encrypts the block for 10 rounds, so our key expansion algorithm will produce 10 round keys with a length of 128 bits. For other structures of block ciphers, the corresponding key expansion algorithm can be obtained by making simple changes. Before presenting the algorithm, we first make some notational conventions. We agree that a word is 4 bytes, that is, 32 bits, and use the array $\mathrm{IK}[0{:}3]$ to represent the initial key of 4 words, and the array $w[0:43]$ to represent the 11 keys including the initial key and the 10 round keys of 44 words. Both initial and round keys are expressed in hexadecimal. Our proposed key expansion algorithm is denoted by Algorithm 1. We need computers with high floating-point precision to better exploit the performance of 1D-STQCM and thus obtain better properties in key expansion.

Algorithm 1: Key expansion Algorithm based on 1D-STQCM

Input: $\mathrm{IK}[0{:}3]$.

Output: $w[0:43]$.

Initial:

Let $x[0:3] = \mathrm{IK}[0{:}3]$;
Set $w[0:3] = \mathrm{IK}[0{:}3]$;
Set control parameter $r = \max(hex2dec(w[0]), 5)$, 1D-STQCM uses this control parameter.
if $w[0] \oplus w[1] \oplus w[2] \oplus w[3] =$ all zeros **do:**
  $w[0] = w[0] \oplus 36118107$ **// Any number that can eliminate the symmetry will do.**
end if
for i=0, 1, 2, 3 do:
  $x[i] = \dfrac{hex2dec(x[i])}{16^8 - 1}$;
end for
for i=1, …, 100 do:
  for j=0,..,3 do:
    $x[j]$=1D-STQCM($x[j]$);
  end for
end for

for i=4, …, 43 do:
  for j=0,..,3 do:
    $x[j]$=1D-STQCM($x[j]$)
  end for
  $temp = x$;
  for j=0,..,3 do:
    $temp[j] = dec2hex(10^{16} \times x[j] \bmod 16^8)$
  end for
  The bitwise XOR operation of the components of $temp$ assigns the result to $w[i]$;
end for
Output w

Given an initial key, the result of a key expansion is shown in Table 2. Then we analyze the security of the proposed key expansion algorithm.

Table 2 An instance of key expansion using our algorithm.

Round	Round Key
0(Initial key)	0F1571C947D9E8590CB7ADD6AF7F6798
1	7E65712BD13C4285394244BF3CD8CD6A
2	6CBA147DC3B2589D2F295666DAD889C6
3	A7E1DDD08BC2C60133BE18EC73E3F520
4	71B47C1D4E443387BCA43F77EF2C3B24

5	31E3C53F7AF4C192AE6AC7158964CB1B
6	DBDA0082A00868D6604088EBEDE96A55
7	049DCCED770C74A74EA5BE07E8C4B0CA
8	64410DFEE40BCAF9C87E1AE0708E5F46
9	0038AC193043977FB89955FF4EB2749A
10	AD7E9A30FDE653E59C96AD3735F8B38E

4.1 Independence of the round key

To verify the independence of the round key, we need to calculate the number of bit change rate (NBCR). The ideal value of NBCR is 50%, meaning that the round key is independent [27]. To compute NBCR we first compute the Hamming distance, since NBCR is equal to the Hamming distance of two sequences divided by the bit length of the sequence. The Hamming distance between two sequences is defined as different bits in binary. We generated 10,000 round keys from an initial key according to our algorithm, counted the Hamming distance between these round keys and the initial key, and drew the histogram as shown in Fig. 7.

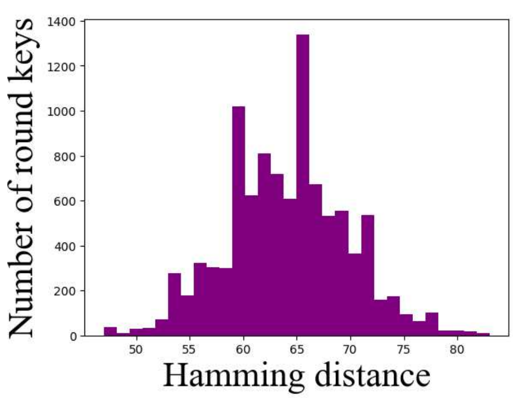

Fig. 7 Distribution of Hamming distance between 10000 round keys and the initial key.

The Hamming distance divided by the key length, that is, divided by 128 bits, yields the NBCR. Naturally we can plot the NBCR distribution of 10000 round keys as shown in Fig. 8. It can be seen that the NBCR of round keys is close to the ideal value of 50%, which indicates that round keys are independent.

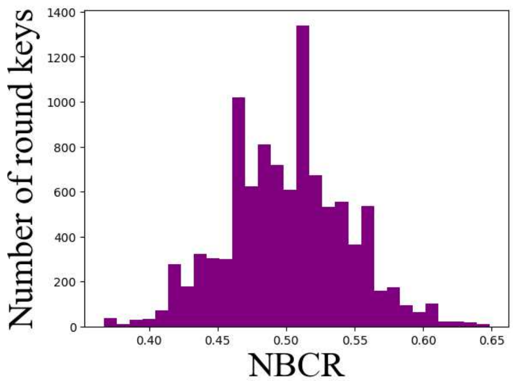

Fig. 8 Distribution of NBCR of 10000 round keys.

4.2 Strict avalanche criterion

After testing the independence of the round key, we also need to test the sensitivity of the key expansion algorithm to the initial key, which manifests as a strict avalanche effect. A strict avalanche effect means that any bit of the initial key is reversed, with a 50% probability for every bit of the round key [28]. We reverse the 1 bit of the initial key in Table 2, apply the key expansion algorithm to obtain 10 round keys, and for each round, calculate the Hamming distance between the corresponding round keys, and the results are shown in Table 3. It can be seen that the Hamming distance between each pair of corresponding round keys is about half of the key length, indicating that our key expansion algorithm satisfies the strict avalanche effect, thus proving the sensitivity to the initial key.

Table 3 Hamming distance between corresponding round keys.

Round	Value	Hamming distance
0(Initial key)	1F1571C947D9E8590CB7ADD6AF7F6798	1

1	36BB7A50B2A3171CE7DCAB909A932D62	70
2	D22D7D34E9B177315B55A3AAFF6F7233	73
3	5C1C3333FD2FEDE4337D554A627E201A	73
4	8AC50398B7B8CF5C59100F2F7D5B8A44	74
5	AD46D24D3417AA4C26ACE0569CCE0BD6	63
6	9657AD31928AF6BAC5C3BC19A9F43C03	61
7	650DBFF33F1CC53179C5B984E0121E8F	52
8	5C75A3B9344C8C96208B94E584DD1CA9	66
9	80910E3ACF17C565DDFE4F0460175354	64
10	31EA9CB8BA229F56E558A606E4F5C4DD	60

4.2 Diffusion and confusion analysis

The combination of confusion and diffusion is considered a fundamental element in achieving the security of cryptographic algorithms. The effects of confusion and diffusion work together to reinforce each other, making the security of cryptographic algorithms more robust. In key expansion algorithms, diffusion can be understood as the idea that small changes in the initial key can be spread out and mixed in the round key by distributing each bit of information in the initial key to as many positions as possible. Based on previous experiments, our key expansion algorithm is sensitive to the initial key and satisfies the diffusion effect.

Confusion, on the other hand, can be understood as creating a highly complex and unpredictable relationship between the initial key and the round key, by making the relationship between the initial key and the round key confusing and complicated. To implement the confusion effect, we use highly unpredictable chaotic mapping in our key extension algorithm.

4.3 The ability to resist side channel attacks

A side-channel attack [29] is a method employed in cryptanalysis that utilizes the physical information leakage arising from the execution of encryption operations by an encryption device, rather than directly attempting to crack the encryption algorithm, in order to obtain sensitive information. The fundamental concept behind a side-channel attack is that the internal state of the encryption device exhibits various physical characteristics, such as changes in power consumption and electromagnetic radiation, during the execution of encryption operations. These physical characteristics are correlated with the device's internal operation process and data, which can be monitored and recorded by specialized devices or sensors. By collecting a significant amount of side-channel data, an attacker can employ statistical analysis, pattern recognition, and other techniques to infer the round key utilized by the encryption algorithm.

Based on our previous analysis, the keys generated by our key expansion algorithm are independent, and even if an attacker manages to obtain a round key, they cannot deduce the initial key. Therefore, our key expansion algorithm effectively withstands side-channel attacks.

4.4 Ability to resist differential attacks

Differential attack is another commonly used method in cryptanalysis. It aims to obtain key information, such as the key or plaintext, by analyzing the output differences of cryptographic algorithms when subjected to different input differences [30]. The fundamental concept behind a differential attack is to select a pair of input plaintexts with a small difference between them and observe the resulting output difference during the algorithm's execution. By repeating this process multiple times, collecting a large number of differential pairs, and performing counting and analysis, an attacker can infer certain bits of the key or the internal state of the algorithm.

The key expansion algorithm satisfies the strict avalanche effect, and the change of initial key does not cause the characteristic difference of round key, which can effectively resist differential attacks.

5 Conclusion

In this study, we have proposed a high-performance 1D chaotic map, named 1D-STQCM. The Lyapunov Exponent and K-Entropy tests conducted on 1D-STQCM have demonstrated its robust performance. Furthermore, our key expansion algorithm generates round keys that exhibit independence from the initial key and sensitivity to changes in the initial key. These characteristics address the limitations found in many existing key expansion algorithms, including the AES key expansion algorithm, and provide effective resistance against side-channel attacks and differential attacks. In the future, the application of 1D-STQCM can be extended to various domains, such as information encryption, random number generation, and the construction of strong S-boxes. The versatility and security properties of 1D-STQCM make it a promising tool for enhancing security measures in these areas.

Data Availability No data was used in this paper.

Declarations None.

Conflict of interest All authors have no relevant financial or non-financial interests to disclose.

Ethical approval All authors accept ethical responsibility.

Inform consent All the authors agreed to submit the manuscript.

References

1. Masoumi, M.: A highly efficient and secure hardware implementation of the advanced encryption standard. J. Inf. Secur. Appl. **48**, 102371 (2019) https://doi.org/10.1016/j.jisa.2019.102371
2. Chen, S., Yu, S., J, L., Chen, G., He, J.: Design and FPGA-based realization of a chaotic secure video communication system. IEEE Trans. Circuits Syst. Video Technol. **28**(9), 2359-2371 (2018) https://doi.org/10.1109/TCSVT.2017.2703946
3. Wu, S., Li, Y., Li, W., Li, L.: Chaos criteria design based on modified sign functions with one or three-threshold. Chinese J. Electron. **28**(2), 364-369 (2019) https://doi.org/10.1049/cje.2018.02.001
4. Liu, X., Tong, X., Wang, Z., Zhang, M., Fan, Y.: A novel devaney chaotic map with uniform trajectory for color image encryption. Appl. Math. Model. **120**, 153-174 (2023) https://doi.org/10.1016/j.apm.2023.03.038
5. Elsadany, A.A., Hussein, S., Al-khedhairi, A., Elsonbaty, A.: On dynamics of 4-D blinking chaotic system and voice encryption application. Alex. Eng. J. **70**, 701-718 (2023) https://doi.org/10.1016/j.aej.2023.03.024
6. Zhou, S., Wang, X., Zhang, Y.: Novel image encryption scheme based on chaotic signals with finite-precision error. Inf. Sci. **621**, 782-798 (2023) https://doi.org/10.1016/j.ins.2022.11.104
7. John, S., Kumar, S.N.: 2D Lorentz chaotic model coupled with logistic chaotic model for medical image encryption: Towards ensuring security for teleradiology. Procedia Comput. Sci. **218**, 918-926 (2023) https://doi.org/10.1016/j.procs.2023.01.072
8. Liang, B., Hu, C., Tian, Z., Wang, Q., Jian, C.: A 3D chaotic system with multi-transient behavior and its application in image encryption. Phys. A: Stat. Mech. Appl. **616**, 128624

(2023) https://doi.org/10.1016/j.physa.2023.128624

9. Lai, Q., Chen, Z.: Grid-scroll memristive chaotic system with application to image encryption. Chaos Solit. Fractals. **170**, 113341 (2023) https://doi.org/10.1016/j.chaos.2023.113341
10. Zhu, S., Deng, X., Zhang, W., Zhu, C.: Secure image encryption scheme based on a new robust chaotic map and strong S-box. Math. Comput. Simul. **207**, 322-346 (2023) https://doi.org/10.1016/j.matcom.2022.12.025
11. Sriram, B., Ghaffari, A., Rajagopal, K., Jafari, S., Tlelo-Cuautle, E.: A chaotic map with trigonometric functions: Dynamical analysis and its application in image encryption based on sparse representation and convolutional filters. Optik **273**, 170379 (2023) https://doi.org/10.1016/j.ijleo.2022.170379
12. Liu, L., Wang, J.: A cluster of 1D quadratic chaotic map and its applications in image encryption. Math. Comput. Simul. **204**, 89-114 (2023) https://doi.org/10.1016/j.matcom.2022.07.030
13. Cao, W., Cai, H., Hua, Z.: n-Dimensional Chaotic Map with application in secure communication. Chaos Solit. Fractals. **163**, 112519 (2022) https://doi.org/10.1016/j.chaos.2022.112519
14. Shahna, K.U.: Novel chaos based cryptosystem using four-dimensional hyper chaotic map with efficient permutation and substitution techniques. Chaos Solit. Fractals. **170**, 113383 (2023) https://doi.org/10.1016/j.chaos.2023.113383
15. Peng, Y., He, S., Sun, K.: A higher dimensional chaotic map with discrete memristor. Int. J. Electron. Commun. **129**, 153539 (2021) https://doi.org/10.1016/j.aeue.2020.153539
16. Wang, L., Sun, K., Peng, Y., He, S.: Chaos and complexity in a fractional-order higher-dimensional multicavity chaotic map. Chaos Solit. Fractals. **131**, 109488 (2020)

https://doi.org/10.1016/j.chaos.2019.109488

17. Boriratrit, S., Fuangfoo, P., Srithapon, C., Chatthaworn, R.: Adaptive meta-learning extreme learning machine with golden eagle optimization and logistic map for forecasting the incomplete data of solar irradiance. Energy and AI. **13**, 100243 (2023) https://doi.org/10.1016/j.egyai.2023.100243
18. Si, Y., Liu, H., Chen, Y.: Constructing a 3D Exponential Hyperchaotic Map with Application to PRNG. Int. J. Bifurcat. Chaos. **32**(7), 2250095 (2022) https://doi.org/10.1142/S021812742250095X
19. Belazi, A., El-Latif, A.A.A.: A simple yet efficient S-box method based on chaotic sine map. Optik **130**, 1438-1444 (2017) https://doi.org/10.1016/j.ijleo.2016.11.152
20. Briggs, K.: An improved method for estimating Liapunov exponents of chaotic time series. Phys. Lett. A. **151**(1), 27-32 (1990) https://doi.org/10.1016/0375-9601(90)90841-B
21. Li, D., Li, J., Di, X.: A novel exponential one-dimensional chaotic map enhancer and its application in an image encryption scheme using modified ZigZag transform. J. Inf. Secur. Appl. **69**, 103304 (2022) https://doi.org/10.1016/j.jisa.2022.103304
22. Liu, H., Kadir, A., Xu, C.: Cryptanalysis and constructing S-Box based on chaotic map and backtracking. Appl. Math. Comput. **376**, 125153 (2020) https://doi.org/10.1016/j.amc.2020.125153
23. Si, Y., Liu, H., Chen, Y.: Constructing keyed strong S-Box using an enhanced quadratic map. Int. J. Bifurcat. Chaos. **31**(10), 2150146 (2021) https://doi.org/10.1142/S0218127421501467
24. Liu, H., Kadir, A., Xu, C.: Color image encryption with cipher feedback and coupling chaotic map. Int. J. Bifurcat. Chaos. **30**(12), 2050173 (2020) https://doi.org/10.1142/S0218127420501734

25. Liu, B., Xiang, H., Liu, L.: Reducing the dynamical degradation of digital chaotic maps with time-delay linear feedback and parameter perturbation. Math. Probl. Eng. **2020**, 4926937 (2020) https://doi.org/10.1155/2020/4926937
26. Zhu, L., Jiang, D., Ni, J., Wang, X., Rong, X., Ahmad, M., Chen, Y.: A stable meaningful image encryption scheme using the newly-designed 2D discrete fractional-order chaotic map and Bayesian compressive sensing. Signal Process. **195**, 108489 (2022) https://doi.org/10.1016/j.sigpro.2022.108489
27. Hua, Z., Li, J., Chen, Y., Yi, S.: Design and application of an S-box using complete Latin square. Nonlinear Dyn. **104**(1), 807-825 (2021) https://doi.org/10.1007/s11071-021-06308-3
28. Li, L., Liu, J., Guo, Y., Liu, B.: A new S-box construction method meeting strict avalanche criterion. J. Inf. Secur. Appl. **66**, 103135 (2022) https://doi.org/10.1016/j.jisa.2022.103135
29. Fang, M., Xu, K., Yang, T., Meng, F., Yu, C.: AES intermediate variables vulnerability recognition based on side channel attacks. Appl. Res. Comput. **30**, 1536-1539 (2017)
30. Ma, S., Jin, C., Guan, J., Liu, S.: Improved differential attacks on the reduced-round SNOW-V and SNOW-Vi stream cipher. J. Inf. Secur. Appl. **71**, 103379 (2022) https://doi.org/10.1016/j.jisa.2022.103379