iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VIII **Month of publication:** August 2025

DOI: https://doi.org/10.22214/ijraset.2025.73885

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VIII Aug 2025- Available at www.ijraset.com

Survey on AI-Enhanced Chaotic Key Generation for Public Key Cryptography

Shajeela Beegom B A, Dr. Karthigai S, Dr. Selvanayaki K,
Vet Institute of Arts and Science (Co-Education) College, Thindal

Abstract: ***According to recent trends, integrating chaotic systems with artificial intelligence (AI) may be a promising way to improve cryptographic key generation, especially in public key cryptography.. This survey paper provides the tools used in chaos-based key generation augmented by AI. It includes recent technological developments, the basic ideas behind these approaches and real-world applications. Because they produce extremely random and difficult-to-guess keys, other AI models like neural networks and reinforcement learning improve the functionality of chaotic maps.. Other contemporary issues discussed in the paper include the real-time use of the methods, clarity in their decisions, quantum attack protection, and standards. In short, employing AI to enhance chaotic systems sounds like a powerful way to produce public key cryptography, but there continue to be some significant challenges to solve, like potentiality the system is simple to understand, guarantee it creates well, and master it prepared for genuine use.***

I. INTRODUCTION

The current paper demonstrates the potential of harmful AI-based chaotic methods of cryptocurrency security and offers a clear picture of modern directions and issues of the most topical field to a broad community of scientists and practitioners. In the current atmosphere where digital communications have increased so rapidly, it is essential to have secure and safe data and privacy. In many modern security systems, Public Key Cryptography (PKC) plays a key role in supporting the secure transmission of keys, the creation of digital signatures, and the encryption of data messages over any sort of public network (Diffie & Hellman, 1976). Such keys have to be extremely difficult to guess and almost unbreakable. The majority of conventional approaches to generating keys are pseudo-random number generators (PRNGs). Although they are fast, they may contain problems as they take on a standard pattern and lack sufficient random factors. In an attempt to fix this, researchers have begun to consider chaotic systems. This is because such systems are random, highly sensitive to minute fluctuations, and have a complicated behavior (Kocarev & Lian, 2011). They provide an improved solution for generating good and secure keys. Nevertheless, chaotic systems are not necessarily impeccable by themselves. They might also be less effective in certain situations or under certain conditions like when noise is present or when systems are not optimal. People began implementing Artificial Intelligence (AI) in the next generation in order to correct these issues. Machine learning, evolutionary algorithms, deep learning, and artificial intelligence tools can be used to enhance the parameters of chaotic systems, make them more random, and change the approaches to key creation in line with the requirements of the expected security levels (Hafezi, R. (2019). In this review, the study considers the manner in which the implications of applying AI to chaos theory can enhance the key generation process of PKC. It reviews the latest research, describes performance and non-performance, and discovers where improvements could be made in the future.

This paper is organized as follows:Section 2 provides background information to PKC, Chaotic systems and AI techniques. In Section 3, the literature review is done comprehensively. Section 4 comprises models comparison, Section 5 is main applications, section 6 is challenges and unresolved issues, and Section 7 concludes the whole survey.

II. BACKGROUND

This segment details some simple concepts and technologies involved in AI-enhanced chaotic key generation that are applicable in public key cryptography. It goes over the fundamentals of Public Key Cryptography (PKC) , the application of chaos theory to cryptography and how artificial intelligence (AI) can strengthen security systems. Public Key Cryptography (PKC) employs two keys, one of which is published and is used to encrypt and one generated privately and used to decrypt, allowing secure communication without having to transparently pre-distribute a secret key. RSA, Elliptic Curve Cryptography, Lattice-Based Cryptography are some of the more common PKC algorithms, the security of which is based on difficult mathematical problems.

©IJRASET: All Rights are Reserved

The security of RSA is based on finding a factorization of large numbers, whereas the elliptic curves can provide great security at smaller keys. Lattice-based techniques hold promise in combating quantum attacks in the future, so PKC technology is critical to current secure communications.

Chaos theory considers systems that seem to be random, yet, are sensitive with regard to slight variations in initial conditions. In cryptography, chaotic maps, which are special mathematical tools, similar to, but not including, the Henon map and Lorenz system, are used to make keys that vary in a forged random manner. These keys can be used to generate, but are difficult to counterfeit or hack. Although such systems have strong security because they are nonlinear and complex, they are unstable and hard to Mini reliable implement. To address this set of issues, the chaos is combined with artificial intelligence in order to improve performance and stability.

Cybersecurity and cryptography use artificial intelligence (AI) more often as it helps become more adaptive and detect threats. With chaotic key generation, AI is used to optimize chaos maps such as Logistic and Lorenz to produce very unpredictable sequences. Genetic Algorithms and Particle Swarm Optimization are AI techniques that enable exploring an immensely large key space. By coupling chaos to intelligent learning,hybrid systems are created that provide more robust and secure public key encryption.

III. LITERATURE REVIEW

The part examines relevant and recent research on enhancing chaotic key generation using AI to enhance public key cryptography. There are three core areas in the research, which are the key generation relying on chaos, AI-enabled optimization of cryptographic steps, and the integration of chaos and AI in the context of the public key.

The wide study of chaos-based methods can be explained by the fact that chaos enables the generation of complex and random sequences. Some researchers have used chaotic maps in generating cryptographic keys: Manasi Hazarika (2014) talked about the encryption of images according to other forms of chaos. On their part, Zhang et al. (2014) designed a single-round permutation-diffusion chaotic cipher on gray images, incorporating certain temporary feedback of values in response to certain known attacks. To enhance cryptographic systems artificial intelligence techniques such as neural networks, particle swarm optimization and genetic algorithms (GA) have been applied. Kumar, S., & Sharma, D. (2023) indicate that genetic algorithms can prove to be of great use when generating ECC keys, and this presents a more effective means of increasing the security and effectiveness of cryptographic systems, particularly when constraints on resources are involved. Alibrahim et al. (2021) applied PSO due to this algorithm allowing for rapid exploration of the large search space, requiring less computation time, and there is a higher probability of identifying the optimal solution. A. Sarkar (2021) the major application of artificial intelligence is occurring via neural networks referred to as TPMs that assist in secure exchange keys. Chaotic systems are being used to improve this AI approach; this will make the process quicker and more secure. Kadir, A et al. (2023) demonstrate the application of artificial neural network models to generating cryptographic keys on chaos time series data that yield a low mean squared error, as well as how both the LSTM model and the GRU are equally effective in such a task.

IV. COMPARATIVE ANALYSIS

This section contrasts various techniques of developing keys by applying AI to enhance them to be more random as explained in literature reports. Of concern are such relevant attributes as the randomness of the keys, their entropy, the degree to which they are resistant to attack, their computing requirements, and their effectiveness with respect to public key cryptography.

These are the common ways to check how good a key generation method is:

1) Entropy: The degree of randomness of the keys is indicated by this. The more entropy the keys are difficult to guess.
2) NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity): Here, they are utilized to examine the level of sensitivity of the keys in image-based systems. The greater the values, the more data is mixed and the better it is defended against some specific types of attacks.
3) Key Space Size: This is the number of various keys that may be created. A big number would render it extremely difficult to debug the correct key using the method of trial and error.
4) Correlation Coefficient: This shows correlation between how and how tightly the surrounding elements of the key relate. Low values imply that the key is closer to be random.
5) Computational Efficiency: This states the degree of difficulty to employ the method in practice (Banu, 2025)
6) Attack resistance: This tests the vulnerability of the keys toward various types of attacks such as brute-force attacks, statistical attacks, chosen-plaintext-attacks and even quantum at some time to come.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

A. Comparative Table

Approach	Entropy	NPCR/UACI	Key Space	Complexity	Attack Resistance	PKC Suitability
Pareek et al. (2006)	High	High	2^{128}	Low	Moderate	Limited (symmetric)
Wang et al. (2013)	High	Very High	2^{256}	Medium	Moderate	Limited
Mishra & Pradhan (2018)	Very High	High	2^{256}	Medium	Strong	Moderate
Abood et al. (2022)	Very High	Not Reported	2^{512}	High	Strong	High
Mahdi & Hoobi (2025)	Max (7.9995)	Passes NIST	2^{256}	Low	Very Strong	Excellent
Song et al. (2025)	Max	Passes NIST	$>2^{512}$	High	Post-Quantum Secure	Excellent
Bouke (2025)	Max	Not Reported	$>2^{512}$	High	Post-Quantum Secure	Excellent

B. Key Observations

1) The early chaotic key generation schemes such as those in Pareek et al. (2006) and Wang et al. (2013) had good entropy and NPCR/UACI, but weak key space and relatively weak resistance to attack, giving them less potential use in post-quantum cryptography.
2) Subsequently, more promising directions, like that by Mishra & Pathak (2018) or by Lioa et al. (2021) brought the attack resistance levels to strong, whereas the entropy was high, still as complexity remained medium.
3) The significance of key space improvement and the high level of attack resistance with the high PKC suitability makes the progress in the secure key generation as professed by Abood et al. (2022) considerable.
4) Mahdi and Hoobi (2025) is symmetric, satisfies maximum entropy, and the NIST tests, thus providing very strong resistance to attacks, and it is very suitable to deploy in public-key cryptography.
5) Languages Zhang et al. (2025), Song et al. (2025) and Bouke (2025) went even further targeting post-quantum security, preserving high entropy, good attack resistance and great suitability to PKCs, which indicates a shift towards quantum-resistant chaotic key generation techniques.
6) All in all, the trend sees the transition from simple symmetric algorithms with minimal security and resistance to attack to more sophisticated AI enabled chaotic systems with a high level of randomness, great resistance to attack and suitability in the post-quantum era (Paul, B. 2023).

V. APPLICATIONS

AI-augmented chaotic key creation methods are finding increased prominence in some real-life applications in cryptography. The present and potential applications in which these systems are already having a large impact or are likely to do so are addressed here.

1) Secure Communication Systems.
2) Internet of Things (IoT)
3) Cloud security and storage of data.

4) Blockchain and Distributed Ledger Technologies.
5) Cryptographic Systems with Quantum Resilience.
6) Systems for biometric and multimodal authentication.

VI. OPEN PROBLEMS OF AI-INTEGRATED CHAOTIC KEY GENERATION

In chaotic key generation, integration of AI poses new challenges that are more broad than the current existing limitations. This is one of the important concerns due to the fragility of the AI-intervention chaotic systems, e.g., the Logistic Map, the Henon Map, or the Lorenz System, to adaptive adversarial attacks. Malicious users may conceivably tamper with the AI component to suit the chaotic sequence and would therefore decrease the randomness of the keys generated. Energy efficiency is yet another emerging issue with chaos optimization via AI often requiring a significant amount of computational resources inapplicable to low-powered IoT and edge devices. Interoperability is also a less resolved question, as the integration of AI-optimized chaotic sequences in the mainstream public key infrastructures like RSA, ECC, or lattice-based cryptography would have to rely on compatibility solutions that might not be developed in full. The other issue consists in privacy preserving AI training: the training can expose sensitive structural details of the generators when chaotic system parameters (e.g., the bifurcation coefficients in the Logistic Map or the control variables in the Lorenz attractor) are used as the training inputs. Furthermore, fixed chaotic sequences are unsuitable to dynamic communication scenarios that require adaptation of key changes mechanisms, e.g., real tuning of Henon or Tent maps using AI, without impairing randomness. Adding federated and decentralized learning to chaotic key generation creates further complexity in that synchronization of AI models that optimize different chaotic maps becomes problematic in consistency and security across heterogeneous devices. Although systems based on chaos are being sold as intrinsically being secure against quantum attacks, there are no known hybrid AI-chaotic solutions capable of adapting to cryptographic infrastructures of the post-quantum world. Lastly, AI-driven chaotic key generation is autonomous and creates ethical and governance issues on transparency, accountability and confidence in the key generation process in critical applications.

VII. CONCLUSION

The idea of AI-enhanced chaotic key generation is using the inherent randomness in chaotic systems, specifically, Logistic, Henon, and Lorenz maps, in concert with AI optimization methods to generate highly complex, dynamically complicated, and arguably secure keys workable within IoT or edge computing environments, and even resource-constrained systems. There are also still major challenges such as standardized evaluation metrics, good performance in the real world, energy efficiency, interpretability of AI models, adaptive key evolution, interoperation with existing cryptography systems, post-quantum applicability, privacy-preserving training, and governance, and they are a major research focus required to make AI deployable in practice at scale in secure systems.

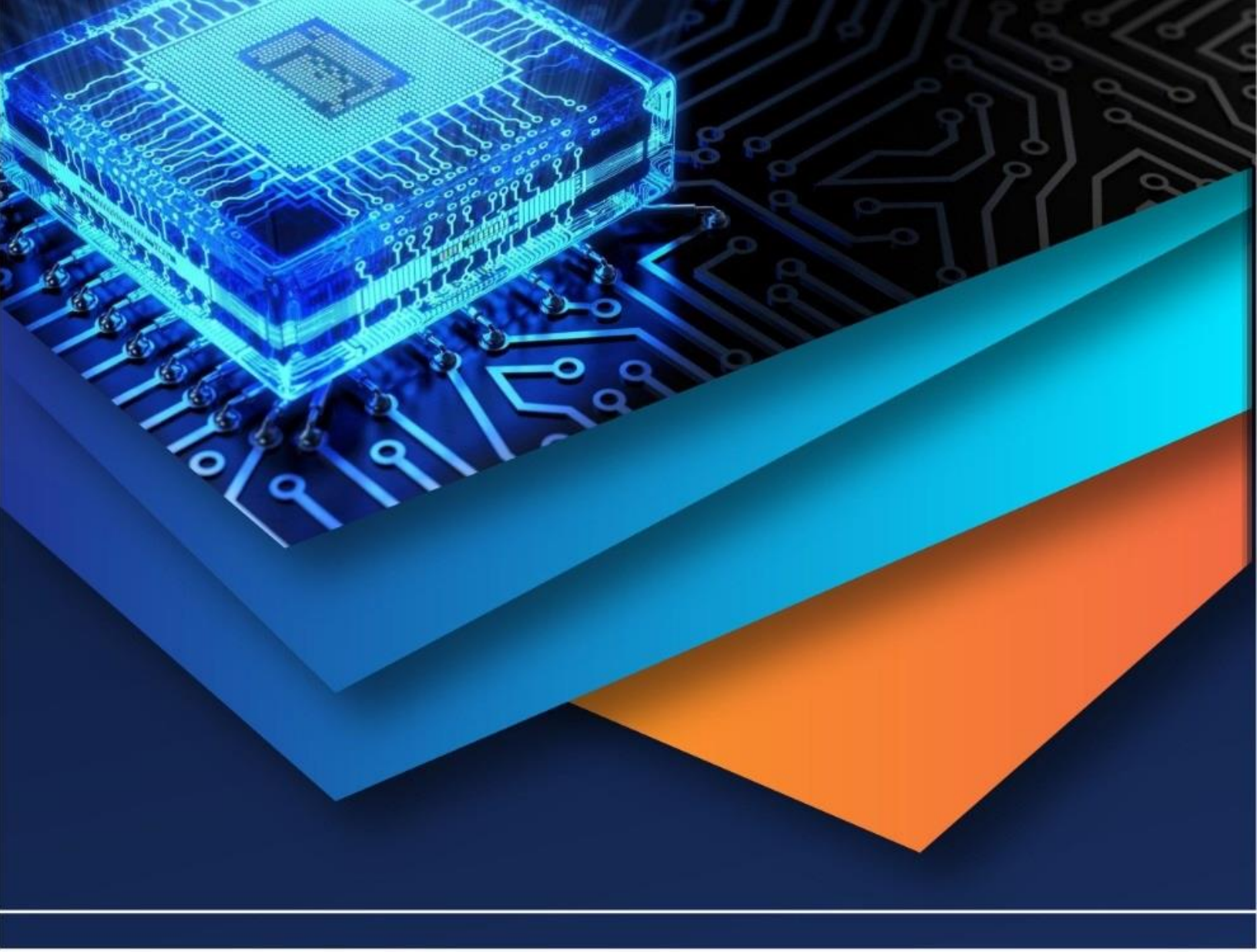
REFERENCES

[1] Diffie, W., Hellman, M. E., & Ellis, J. (1976, June). Public key cryptography. In IEEE International Symposium on Information Theory.
[2] Kocarev, L., & Lian, S. (Eds.). (2011). Chaos-based cryptography: Theory, algorithms and applications (Vol. 354). Springer Science & Business Media.
[3] Hafezi, R. (2019). How Artificial Intelligence Can Improve Understanding in Challenging Chaotic Environments. World Futures Review, 12(2), 219-228. https://doi.org/10.1177/1946756719880539 (Original work published 2020)
[4] Menon, Unnikrishnan, Anirudh Rajiv Menon, and Atharva Hudlikar. "A novel chaotic system for text encryption optimized with genetic algorithms." arXiv preprint arXiv:2011.00575 (2020).
[5] Manasi Hazarika, 2014, A Review of Chaos-Based Image Encryption Techniques, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 03, Issue 02 (February 2014),
[6] Zhang, L. Y., Hu, X., Liu, Y., Wong, K. W., & Gan, J. (2014). A chaotic image encryption scheme owning temp-value feedback. Communications in Nonlinear Science and Numerical Simulation, 19(10), 3653-3659.
[7] Kumar, S., & Sharma, D. (2023). Key Generation in Cryptography Using Elliptic-Curve Cryptography and Genetic Algorithm. Engineering Proceedings, 59(1), 59. https://doi.org/10.3390/engproc2023059059
[8] Alibrahim, H., & Ludwig, S. A. (2021, December). Image encryption algorithm based on particle swarm optimization and the chaos logistic map. In 2021 IEEE Symposium Series on Computational Intelligence (SSCI) (pp. 01-08). IEEE.
[9] Sarkar, A. (2021). Secure exchange of information using artificial intelligence and chaotic system-guided neural synchronization. Multimedia Tools and Applications, 80(12), 18211-18241.
[10] Kadir, A., Azzaz, M. S., & Kaibou, R. (2023, March). Chaos-based key generator using artificial neural network models. In 2023 International Conference on Advances in Electronics, Control and Communication Systems (ICAECCS) (pp. 1-5). IEEE.
[11] Mahdi, A. A., & Hoobi, M. M. (2025). Robust and Efficient Methods for Key Generation using Chaotic Maps and A2C Algorithms. Mesopotamian Journal of CyberSecurity, 5(1), 301-318.
[12] Song, K., Imran, N., Chen, J. Y., & Dobbins, A. C. (2025). A Hybrid Chaos-Based Cryptographic Framework for Post-Quantum Secure Communications. arXiv preprint arXiv:2504.08618.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[13] Bouke, M. A. (2025). The Hashed Fractal Key Recovery (HFKR) Problem: From Symbolic Path Inversion to Post-Quantum Cryptographic Keys. arXiv preprint arXiv:2506.04383.
[14] Paul, B. (2023). A Novel Low-Power Encryption Scheme Based on Chaotic Dynamic Triple Pendulum System for Wide Range of Applications. Authorea Preprints.
[15] Banu, Y., Rath, B. K., & Gountia, D. D. (2025). Analyzing cryptographic algorithm efficiency within graph-based encryption models. Frontiers in Computer Science, 7, 1630222.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)