A review of Chaotic Maps used for Generating Secure Random Keys

Bahaa Abdulwahid Hameed[1]* and *Ekhlas* k. Gbashi[1]

[1]Computer Science, University of Technology Baghdad, Iraq

Abstract. The fusion of chaos theory and cryptography has yielded a dynamic landscape of innovative solutions for safe random key generation. This paper presents a comparison of several studies conducted in this field, aiming to distill key insights and discern common threads. Amidst the diversity of proposals, a consistent architectural framework emerges, while the true differentiators lie in the selection, configuration, and utilization of chaotic maps. These maps, harnessed for their inherent unpredictability, have a significant impact on how reliable and secure cryptographic systems are. Thus survey highlights the enduring relevance of chaotic maps as versatile tools in the cryptography arsenal. The interplay between mathematical complexity and computational expediency stands as a central theme, illustrating the delicate equilibrium researchers must navigate. As chaos-based cryptographic systems continue to evolve, this analysis serves as a compass for both practitioners and theoreticians, offering insights into the evolving landscape of safe key generation, and the challenges and opportunities that lie ahead.

1 Introduction

Regarding contemporary cryptography, the secure and unpredictable generation of cryptographic keys holds paramount importance. The foundation of confidentiality, integrity, and authenticity in digital communication rests upon the robustness of these keys. In recent years, the integration of chaotic maps into cryptographic key generation has emerged as a captivating avenue to enhance the security and unpredictability of generated keys [1]. Chaotic maps, known for their deterministic yet highly sensitive behavior to initial conditions, exhibit inherent qualities that align well with the requirements of cryptographic applications. The term "chaos" might evoke images of randomness, but in the context of chaotic systems, it refers to a unique type of complex and aperiodic behavior. This characteristic is precisely what renders chaotic maps invaluable in generating secure cryptographic keys [2]. One of the central challenges in cryptographic key generation is the need for true randomness. The use of pseudo-random number generators (PRNGs) in conventional procedures is common. which, despite their name, are deterministic algorithms that produce sequences that can become predictable over time. This predictability introduces vulnerabilities that malicious actors can exploit. In contrast, chaotic maps harness the inherent deterministic chaos to provide a fresh perspective on generating randomness [3]. The introduction of chaos theory to the realm of cryptography offers several advantages. The sensitivity of chaotic systems to initial conditions is very high. Even a slight alteration to the initial parameters can produce remarkably different results. This property contributes to the creation of sequences that, while deterministic, are seemingly random and resistant to prediction. Furthermore, the intricate mathematical underpinnings of chaotic maps enhance the complexity of the generated keys, thereby fortifying their security [4]. This paper embarks on a comprehensive review of the utilization of chaotic maps for the generation of secure random cryptographic keys. Through an examination of the state of research and development in that field, we anticipate to offer a comprehensive grasp of the benefits, drawbacks, and possible uses of using chaotic maps in cryptographic systems. We will delve into the intricacies of various chaotic map types, their properties, and their suitability for generating keys that meet the stringent requirements of modern cryptographic protocols. Through this exploration, we seek to illuminate the promise that chaotic maps hold in advancing the state of cryptographic key generation. By providing a comprehensive view of their significance, we hope to inspire further research and development in this exciting and impactful intersection of chaos theory and cryptography [5].

* Corresponding author: bahaa.a.hameed@gmail.com

2 overview of chaotic system

Chaotic systems are a class of dynamic systems characterized by sensitive dependence on initial conditions, complex interactions, and the emergence of seemingly random actions from deterministic equations. In chaotic systems, over time, even a slight alteration to the initial conditions can produce radically different results, making their long-term behavior appear random and unpredictable [6]. Chaotic systems characterized by their extreme sensitivity to initial conditions. Over time, a small alteration to the system's initial state can produce radically different results. This characteristic, sometimes called the "butterfly effect," illustrates how small perturbations in the system's initial state can lead to significant divergence in its future trajectory [7]. Chaotic systems typically described by nonlinear equations [8]. Nonlinearity introduces complex interactions and feedback loops within the system, giving rise to a wide range of behaviors, including periodic, quasiperiodic, and chaotic motion [9].

Chaotic systems are intricate mathematical constructs that exhibit complex, unpredictable behavior. This behavior harnessed for various applications, including the generation of encryption keys in cryptography. Chaotic systems can also use to extract true randomness from their chaotic trajectories [10]. The chaotic data can be sampled and manipulated to produce high-quality random numbers that suitable for a variety of cryptographic applications. By capitalizing on the sensitive dependence on initial conditions and the apparent randomness of chaotic trajectories, security mechanisms can developed that are resistant to certain types of attacks and provide a higher level of encryption strength [11]. It is important to note that while chaotic maps can be a valuable source of randomness for key generation, their use requires careful implementation and analysis [12]. Factors like the choice of map, parameter selection, and security considerations all influence the effectiveness of the key creation procedure [13]. Additionally, the security of the system relies on keeping the initial condition and other parameters secret from potential attackers [14]. As cryptography evolves, key generation from chaotic maps remains a method of interest to enhancing the security of various communication and data protection applications. Chaotic systems are like mathematical puzzles that show how tiny changes can lead to surprising, unpredictable results [15]. This unpredictability has practical uses, from making secret codes for secure messages to helping us understand things like weather patterns [16]. Chaos reminds us that even in the midst of complexity, there is a hidden order waiting to discovered, holding relevance in fields from science to safeguarding our digital world [17].

3 Literature Review

This literature review dedicated to the investigation of various studies that explore the use of chaotic maps for the generation of random cryptographic keys. Through an in-depth examination of these studies, we aim to shed light on the diverse approaches, methodologies, and findings in this emerging field of cryptography. Through the integration of the knowledge obtained from these investigations, we will acquire a thorough understanding of the suitability and efficiency of chaotic maps as a method for key generation.

In [18], In this research, a novel approach to cryptography based on chaotic maps is introduced. In this innovative technique, confusion and diffusion processes implemented within the spectral domain, specifically on the Discrete Cosine Transform (DCT) coefficients. This method allows for quick encryption without the need for a large number of confusion and diffusion iterations, which are usually necessary in the spatial domain. Additionally, the diffusion pattern generated using a random number generator following a Gaussian distribution. The method leverages the Bakers map and is capable of producing encryption keys with a length of 128 bits, with the potential for further extension. and the simulations and experimental assessments unequivocally demonstrate the following attributes of the proposed image encryption system:

(1) An exceptionally extensive key space,
(2) A heightened susceptibility to variations in secret keys,
(3) An information entropy level closely approximating the ideal value of 8, and
(4) Markedly low correlation coefficients, approaching the desired value of 0. Consequently, The thorough analysis clearly demonstrates the security, effectiveness, and robustness of the suggested image encryption algorithm.

In [19], This work presents a novel symmetric image encryption algorithm that makes use of Henon's chaotic system and creative pixel shuffling to apply byte sequences to images. Image encryption produced by this method is incredibly effective and efficient. By enhancing both confusion and diffusion processes, experimental and statistical analysis demonstrate heightened sensitivity to encryption keys, establishing the proposed image encryption algorithm as a robust solution for enhancing security in digital image transmission. When applied to a test image, this method achieves significantly elevated levels of image security, making encrypted images impervious to cryptanalysis by potential eavesdroppers. The image encryption method combined with a secret key is the foundation of security. Because chaos is inherently random, it guarantees a high degree of security. Relocating pixels from their original positions to new ones results in pixel confusion, whereas byte sequences produced by the Henon map cause diffusion.

In [20], This paper presents a new image encryption technique that relies on chaotic maps and affine transformations. It introduces an efficient encryption scheme based on chaos, boasting an increased key space. Notably, a single encryption round significantly enhances the range of available keys. This method eliminates pixel correlations in the image by using random chaotic sequences and employing simple XOR and addition operations. To enhance the system's resilience against potential attacks, an affine transformation is included to generate the final encrypted image. The security of this proposed method confirmed through a comprehensive analysis, covering aspects such as histogram, contrast, PSNR (Peak Signal-to-

Noise Ratio), entropy, correlation, key space, key sensitivity, and differential attack. Leveraging the distinct characteristics of chaotic maps, such as sensitivity to initial conditions, control parameters, structural complexity, and resistance to attacks, the envisioned approach proves to be a reliable, practical, and robust solution for various secure communication applications.

In [21], a work presents a digital voice signal serves as the foundation and a chaotic map harnessed for system implementation. Chaotic maps exhibit a random distribution across their parameter space, offering versatility through discrete time system parameterization. Moreover, these maps possess multiple dimensions, each contributing to a substantial key space. This inherent property endows the proposed system with formidable encryption capabilities when juxtaposed with classical traditional methods or analog scrambling techniques. The outcomes clearly demonstrate that even the slightest alteration in initial conditions renders the recovery of original information nearly impossible. The proposed system exhibits remarkable encryption prowess compared to conventional methods. Upon implementing the XOR chaotic system based on the Hénon map, the results display a colossal key space, measuring 3.8426×10^128, a figure magnified by the square of the parameter range. To further augment the system's key space, the dimension of the chaotic map used in the third method (a comparative approach) of XOR chaotic binary sequence is expanded, thereby reinforcing the encryption's resilience and strength.

In [22], This paper presents a novel method of generating keystreams by merging the 3D Henon map and the 3D Cat map. This method's basic idea is to use the 3D Henon map to generate random numbers, which then transformed into a binary sequence. The 3D Cat map used to perform XOR and permutation operations on these positions within the sequence. The recently developed keystream generator has passed the NIST statistical test suite, indicating its competence. Moreover, security analysis emphasizes its large key space and its high initial condition sensitivity.

In [23] this paper proposes chaotic system exhibits remarkable sensitivity to initial values and system parameters, anchoring its security on a concealed key in conjunction with the image encryption method. Chaos, renowned for its inherent randomness, underpins the robustness of this system. They harnessed the inherent randomness of chaotic techniques, specifically the Arnold cat map and Henon map. The Henon map used to generate the encryption key, and the Arnold cat map is used to shuffling pixels. Importantly, the decryption process mirrors the encryption process, employing the same key for both operations. This approach serves to safeguard data, rendering it inaccessible to unauthorized individuals.

In[24], this study presents a more secure key generation algorithm, utilizing chaos theory and initial key, while significantly reducing processing time. The resultant key then employed in the AES (Advanced Encryption Standard) algorithm. The key generation process involves several steps. Initially, numerous operations performed based on values derived from chaotic equations to generate a 2048-bit sequence. Subsequently, this primitive initial key leverages chaos theory results to create 64 symbols (equivalent to 512 bits), thereby yielding a suitable key characterized by randomness and complexity. The result of the first key generation run through a primitive table to generate an additional 512 bits. The output of the first key and the primitive table then subjected to an XOR operation, which produces an extra 512 bits. These processes result in the formation of a 3584-bit key. Experimental results clearly indicate that the proposed key generation method offers the advantage of a significantly expanded key space, providing robust protection against brute force attacks. Consequently, the findings demonstrate a higher level of protection, underpinned by the strong security features of the strong key.

In [25], The Two-Dimensional Hénon map and the Two-Dimensional Rational map combined in this paper to present a novel method for creating a random key generator. This generator's basic operation is to take the outputs of these two chaotic maps, convert them to 64-bit numbers, and then combine them using XOR and other operations. The resulting random key sequences have undergone rigorous evaluation, including assessment by the NIST test group and traditional statistical methods. A new pseudo-random number generator called the Chaotic Key Number Generator (CKNG) created by taking advantage of the special qualities of chaotic maps. This generator enhances security by employing a multi-level approach with Two-Dimensional Hénon and Two-Dimensional Rational maps. (CKNG) has undergone extensive testing, successfully passing NIST tests. Notable characteristics of the generated keys include a substantial key length (2213 bits), high sensitivity to changes in initial input values, serializability, non-interrelatedness, and robust security against various attacks, including differential and brute-force attacks. This generator exhibits exceptional capacity to produce vast and unlimited pseudo-random sequences, rendering it highly valuable in diverse encryption applications. The combination of chaotic maps with XOR operations disrupts the underlying structure of the initial function, leading to unpredictable randomness. Additionally, its simplicity of implementation makes it an attractive choice. Based on the features and results observed with (CKNG), it is evident that this generator excels in generating extensive pseudo-random numbers suitable for a wide range of encryption applications.

In [26]. This paper presents a chaotic key generator based on the 3D Lorenz system and the 2D Henon map. The initial conditions, represented as (x0, y0) for the 2D Henon chaotic map and (x0, y0, z0) for the 3D Lorenz chaotic system, serve as input. Only floating-point numbers are considered, and specifically, the first four digits from these numbers are used. To enhance randomness, the method involves selecting the first two digits from these four-digit numbers, followed by the remaining two digits. The suggested method shows promise in producing a large number of key sequences that are useful for a variety of cryptographic uses. It guarantees the quality of the generated key sequences, is sensitive to the initial values (keys), and provides a high level of security against various kinds of attacks.

In [27] A two-dimensional hyperchaotic map based on the one-dimensional Hénon and one-dimensional Sine maps was presented in this study. They improved uniformity and randomness by applying a remainder-after-division function, and the outcome was the development of the Two-Dimensional Enhanced Hyperchaotic HénonSine map (2D-EHSHM). This enhanced map demonstrates improved pseudorandom properties compared to the original version, as evidenced by analyses of the Lyapunov exponent, attractor trajectory, bifurcation diagram, histograms, and sensitivity during initialization.

Furthermore, as our analysis has shown, they proposed a novel pseudorandom number generator (PRNG) algorithm that produces 8-bit pseudorandom numbers with a high degree of randomness. The initial conditions and control parameters of this PRNG derived through an indirect seed calculation, which based on a secret key made up of sixty hexadecimal characters. The PRNG-EHSHM subjected to extensive testing, which included a thorough evaluation in comparison to the NIST 800-22 randomness tests, as well as a number of cryptographic security analyses. The evaluations yielded satisfactory results, indicating the possibility of using this PRNG in cryptography, especially in embedded security systems that use inexpensive processors.

In [28], This paper presents an optical cryptosystem with improvements from the gyrator transform and the Hénon chaotic map for meaningful color images. Three levels of security provided by this cryptosystem: security for image appearance, analysis, and content. They have also suggested employing polarization-assisted electro-optical methods to create compact and effective implementations of this cryptosystem. It has shown that the cryptosystem is resilient to a variety of attacks, including statistical and classical ones (like chosen-plaintext and chosen-ciphertext attacks). Furthermore, numerical results highlight how sensitive the suggested scheme is to even small changes in the secret key, rendering decryption impossible in the absence of complete knowledge of the secret key (thereby solving the silhouette problem). It has confirmed that the cryptosystem is resilient to noise and occlusion attacks. Our suggested cryptosystem performs better than other recently developed cryptosystems in terms of resilience and visual security.

In [29], This paper proposes a new method for building a dynamic S-Box that makes use of shifting, a 1D circular map, and the user's 8-character password key. According to the study's findings, the suggested approach creates a secure S-BOX that exhibits 255 distinctions when a single bit of the key is changed, changing about 99% of the S-Box. In addition, an inverse table for the S-Box (16*16) created using the S-Box output produced by the previously mentioned recommendations in order to derive values for each S-Box value based on the intersection of column and row. They assess their S-Box's efficacy using a range of defined performance metrics. Every analysis yields extremely encouraging outcomes, confirming that the created S-Box meets every requirement necessary for trustworthy and safe encryption. This method can applied very quickly—a few milliseconds is all it takes.

In [30], This paper proposes a low-power cryptographic solution to protect the privacy and confidentiality of video data that is transferred over an edge-fog-cloud platform. The proposed cryptographic approach structured into three main phases: preprocessing video frames using the Frame Region of Interest Extraction (FROI) technique, generating and distributing secret keys (SK) through an algorithm, and encrypting and decrypting video data using a 2D chaotic map. Key factors affecting the performance of video encryption within the edge-fog-cloud infrastructure include latency, precision, and feasibility. The secret key generation process implemented in the central fog node (CFN), and key distribution and management processes implemented in the cloud-computing layer to improve the distribution procedure's security. Standard evaluation metrics applied to experimental results in order to examine and evaluate the suggested cryptographic technique. Using the Urban Surveillance Video Dataset (USVD), a number of metrics used to evaluate performance, including the rate of memory consumption, encryption time, decryption time rate, key sensitivity analysis, and computational complexity. The outcomes obtained from these measurements validate the appropriateness of the suggested plan for protecting transmitted video data in the edge-fog-cloud architecture from unwanted access. To emphasize the performance evaluation of the suggested approach, experiments conducted that compare scientifically with the most advanced techniques available. In the end, the results of these empirical comparisons suggest that the suggested protocol is better suited for encrypting video frames as they move from the fog layer to the computing cloud layer.

In [31], This paper presents and investigates a new type of lightweight stream cipher that uses the ChaCha20 algorithm in conjunction with a hybrid chaotic map for video encryption. The key generation process uses two different chaotic maps to help with encryption and permutation tasks, respectively. The ChaCha20 algorithm used to support a symmetric scheme for the encryption and decryption of frame sequences. Testing on a variety of video samples used to evaluate the efficacy of the suggested lightweight stream cipher method and confirms its suitability for both encryption and decryption processes. Metrics used in performance evaluation include correlation analysis, differential analysis, information entropy, histogram analysis, and visual tests. When compared to state-of-the-art encryption techniques, the experimental results show that the suggested lightweight encryption method exhibits higher security with a shorter computation time. To summarize, Table 1 provides a comparative summary of recent research in this area.

Table 1. a comparative analysis of recent studies.

Reference No.	Technique	Number bits of key	Performance
[18]	chaotic maps and affine transformation	128 bits	A high level of security, buttressed by the powerful security mechanisms of the secret key.
[19]	Henon's chaotic system	128 bits	Demonstrates security effectiveness against a multitude of attack types.
[20]	chaotic maps and affine transformation	128 bits	These results establish a

			dependable level of security, fortified by the unyielding security attributes of the secret key.
[21]	Hénon map	256 bits	Ensures security integrity against a variety of attack vectors.
[22]	3D Henon map with the 3D Cat map	128 bits	Ensures security integrity in the face of numerous attack varieties.
[23]	The Henon map and the Arnold cat map.	2320 bits	The evaluations yielded positive results, indicating that this PRNG could be useful in cryptography.
[24]	chaos theory and initial key	3584 bits	The results affirm a robust level of security, fortified by the formidable security attributes of the secret key.
[25]	Hénon map and Two-Dimensional Rational Map.	2213 bits	Generates extensive and limitless pseudo-random sequences, making it invaluable for a wide range of encryption applications.
[26]	2D Henon map and the 3D Lorenz system	2808 bits	Provides robust security against a variety of attack vectors
[27]	1D Hénon map and 1D Sine map	128 bits	Ensures security integrity in the face of numerous attack varieties.
[28]	The gyrator transform and the Hénon chaotic map	224 bits	It has confirmed that the cryptosystem is resistant to noise and occlusion attacks.

4 Conclusion

After conducting an in-depth analysis of numerous studies pertaining to the utilization of chaotic maps in the domain of generating secure random keys, it becomes evident that the fundamental architecture underlying these cryptographic systems exhibits a remarkable degree of consistency across various proposals. this survey underscores the foundational role of chaotic maps as versatile tools in the realm of cryptographic key generation. The variations observed within the literature underscore the adaptability of chaotic systems to diverse applications, while the trade-offs between complexity and efficiency reveal a constant tension in their design. As researchers continue to refine their approaches and explore novel chaotic maps, it is certain that the fusion of chaos theory and cryptography will continue to be a fertile ground for innovative and secure key generation solutions.

References

1. H. Y. Zhengmao, et al, "Security Authentication of Dual Chaotic Image Watermarking in Spatial Domain with Spatial and Frequency Domain Characteristics Analysis" Applied System Innovation, 1(4), (2018).
2. H. Nasry, et al, "Multi Chaotic System to Generate Novel S-Box for Image Encryption", in 11th International Conference on Mathematics and Engineering Physics (ICMEP-11) 2022.
3. O Jallouli, "Chaos-based security under real-time and energy constraints for the Internet of Things", PhD. Thesis,Signal and Image processing, Universite de Nantes, Franc, 2017.
4. Ping, P., Xu, F., Mao, Y., Wang, Z.: Designing permutation-substitution image encryption networks with henon map. Neurocomputing 283, 53–63 (2018).
5. A. Kadhim, "New image encryption based on pixel mixing and generating chaos system", Al-Qadisiyah journal of pure science, (2020).
6. M. S. Fadhil, et al, "Designing Substitution Box Based on the 1D Logistic Map Chaotic", in International Scientific Conference of Engineering Sciences (ISCES 2020).

7. H. Demirci and N. Yurtay, "Effect of the Chaotic Crossover Operator on Breeding Swarms Algorithm", Sakarya University Journal of Computer and Information Sciences, 4(1):120-130, April 2021.
8. T.K. Alshekl,y, E.A. Albhrany, "A New Key Stream Generator Based on 3D Hénon map and 3D Cat map ", IJSER, Vol. 8, pp. 2114- 2120, January 2017.
9. M. S. Azzaz, C. Tanougast, S. Sadoudi, and A. Bouridane, "Synchronized hybrid chaotic generators: Application to real-time wireless speech encryption," Communications in Nonlinear Science and Numerical Simulation, vol. 18, no. 8, pp. 2035–2047, Aug. 2013, doi: 10.1016/j.cnsns.2012.12.018.
10. A. Hasheminejad and M. J. Rostami, "A novel bit level multiphase algorithm for image encryption based on PWLCM chaotic map," Optik, vol. 184, pp. 205–213, May 2019, doi: 10.1016/j.ijleo.2019.03.065.
11. A. Alfalou, C. Brosseau, and N. Abdallah, "Simultaneous compression and encryption of color video imag es," Optics Communications, vol. 338, pp. 371–379, Mar. 2015, doi: 10.1016/j.optcom.2014.10.020
12. H. Elkamchouchi, W. M. Salama, and Y. Abouelseoud, "New video encryption schemes based on chaotic maps," IET Image Processing, vol. 14, no. 2, pp. 397–406, Feb. 2020, doi: 10.1049/iet-ipr.2018.5250.
13. F. Sbiaa, S. Kotel, M. Zeghid, R. Tourki, M. Machhout, and A. Baganne, "A selective encryption scheme with multiple security levels for the H.264/AVC video coding standard," in 2016 IEEE International Conference on Computer and Information Technology (CIT), Dec. 2016, pp. 391–398, doi: 10.1109/CIT.2016.53.
14. P. McLaren, W. J. Buchanan, G. Russell, and Z. Tan, "Deriving ChaCha20 key streams from targeted memory analysis," Journal of Information Security and Applications, vol. 48, Oct. 2019, doi: 10.1016/j.jisa.2019.102372.
15. A. M. Raheema ; S. B. Sadkhan ; S. M. Abdul Sattar, Performance Comparison of Hybrid Chaotic Maps Based on Speech Scrambling for OFDM Techniques", 2018 Third Scientific Conference of Electrical Engineering (SCEE).
16. H. A. Ismael ; S. B. Sadkhan, "Security enhancement of speech scrambling using triple Chaotic Maps", 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT).
17. F. Özkaynak, "Cryptographically secure random number generator with chaotic additional input," Nonlinear Dyn., 2014.
18. Shoaib Ansari, Prof. Neelesh Gupta, Prof.Sudhir Agrawal, A Review on Chaotic Map Based Cryptography, International Journal of Scientific Engineering and Technology,2012.
19. Shoaib Ansari , Neelesh Gupta , Sudhir Agrawal, An Image Encryption Approach Using Chaotic Map in Frequency Domain, 2012.
20. N. S. RAGHAVA & ASHISH KUMAR, IMAGE ENCRYPTION USING HENON CHAOTIC MAP WITH BYTE SEQUENCE, International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) ISSN(P): 2249-6831; ISSN(E): 2249-7943 Vol. 3, Issue 5, Dec 2013, 11-18.
21. Amina Mahdi, Saad Saffah Hreshee, Design and implementation of voice encryption system using XOR based on Hénon map, DOI: 10.1109/AIC-MITCSA.2016.7759915,2016.
22. Ekhlas Abbas Albahrani, Tayseer Karam Alshekly, A New Key Stream Generator Based on 3D Henon map and 3D Cat map,International Journal of Scientific and Engineering Research 8(1):2114, 2017.
23. Pranjali Sankhe, Shruti Pimple, Surabhi Singh, Anita Lahane, An Image Cryptography using Henon Map and Arnold Cat Map, International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 04 | Apr-2018.
24. ALa'a Talib khudhair and Abeer Tariq Maolood, Towards Generating a New Strong key for AES Encryption Method Depending on 2D Henon Map, Diyala Journal for Pure Science,2018.
25. Ekhlas Abbas Albahrani, A Combination of Two-Dimensional Hénon Map and Two-Dimensional Rational Map as Key Number Generator, December 2019DOI:10.1109/CAS47993.2019.9075731Conference: 2019 First International Conference of Computer and Applied Sciences (CAS)
26. Ansam Sabah , Shaymaa Hameed, Maisa'a Abid Ali K. Key Generation Based on Henon Map and Lorenz System, Al-Mustansiriyah Journal of Science ISSN: 1814-635X (print), ISSN:2521-3520, Volume 31, Issue 1, 2020.
27. Daniel Murillo-Escobar · Miguel Ángel Murillo-Escobar · César Cruz-Hernández · Adrian Arellano-Delgado · Rosa Martha López-Gutiérrez, Pseudorandom number generator based on novel 2D Hénon-Sine hyperchaotic map with microcontroller implementation, under exclusive licence to Springer Nature B.V. 2022
28. Mohamed G. Abdelfattah, Salem F. Hegazy, Nihal Fayez,S. Obayya,Optical cryptosystem for visually meaningful encrypted images based on gyrator transform and Hénon map, Optical and Quantum Electronics · January 2022.
29. Ala'a Talib Khudhair, Ekhlas Khalaf Gbashi, Abeer Tariq Maolood, "A Noval Dynamic S-Box based on password Key and Circle Map", Iraqi Journal of Science (IJS).2023.
30. Ekhlas K. Gbashi, Abeer Tariq Maolood, Yaseen Naser Jurn " Privacy Security System for Video Data Transmission in Edge-Fog-cloud Environment", *International Journal of Intelligent Engineering and Systems, Vol.16, No.2, 2023.*
31. Abeer Tariq Maolood, Ekhlas Khalaf Gbashi, Eman Shakir Mahmood,"Novel lightweight video encryption method based on ChaCha20 stream cipher and hybrid chaotic map", International Journal of Electrical and Computer Engineering (IJECE), Vol. 12, No. 5, October 2022.