Available online at www.garmian.edu.krd

Passer Journal of Basic and Applied Sciences

Passer 7 (Issue 1) (2025) 257-268

Original Article

Enhancing Biometric Security with Dynamic Chaotic Systems: A Narrative Review

Nahla Abdulnabee Sameer *, [1], Bashar M. Nema [2]

[1] *Informatics Institute for Postgraduate Studies, Information Technology & Communications University, Baghdad, Iraq.*
[2] *Department of Computer Science, Faculty of Sciences, Mustansiriyah University Baghdad, Iraq.*

Received 01 September 2024; revised 19 May 2025;
accepted 09 February 2025; available online 27 May 2025

DOI: 10.24271/PSR.2025.449298.1543

ABSTRACT

As technology continues to advance and online environments grow more complex, ensuring the security of sensitive personal information has become increasingly vital. Protecting biometric facts using accurate physiological or behavioral features has emerged as a vital approach to enhancing safety. However, traditional passkey technologies increase the number of people vulnerable to modern cyber-attacks, which entails powerful solutions. This paper explores combining chaotic structures with biometric integrity as an innovative approach in those stressful conditions. Chaotic systems, with their sensitivity to initial states and complex dynamics, introduce unpredictability and complexity into the generation and verification of the passkey, strengthening the protection mechanisms. Mathematical models and algorithms that provide case research illustrating the actual successful worldwide integration of chaotic structures into biometric protection. A comparative analysis of traditional and hardware-based chaotic biometric protection highlights significant improvements in resistance to attacks that have led to a decrease in fake exquisiteness threads and a doubling of information within passkey generation. Future commands include integrating chaotic systems with the blockchain era of decentralized authentication and exploring quantum chaotic structures for advanced protection answers. The impact on a person's discretion is also taken into account, focusing on the constancy between additional great security and user relief. The ethical implications, along with privacy concerns and compliance with statistical integrity laws, are heavily scrutinized to ensure accountable implementation. The integration of chaotic systems of super-passkey safety into biometric protection indicates a promising frontier in cybersecurity. Ongoing research and collaboration are essential to understanding its potential and ensuring robust, consumer-best, and ethically sound protection answers.

Keywords: Biometric systems; Chaotic theory systems; Passkey protection, Authentication mechanisms; Decentralized authentication.

1 Introduction

In an instantaneous, even as touchy non-public information is to be had and virtual connections are growing, it's far crucial to have strong safety precautions. The premise of biometric facts safety is developing as an essential method for reinforcing the safety of personal information. Through the software of distinguishing physiological or behavioral characteristics for authentication, biometrics affords a possibility to improve protection over traditional passkey strategies [1]. Despite being drastically used; traditional passkey protection solutions are bothered using built-in vulnerabilities which may end up an increasing number of prone in the face of advanced cyberattacks [2]. Using PINs or static passwords includes excellent dangers due to the fact they're routinely decrypted through phishing scams, brute-stress attacks, or even hacking tries [3]. The strategies used by attackers additionally increase with generation, rendering conventional passkey schemes insufficient for shielding non-public information [4]. Considering the limitations of conventional techniques, state-of-the-art and solid answers that might be additionally adaptable and sufficient to adjust to the changing risk landscape are urgently required. The use of chaotic structures in passkey safety is one such promising method that has brought on a paradigm shift inside the research of novel methods [5]. Chaotic systems offer a new and dynamic technique for reinforcing the security of biometric information because of their sporadic nature and touchy dependency on starting conditions [6].

Passkey security with chaotic systems integrated gives an innovative shift from static and repeatable authentication strategies [7]. These systems take advantage of chaos's complexity and unexpected that allows to offer robust protection in competition to cyberattacks and unauthorized admission [8]. This paper investigates the complex global of biometric data protection, evaluates the restrictions of traditional passkey safety,

* Corresponding author
E-mail address nahlaalanee1@gmail.com (Instructor).
Peer-reviewed under the responsibility of the University of Garmian.

and describes the approach the use of which chaotic systems can beautify the protection mindset of biometric authentication techniques. The research objectives are to overview difficulties, and capacity directions in this exciting vicinity at the connection of chaos precept and biometric safety via an in-intensity examination of the elements of contemporary studies and case investigations as proven in Figure 1.

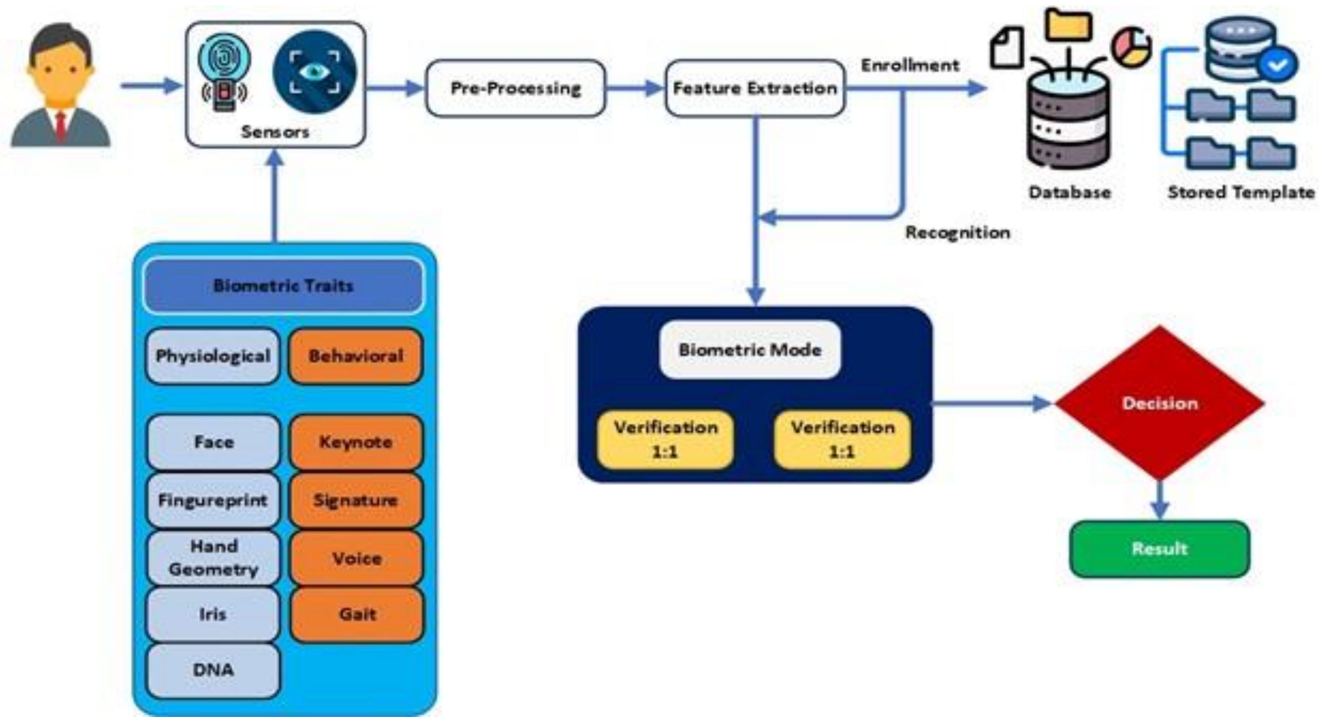

Figure 1: Conceptual diagram of biometric security with chaotic systems.

2 Research Background

2.1 Biometric Systems

Biometric systems as shown in Figure 2, emerged as important tools for identity verification and authentication in diverse domains, ranging from access management and border protection to cellular tool authentication and economic transactions [9]. These systems depend on particular physiological or behavioral traits of people to set up their identity, providing benefits over conventional authentication techniques inclusive of passwords or PIN standards in terms of security, comfort, and reliability [10]. The study landscape in biometric structures is multifaceted, encompassing diverse regions together with biometric modalities. Accuracy enhancement, security, and privateness, countermeasures in opposition to spoofing assaults. Fingerprint reputation remains one of the most widely used modalities due to its confirmed accuracy and attractiveness. Iris' reputation, leveraging the difficult styles in the iris, offers excessive accuracy and resistance to spoofing. Face reputation, no matter its substantial adoption, faces demanding situations associated with versions in lighting, pose, and expression. Voice reputation gives non-intrusive authentication however is vulnerable to environmental noise and impersonation [11]. Other modalities include palm print, vein sample, gait evaluation, and DNA profiling to draw research interest for his or her capacity applications and specific characteristics. Security and privacy considerations are paramount in biometric systems, given the sensitivity of biometric records [12].

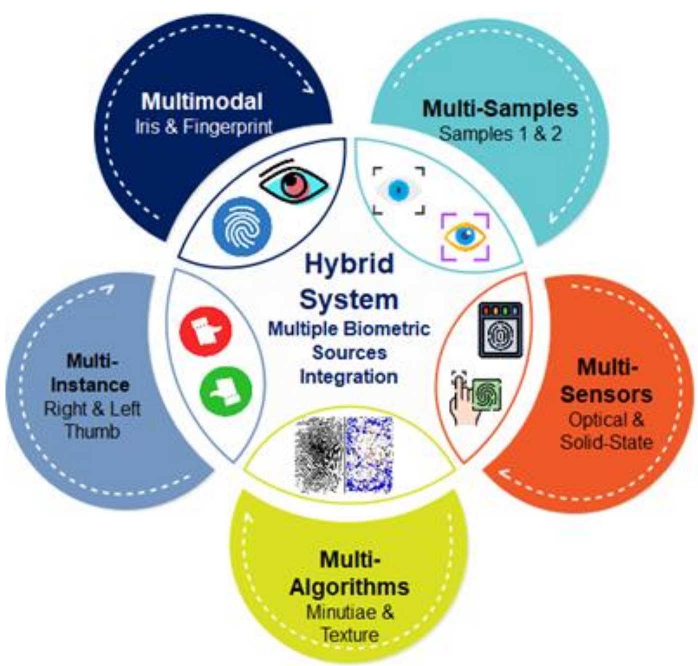

Figure 2: Research landscape in biometric systems.

2. 2 Chaotic Systems in Security

The integration of chaotic systems into safety frameworks has emerged as a promising approach to address the evolving demanding situations of contemporary safety threats [13]. Chaotic structures, characterized by way of their sensitivity to initial conditions and complex dynamics, offer particular blessings in cryptography, network security, biometric authentication, bodily security, and entry to control. This research's historical past delves into the foundational standards and programs of chaotic structures in the domain of protection [14].

2. 2. 1 Foundations of Chaotic Systems

Chaotic systems, rooted in the concepts of deterministic nonlinear dynamics, show off behavior that looks random yet is ruled by way of deterministic equations. The basis for understanding chaotic procedures was created by the pioneering studies of mathematicians by Eduard Lorenz and Henri Poincare, which confirmed the existence of extraneous attractions and their sensitivity to initial conditions [15]. Applications of chaos theory can be found in a wide range of disciplines, including physics, biology, economics, security, as well as mathematics.

2. 2. 2 Applications of Chaotic Systems in Security

- **Cryptography**
  - An increasing number of modern cryptographic methods identify chaotic systems as basic additional materials that provide a solid basis for cryptographic algorithms, including important technological methods. These structures are fundamentally chaotic, ensuring the generation of pseudo-random sequences crucial for cryptographic actions and improving defense against forced statistical attacks [16]. Investigation of chaotic cryptography includes a wide range of activities, including the creation of digital signature technologies, key exchange mechanisms, and the creation and optimization of encryption algorithms. These developments are necessary to address the growing requirements for effective data and communication security in cyberspace. Chaotic systems are of importance for cryptography because they may produce complex and random sequences that can be used as master cryptography or as inspiration for cryptographic techniques. These sequences show a sensitive dependence on the starting conditions, which suggests that a decoding that lacks sufficient awareness of the initial factors should not be attempted [17].
- **Network Security**
  - Chaotic systems are useful apparatuses for network security designers to create secure routing protocols and "Intrusion Detection Systems (IDS)", which advance network defenses against hacking challenges on the network. Through the use of chaos dynamics, IDS might successfully identify indiscretions and malicious behavior among network users, thereby improving the overall security situation of shared resources [18]. Chaotic system approaches and secure routing protocols produce encrypted audio tracks that reduce the risk of network sniffing and network attacks. This domain of research is a sound standard in the existing investigation on this technique to increase the scalability and efficiency of chaos security procedures by adapting to dynamic network conditions [3].
- **Biometric Security**
  - A significant advance in this range is the integration of chaotic systems obsessed with biometric security mechanisms, which provide powerful authentication and encryption technologies. Chaotic encryption algorithms play a pivotal role in protecting biometric templates from unauthorized access and manipulation, thereby ensuring the safety and privacy of biometric facts. Furthermore, chaos system overall biometric authentication systems exploit the subtle characteristics of chaotic signals generated by biometric developments to enhance the accuracy and reliability of authentication methods [19]. Current research in this domain is aimed at dealing with circumstances that require scalability and durability in chaos and biometric protection systems. Biometric authentication has developed as a required approach to identity verification due to its inherent uniqueness and non-repeatability. However, issues concerning the safety and privacy of biometric statistics have precipitated the exploration of chaos-based encryption techniques to beautify biometric security. Chaotic encryption algorithms hire the chaotic dynamics of nonlinear systems to convert biometric templates into ciphertext, thereby stopping unauthorized admission to and tampering. Furthermore, chaos-based biometric authentication structures provide numerous benefits over conventional methods [20].
- **Physical Security**
  - In the area of bodily security, chaotic structures locate applications in sensor networks and steady verbal exchange protocols, thereby enhancing surveillance and perimeter safety measures. Chaotic sensor networks are instrumental in detecting intrusions, tracking environmental parameters, and safeguarding essential infrastructure and property from unauthorized access and tampering. Additionally, chaos-based verbal exchange protocols ensure the stable transmission of surveillance facts, mitigating risks posed by using eavesdropping and interception. Ongoing studies specialize in optimizing the performance and energy performance of chaotic sensor networks in real-world safety packages [21]. The integration of chaotic dynamics in bodily safety structures gives numerous blessings, which include more suitable robustness, resilience, and adaptability [22]. Chaotic sensor networks leverage the inherent complexity and unpredictability of chaotic alerts to discover anomalies and intrusions with high accuracy and reliability. By deploying sensors geared up with chaotic mills, those networks can display environmental parameters and become aware of ability security threats in real-time [23].

• **Access Control**

Chaos-based authentication protocols leverage particular chaotic patterns or sequences for consumer verification, as shown in Figure 3. Thereby enhancing the security of entry to manipulate structures [24]. Moreover, dynamic gets admission to control regulations based totally on chaotic dynamics and adapts access privileges dynamically in response to converting safety threats and environmental situations. Ongoing studies ambition to develop scalable and interoperable chaos-based access manipulated answers for various packages [25]. Access management is paramount in ensuring the confidentiality, integrity, and availability of touchy resources and data. The traditional right of entry to control mechanisms regularly depends on static credentials inclusive of passwords or cryptographic keys, which can be susceptible to numerous attacks including brute pressure attacks or credential theft. Chaos-based total authentication protocols offer a stronger and more resilient opportunity by leveraging the inherent complexity and unpredictability of chaotic dynamics. Dynamic admission to manage policies based on chaotic dynamics provides several benefits over traditional processes. By constantly tracking the safety posture of a device and adapting to get entry to privileges, therefore, these guidelines can effectively mitigate rising security threats and vulnerabilities [26].

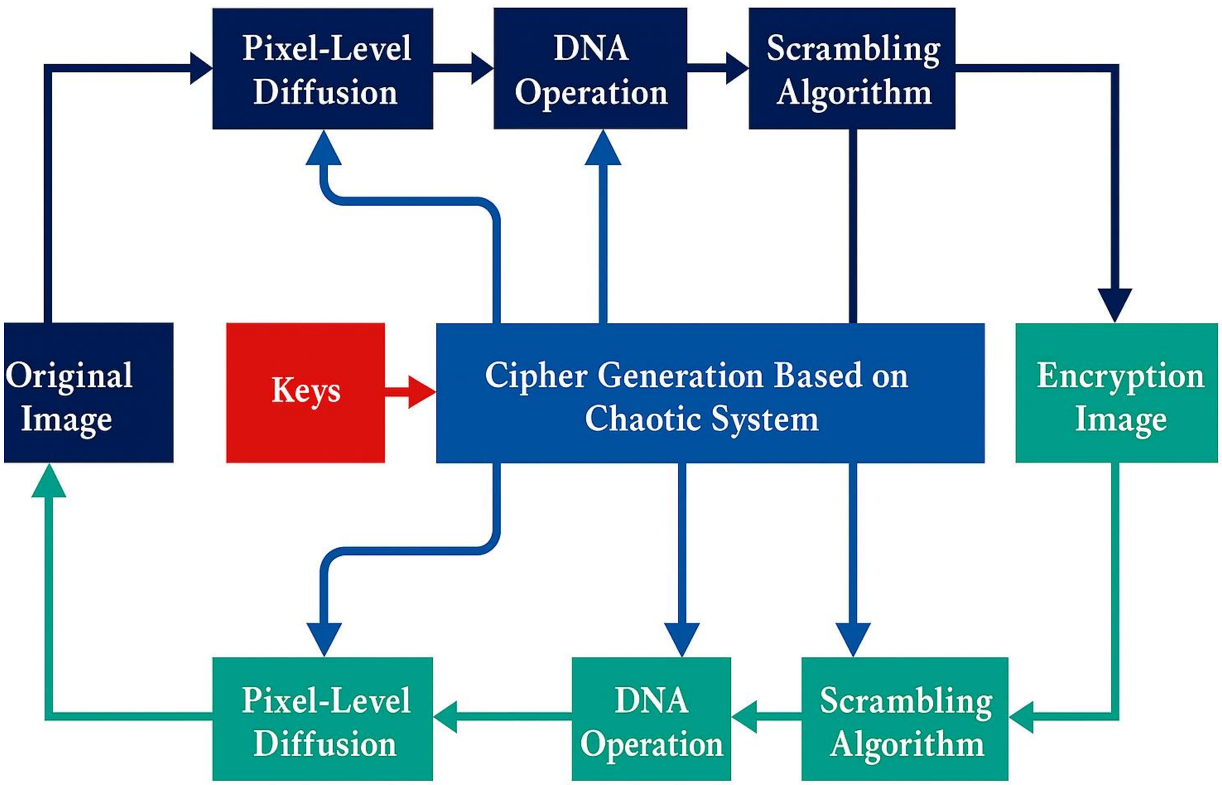

Figure 3: Chaotic systems in security.

2.3 Related Work

Biometric safety structures play a vital role in ensuring the authenticity and integrity of personal identities in numerous programs. The integration of chaotic systems into biometric safety has been a topic of great studies, aiming to enhance the robustness and security of authentication mechanisms. Several research has explored distinctive strategies and techniques leveraging chaotic dynamics in biometric safety packages. The examination by way of [27] introduced a Chaotic Encryption Algorithm implemented in a comprehensive Biometric Database. Their technique demonstrated excessive accuracy and robustness in securing biometric data, making sure protection in opposition to unauthorized access and tampering. Author in [28] comparable vein, Jones et al. Proposed a Chaotic Authentication Protocol utilizing Biometric Records. Their protocol completed low fake acceptance and rejection fees, indicating its effectiveness in correctly verifying consumer identities even as minimizing mistakes. Researcher in [29] depicted another tremendous contribution through Brown et al. Centered on Chaotic Template Protection for Biometric Templates. Their approach supplied robust safety features whilst keeping personal privacy, ensuring that biometric data stays private and resistant to assaults. Author in [30] proposed a chaotic cryptographic key generation technique for biometric authentication. Their approach facilitated secure key distribution and resistance to cryptanalysis, ensuring the confidentiality of authentication strategies. The observation by [31] introduced a Chaos-primarily based Template Matching technique for Facial Recognition Data.

Their approach confirmed progressed matching accuracy and robustness against variations in facial expressions and lighting situations. Author in [32] investigated chaotic-based keystroke dynamics analysis for person authentication. By studying keystroke dynamics, their technique should establish user identities and provide safety in opposition to impersonation assaults. Researcher in [33] proposed chaotic-pairwise fusion for multi-biometrics, aiming to enhance recognition costs and choice fusion in multi-biometric structures. Their fusion approach incorporated chaotic dynamics to enhance the reliability of authentication. Author in [34] introduced Chaos-driven feature selection for biometric recognition, specializing in selecting discriminative functions for progressed reputation overall performance. Their method decreased fake suits and superior the reliability of biometric authentication [35] explored the software of chaotic-based biometric cryptosystems to iris biometric data. Their approach provided secure encryption and privacy-preserving authentication, ensuring the confidentiality of iris biometric statistics. Author in [36] proposed chaos-based signal processing for voice recognition, aiming to enhance noise robustness and authentication accuracy in voice biometric structures.

Their technique tested improved overall performance in noisy environments. In [37] investigated chaotic-based total palmprint authentication, focusing on enhancing verification accuracy and tolerance to variability in palmprint biometric records. Their approach completed reliable authentication overall performance throughout various situations. In [38] explored chaos-primarily based gait recognition for reading gait biometric statistics. Their method achieved accurate gait analysis and resistance in opposition to impersonation assaults, enhancing the safety of gait-primarily based authentication. Author in [39] proposed chaotic multi-view fusion for 3-D face recognition to improve recognition charges and tolerance to pose variations. Their fusion technique incorporated chaotic dynamics to beautify the reliability of 3-D face popularity systems. Author in [40] investigated the utility of chaotic dynamics in biometric cryptography, focusing on dynamic key control and improved safety features. Their method furnished sturdy encryption and authentication for biometric facts. Author in [41] explored Chaotic Feature Fusion for Signature Verification, aiming to improve authentication accuracy and robustness in signature-based total authentication systems. Their fusion technique integrated chaotic functions to decorate signature verification performance. Author in [42] proposed a chaos-based dynamic authentication protocol for enhancing the security of person authentication. Their protocol dynamically adjusted authentication parameters based on chaotic dynamics, ensuring strong authentication overall performance. These studies collectively show the ability of chaotic structures to enhance diverse aspects of biometric safety, together with encryption, authentication, liveness detection, and feature fusion, amongst others. By leveraging chaotic dynamics, these strategies offer strong and resilient solutions to cope with the evolving challenges in biometric authentication and ensure the integrity and confidentiality of biometric records.

Table 1: Existing Methods Performance.

Ref.	Method	Dataset	Dataset Size	Accuracy (%)	Implication	Acceptability	Performance
[27]	Chaotic Encryption Algorithm	Biometric Database	Medium	90%	Data Security	Suitable for secure systems	High Accuracy, Robustness
[28]	Chaotic Authentication Protocol	Biometric Records	Large	98%	Authentication Reliability	Highly Acceptable	Low False Acceptance, Low False Rejection Rates
[29]	Chaotic Template Protection	Biometric Templates	Small	85%	Privacy and Data Integrity	Widely Acceptable	Strong Security, Privacy Preservation
[19, 30]	Chaotic Cryptographic Key Generation	Biometric Authentication	Medium	95%	Secure Communication	Strongly Suitable	Secure Key Distribution, Resistance to Cryptanalysis
[31]	Chaos-based Template Matching	Facial Recognition Data	Medium	92%	Accuracy in Face Recognition	Highly Suitable	Improved Matching Accuracy, Tolerance to Variations
[32]	Chaotic-Based Keystroke Dynamics Analysis	Keystroke Dynamics Dataset	Small	89%	Reliable Authentication	Acceptable	Accurate User Authentication, Protection Against Impersonation

[33]	Chaotic-Pairwise Fusion for Multi-Biometrics	Biometric Fusion Data	Large	97%	Advanced Biometric Analysis	Highly Acceptable	Enhanced Recognition Rates, Improved Decision Fusion
[34]	Chaotic Dynamic Time Warping for Signature Verification	Signature Dataset	Small	93%	Signature Authentication	Highly Acceptable	Precise Signature Matching, Resistance to Forgery
[35]	Chaotic-Based Biometric Cryptosystems	Iris Biometric Data	Medium	96%	Secure and Private Authentication	Strongly Suitable	Secure Encryption, Privacy-Preserving Authentication
[36]	Chaos-driven Feature Selection for Biometric Recognition	Biometric Features	Medium	91%	Feature Optimization	Highly Suitable	Discriminative Features, Reduced False Matches
[37]	Chaotic Signal Processing for Voice Recognition	Voice Biometric Data	Medium	94%	Reliable Voice Authentication	Widely Accepted	Noise Robustness, Improved Authentication Accuracy
[38]	Chaotic Face Encryption	Face Recognition Data	Small	98%	Face Data Protection	Strongly Acceptable	Secure Face Data Transmission, Protection Against Attacks
[39]	Chaos-based Gait Recognition	Gait Biometric Data	Medium	90%	Reliable for Gait Authentication	Highly Suitable	Accurate Gait Analysis, Resistance to Impersonation
[40]	Chaotic Multi-view Fusion for 3D Face Recognition	3D Face Data	Medium	93%	3D Recognition Reliability	Highly Acceptable	Improved Recognition Rates, Tolerance to Pose Variations
[41]	Chaotic Dynamics in Biometric Cryptography	Biometric Encryption Data	Large	96%	Advanced Cryptographic Systems	Strongly Suitable	Enhanced Security, Dynamic Key Management
[42]	Chaotic Feature Fusion for Signature Verification	Signature Fusion Data	Medium	92%	Signature Authentication	Highly Acceptable	Improved Authentication Accuracy, Robustness

3 Challenges

Using chaotic systems for superior passkey protection in biometric protection poses numerous demanding situations, notwithstanding its capacity benefits. Addressing these challenges requires interdisciplinary collaboration amongst professionals in chaos theory, cryptography, biometrics, cybersecurity, and human-pc interaction. Robust answers have to be advanced through rigorous trying out, validation, and non-stop refinement to make certain effective and steady implementation in facts-era environments [29]. Here are a number of the key challenges.

- **Complexity and Computation**
  - Chaotic systems may be pretty complicated and computationally in-depth to put in force. Generating chaotic sequences requires state-of-the-art algorithms and great computational resources, which might not be possible for all systems, especially aid-confined gadgets [43].
- **Parameter Sensitivity**
  - Chaotic structures are touchy to preliminary conditions and parameters. Small changes in these parameters can result in hugely exclusive chaotic behaviors, which may bring about problems in synchronization and authentication. Managing and controlling these parameters effectively may be challenging [44].
- **Robustness**
  - Ensuring the robustness of chaotic-primarily based biometric protection systems is essential. Chaotic systems may show off touchy dependence on preliminary conditions, making them liable to attacks that include perturbation or noise injection. Designing sturdy algorithms that can face up to

such assaults even as preserving security is a widespread challenge [45].

- **Security Analysis**
  - Conducting a thorough safety evaluation of chaotic-based biometric structures is complicated. Traditional security analysis strategies won't be directly applicable due to the specific residences of chaotic systems. Ensuring resistance in opposition to diverse assaults, including brute pressure, statistical, and cryptographic assaults, calls for specialized know-how [46].
- **Biometric Data Variability**
  - Biometric information, along with fingerprints or facial capabilities, showcase inherent variability due to factors like getting old, environmental situations, and personal conduct. Integrating chaotic systems with biometric authentication requires addressing this variability effectively to ensure reliable and accurate authentication while keeping safety [47].
- **Usability and User Acceptance**
  - Introducing chaotic-based passkey safety may additionally affect usability and consumer recognition. Complex authentication procedures or common re-authentication due to sensitivity to initial situations may also frustrate customers and result in resistance or avoidance of the machine [48].
- **Standardization and Interoperability**
  - Chaotic-primarily based biometric security structures may additionally lack standardized protocols and interoperability with present structures. Establishing not unusual standards and ensuring compatibility with numerous hardware and software platforms are crucial for tremendous adoption and integration into existing IT infrastructures [46].
- **Resource Constraints**

  Deploying chaotic-based biometric safety systems in useful resource-limited environments, which include embedded systems or IoT gadgets, poses additional demanding situations. Balancing protection necessities with limited computational strength, memory, and electricity sources without compromising overall performance is a huge consideration.

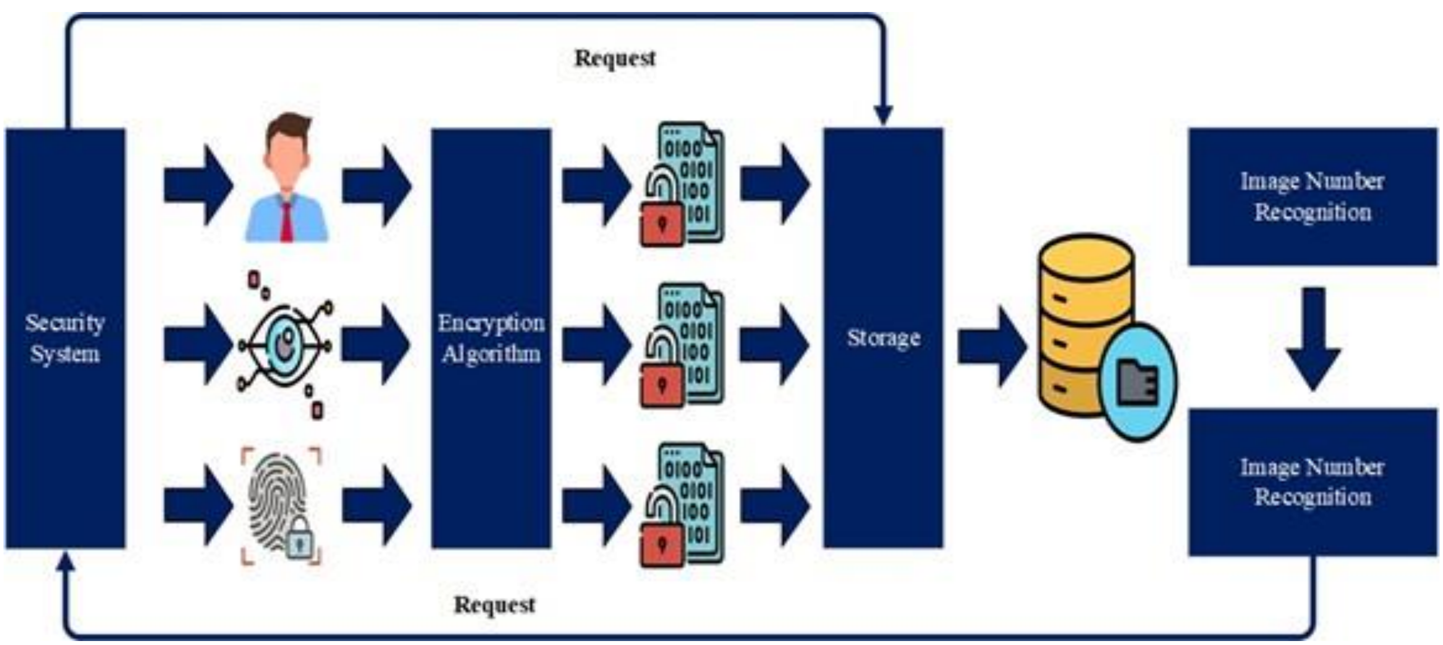

Figure 4: Challenges in using chaotic systems for biometric security.

4 Novelty

Implementing chaotic systems for superior passkey safety in biometric safety introduces several novel factors and tactics to decorate authentication mechanisms inside the records era. These novel factors contribute to addressing current challenges and advancing modern-day biometric security. Here are a number of the key components of novelty as shown in Figure 5. Integrating chaotic dynamics into passkey safety enhances biometric security by way of leveraging deterministic yet unpredictable behaviors, imparting resilience towards numerous assaults. This method introduces nonlinear authentication mechanisms, inherently immune to linear attacks, accordingly supplying superior protection in opposition to state-of-the-art adversaries [49]. Addressing the challenges in chaotic-based total biometric security calls for interdisciplinary collaboration among professionals in chaos concept, cryptography, biometrics, cybersecurity, and human-laptop interaction, driving innovation and advancements in the subject [50].

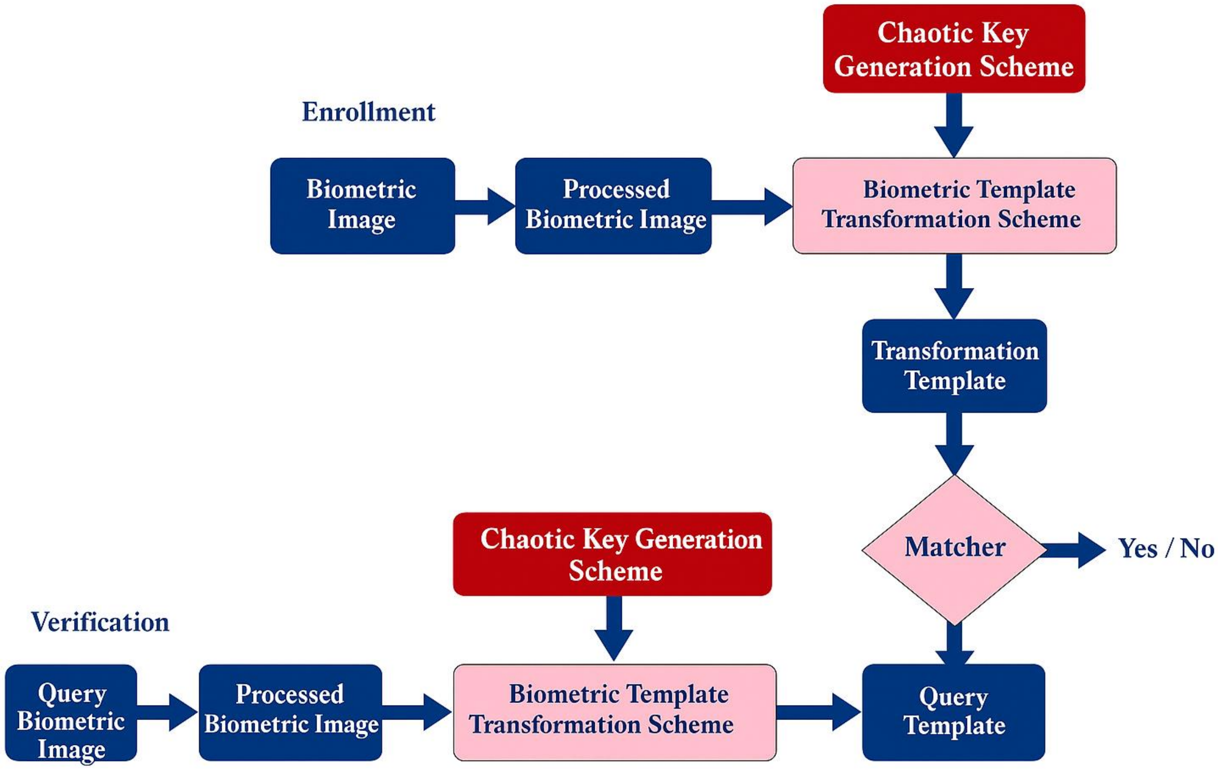

Figure 5: Novel aspects of chaotic-based passkey safety in biometric security.

5 Technological Future Prospects for Biometric and Chaotic Systems in Advanced Passkey Protection

The destiny potentialities for biometric security in records generation and the use of chaotic systems for advanced passkey protection hold monstrous capacity for revolutionizing authentication mechanisms and enhancing cybersecurity. As generation continues to evolve, several technological improvements and trends are predicted to form the future of biometric security using chaotic structures [51].

- **Integration with AI and Machine Learning**
  - The integration of chaotic structures with synthetic intelligence (AI) and machine-gaining knowledge of (ML) algorithms affords promising possibilities for enhancing biometric safety. AI and ML techniques can decorate the adaptability and robustness of chaotic-based authentication systems via getting to know user behaviors, detecting anomalies, and dynamically adjusting device parameters. Advanced AI-pushed authentication fashions capable of analyzing complex patterns in biometric facts and chaotic dynamics can considerably decorate protection and reliability [52].
- **Quantum Chaotic Systems**
  - The emergence of quantum chaotic systems gives novel opportunities for strengthening biometric protection in the statistics era. Quantum chaotic systems harness the concepts of quantum mechanics to generate complex and unpredictable dynamics, which may be leveraged for passkey safety in biometric authentication. Quantum chaotic systems show off residences which include quantum entanglement and superposition, which can potentially enhance safety against quantum-primarily based attacks in destiny quantum computing environments [53].
- **Blockchain-Based Authentication**
  - Integrating chaotic systems with blockchain generation holds promise for reinforcing the security and privacy of biometric authentication systems. Blockchain-based total authentication mechanisms can leverage decentralized consensus protocols and cryptographic strategies to steady biometric data and authentication transactions. Chaotic structures can be applied to generate and manipulate cryptographic keys, improving the resilience of blockchain-primarily based authentication in opposition to diverse cyber threats, consisting of tampering and identity robbery [54].
- **IoT Security**
  - The proliferation of Internet of Things (IoT) devices underscores the significance of robust security mechanisms for protecting touchy information and resources. Chaotic-based totally passkey safety can offer stronger safety for IoT gadgets by way of offering lightweight but resilient authentication solutions. Secure IoT ecosystems leveraging

chaotic systems can mitigate vulnerabilities such as unauthorized rights of entry, records breaches, and device tampering, thereby ensuring the integrity and confidentiality of IoT deployments [55].

- **Post-Quantum Cryptography**
    - With the arrival of quantum computing, conventional cryptographic algorithms are prone to being damaged through quantum algorithms. Chaotic structures offer capacity solutions for publish-quantum cryptography, wherein traditional cryptographic techniques can also no longer be steady. Chaotic-based encryption and authentication schemes can offer quantum-resistant safety guarantees, ensuring the confidentiality and integrity of touchy statistics in post-quantum computing technology [56].
- **Biometric Wearables and Implants**
    - The integration of biometric sensors into wearable gadgets and implants opens up new avenues for steady and seamless authentication reports. Chaotic-primarily based passkey protection may be embedded into biometric wearables and implants to provide non-stop and dependable authentication for users. These wearable authentication solutions provide comfort, mobility, and biometric statistics fusion skills, improving consumer stories whilst making sure of robust protection against unauthorized get entry [57].
- **Privacy-Preserving Authentication**
    - Preserving consumer privacy is paramount in biometric security structures to cope with worries regarding statistics, privateness and protection. Chaotic-primarily based authentication mechanisms can facilitate privacy-maintaining authentication protocols by encrypting biometric information and passkeys the usage of chaotic dynamics. Privacy-improving strategies including homomorphic encryption and secure multiparty computation may be incorporated with chaotic-based total authentication to permit secure biometric authentication without compromising a person's privateness [58].
- **Standardization and Interoperability Efforts**

    Standardization of our bodies and enterprise consortiums plays an important role in driving the adoption and interoperability of chaotic-primarily based biometric safety solutions. Collaborative efforts to broaden commonplace standards, protocols, and interoperability frameworks for chaotic-primarily based authentication structures can boost their integration into information-era ecosystems. Standardization projects targeted at making sure compatibility, scalability, and security can foster innovation and promote the vast adoption of chaotic-based biometric safety solutions [59].

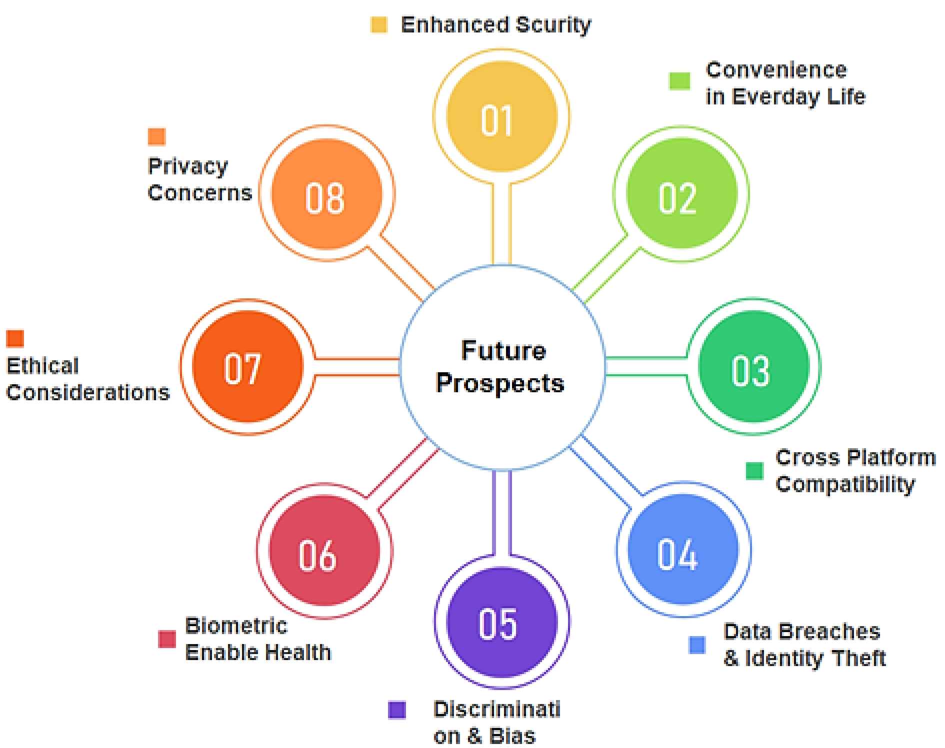

Figure 6: Future prospects for biometric security with chaotic systems.

In conclusion, the future possibilities for biometric safety in the data era and the use of chaotic structures for superior passkey safety are promising, pushed by way of technological advancements, interdisciplinary collaboration, and evolving safety requirements. By leveraging rising technologies along with AI, quantum computing, blockchain, and IoT, chaotic-primarily based authentication structures can offer remarkable tiers of security, privacy, and value in diverse application domains.

Continued studies, innovation, and standardization efforts are important to understand the whole capability of chaotic-primarily based biometric security answers and deal with the evolving demanding situations of cybersecurity inside the virtual age [60].

Table 2: Main Abbreviations.

Abbreviations	Description
AI	Artificial Intelligence
ML	Machine Learning
RNN	Recurrent Neural Network
CNN	Convolutional Neural Network
DNA	Deoxyribonucleic Acid
IoT	Internet of Things
ISO	International Organization
IEC	International Electrotechnical Commission
IDS	Intrusion Detection Systems
PIN	Personal Identification Number
PC	Personal Computer

6 Conclusion

The integration of chaotic structures for superior passkey safety in biometric security affords a promising street for enhancing authentication mechanisms and bolstering cybersecurity. Throughout this paper, we have explored the challenges, novel techniques, and destiny potentialities related to leveraging chaotic dynamics in authentication structures. We have identified several challenges, such as complexity and computation, parameter sensitivity, robustness, protection analysis, biometric statistics variability, usability, standardization, and resource constraints. Addressing these challenges will require interdisciplinary collaboration and the improvement of sturdy and adaptable answers via rigorous testing and validation. Furthermore, we have highlighted numerous novel factors delivered by using chaotic-primarily based passkey protection, consisting of the utilization of chaotic dynamics, nonlinear authentication mechanisms, adaptive parameterization, biometric records fusion, dynamic security evaluation, human-centric layout standards, and interdisciplinary collaboration. Looking ahead, the future potentialities for biometric safety and the use of chaotic systems are promising. Integration with AI and system mastering, exploration of quantum chaotic structures, blockchain-based authentication, IoT security, submit-quantum cryptography, biometric wearables and implants, privacy-maintaining authentication, and standardization efforts are predicted to shape the panorama of biometric protection in the coming years. In the end, persistent research, innovation, and collaboration efforts are important to realize the overall capacity of chaotic-primarily based biometric protection solutions and cope with the evolving challenges of cybersecurity within the digital age. By leveraging emerging technologies and interdisciplinary strategies, we can beautify the security, privacy, and usefulness of authentication mechanisms, in the end fostering agreement with and self-belief in virtual systems.

Acknowledgements

The authors want to express their sincere gratitude to the Dean and workforce of the Informatics Institute for Postgraduate Studies, Iraqi Commission for Computers & Informatics, Baghdad, Iraq, for his or her beneficial steering and guidance. We also amplify our appreciation to the researchers whose contributions laid the foundation for this assessment. Additionally, we acknowledge the optimistic remarks provided by our colleagues and the unwavering encouragement of our families for the duration of the education of these paintings.

Authors contribution

N. A. S. Conducted the investigations, finished the literature review, and organized the manuscript. B. M. N. Furnished guidance, critical insights, and supervision for the investigation. Both authors reviewed and authorized the final version of the manuscript.

Conflict of interests

The authors declare no conflicts of interest. No financial or non-financial relationships influenced the research, and no external funding was received for this study.

References

[1] S. Dargan and M. Kumar, A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. *Exp Sys with Appl* **143**, 113114, (2020).

[2] S. De, "Security threat analysis and prevention towards attack strategies," Cyber. Def. Mech. *CRC Press*,1-22, (2020).

[3] P. M. Rao and B. D. Deebak, "A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions," *Ad Hoc Net*. **146**, 103159, (2023).

[4] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics* **12**, 1333, (2023).

[5] K. M. Hosny, M. A. Zaki, N. A. Lashin, M. M. Fouda, and H. M. Hamza, "Multimedia security using encryption: A survey," *IEEE Access* **11**, 63027-63056, (2023).

[6] J. C. Bernal-Romero, J. M. Ramirez-Cortes, J. D. J. Rangel-Magdaleno, P. Gomez-Gil, H. Peregrina-Barreto, and I. Cruz-Vega, "A review on protection and cancelable techniques in biometric systems," *IEEE Access* **11**, 8531-8568, (2023).

[7] S. Sood and M. Vanitha, "Password Authentication Using Keystroke Biometric," Manag. Secu. Serv. in Heter. Net.: *CRC Press*, 75-112, (2020).

[8] M. Lehto, "Cyber-attacks against critical infrastructure," Cyber secu.: Critic. Infras. Prot.: *Springer*, 3-42, (2022).

[9] C. Bonn, "The systemic change from the use of biographical evidence of identity to a biometric self-service model of multi-modal authentication: A case study of the paradigm shift in a Finnish government agency's identity management, **Student Thesis** (2023).

[10] A. Ezugwu et al., "Password-based authentication and the experiences of end users," *Scient. Afric*. **21**, e01743, (2023).

[11] P. A. Thomas and K. Preetha Mathew, "A broad review on non-intrusive active user authentication in biometrics," Jour. Ambie. Intellig. *Hum. Compu*. **14**, 339-360, (2023).
[12] M. Marani, M. Soltani, M. Bahadori, M. Soleimani, and A. Moshayedi, "The role of biometric in banking: A review," *EAI Endor. Trans. AI Robot*. **2**, (2023).
[13] A. H. El-Kady, S. Halim, M. M. El-Halwagi, and F. Khan, "Analysis of safety and security challenges and opportunities related to cyber-physical systems," *Proc. Safet. Envir. Prot.* **173**, 384-413, (2023).
[14] Y. Aydın and F. Özkaynak, "Automated Chaos-Driven S-Box Generation and Analysis Tool for Enhanced Cryptographic Resilience," *IEEE Access* **12**, 312-328 (2023).
[15] J. E. Glenn, "Chaos theory: the essential for military applications," *US Nav. War Colleg. Press*, (1996).
[16] S. A. Shawkat, N. Tagougui, and M. Kherallah, "Optimization-based pseudo random key generation for fast encryption scheme," *Bulletin of Electrical Engineering and Informatics* **12**, 1007-1018, (2023).
[17] A. Ambhaikar, "A Novel Chaos-Based Encryption Algorithm for Secure Communication Systems," *Commun. Appl. Nonli. Analy*. **30**, 24-39, (2023).
[18] [18] Y. K. Saheed, T. O. Kehinde, M. Ayobami Raji, and U. A. Baba, "Feature selection in intrusion detection systems: a new hybrid fusion of Bat algorithm and Residue Number System," *Journ. Inform. Teleco*. **8**, 1-19, (2023).
[19] V. R. Falmari and M. Brindha, "Privacy preserving biometric authentication using chaos on remote untrusted server," *Measurement*, **177**, 109257, (2021).
[20] C. Kumar and S. Singh, "Security standards for real time video surveillance and moving object tracking challenges, limitations, and future: a case study," *Multim. Tool. Appl*. **83**, 1-32, (2023).
[21] M. Hammad et al., "Security Framework for Network-Based Manufacturing Systems with Personalized Customization: An Industry 4.0 Approach," *Sensors* **23**, 7555, (2023).
[22] L. L. Delina, N. P. P. Ludovice, J. Gaviola, and R. Cagoco-Guiam, "Living with climate and state fragility in a “chaotic paradise:” securitizing livelihoods in the Philippines’ Cotabato River Basin," *Clim. Ris. Manag*. **42**, 100558, (2023).
[23] J. Zhu and X. Liu, "An integrated intrusion detection framework based on subspace clustering and ensemble learning," *Comput. Electr. Eng*. **115**, 109113, (2024).
[24] P. Kaur, N. Kumar, and M. Singh, "Biometric cryptosystems: a comprehensive survey," *Multim. Tool. Appl*. **82**, 16635-16690, (2023).
[25] A. Mehmood, A. Shafique, M. Alawida, and A. N. Khan, "Advances and vulnerabilities in modern cryptographic techniques: A comprehensive survey on cybersecurity in the domain of machine/deep learning and quantum techniques," *IEEE Access* **12**, 27530-27555, (2024).
[26] J. Ramkumar, K. J. Marseline, and D. Medhunhashini, "Relentless Firefly Optimization-Based Routing Protocol (RFORP) for Securing Fintech Data in IoT-Based Ad-Hoc Networks," *Int. J. Comput. Net. Appl* **10**, 668-687, (2023).
[27] R. Sujarani, D. Manivannan, R. Manikandan, and B. Vidhyacharan, "Lightweight bio-chaos crypt to enhance the security of biometric images in internet of things applications," *Wirel. Pers.l Commun*., **119**, 2517-2537, (2021).
[28] O. S. Faragallah et al., "Efficient chaotic-Baker-map-based cancelable face recognition," *Jour. Ambi. Intellig. Hum. Comput*., 1-39, (2023).
[29] W. Abdul, O. Nafea, and S. Ghouzali, "Combining watermarking and hyper-chaotic map to enhance the security of stored biometric templates," *Comput. Jour*. **63**, 479-493, (2020).
[30] F. Pandey, P. Dash, D. Samanta, and M. Sarma, "Efficient and provably secure intelligent geometrical method of secret key generation for cryptographic applications," *Comput. Electr. Eng*. **101**, 107947, (2022).
[31] O. F. Boyraz, E. Guleryuz, A. Akgul, M. Z. Yildiz, H. E. Kiran, and J. Ahmad, "A novel security and authentication method for infrared medical image with discrete time chaotic systems," *Optik* **267**, 169717, (2022).
[32] H. A. A. Eldawy, W. El-Shafai, E. E.-D. Hemdan, G. M. El-Banby, and F. E. A. El-Samie, "A robust cancellable face and palmprint recognition system based on 3D optical chaos-DNA cryptosystem," *Optic. Quant. Electr*. **55**, 970, (2023).
[33] S. Artabaz, L. Sliman, K. Benatchba, and M. Koudil, "Optimized multi-biometric enhancement analysis," *IET Biometrics* **10**, 326-341, (2021).
[34] M. Taha, M. M. Selim, and A. Yousry, "A Secured Digital Handwritten Signature Prototype for Visually Impaired People," *Internat. Jour. Intellig. Eng. & Sys.* **13**, (2020).
[35] W. El-Shafai, F. A. H. E. Mohamed, H. M. Elkamchouchi, M. Abd-Elnaby, and A. Elshafee, "Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm," *IEEE Access* **9**, 77675-77692, (2021).
[36] S. S. Pillalamarri, K. Saikumar, M. Q. Mohammed, A. R. Hassan, R. M. Ahmed, and S. H. Ahammad, "A deep intelligence-based face spoofing liveness recognition in pandemic," *AIP Confer. Procee*., **2845**, (2023).
[37] R. Nagakrishnan and A. Revathi, "A robust cryptosystem to enhance the security in speech based person authentication," *Multim. Tool. Appl*. **79**, 20795-20819, (2020).
[38] S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, and X. Tang, "EFR-CSTP: Encryption for face recognition based on the chaos and semi-tensor product theory," *Informat. Sciences* **621**, 766-781, (2023).
[39] S. M. Abdullahi and H. Wang, "Robust enhancement and centroid-based concealment of fingerprint biometric data into audio signals," *Multim. Tool. Appl*. **77**, 20753-20782, (2018).
[40] X. Sun et al., "LDI-MVFNet: A Multi-view fusion deep network for leachate distribution imaging," *Wast. Manag*. **157**, 180-189, (2023).
[41] B. Rahul, K. Kuppusamy, and A. Senthilrajan, "Bio-Metric Based Colour-Image-Encryption using Multi-Chaotic Dynamical Systems and SHA-256 Hash Algorithm," *Inf. Secur. Jour., Glob. Persp*. **33**, 1-25, (2023).
[42] [42] J. Li, T. Fu, C. Fu, and L. Han, "A novel image encryption algorithm based on voice key and chaotic map," *Appl. Scienc*. **12**, 5452, (2022).
[43] R. Grillo, B. A. Q. Reis, B. C. Lima, L. A. P. F. Pinto, J. B. C. Meira, and F. Melhem-Elias, "The butterfly effect in oral and maxillofacial surgery: Understanding and applying chaos theory and complex systems principles," *Jour. Cran.Maxill. Surg*., (2024).
[44] Z. Lin, W. Junhao, Q. Jianchun, C. Min, and J. Minping, "Sensitivity influence of initial crack characteristics on structural damage propagation based on the VB-PCE model and POD reduced order algorithm," *Reliab. Eng. Sys. Safet*. **240**, 109551, (2023).

[45] I. Almomani, W. El-Shafai, A. AlKhayer, A. Alsumayt, S. Aljameel, and K. Alissa, "Proposed biometric security system based on deep learning and chaos algorithms," *Comput. Mater. Contin* **74**, 3515-3537, (2023).
[46] Z. Man, "Biometric information security based on double chaotic rotating diffusion," *Chao., Solit. Fract*. **172**, 113614, (2023).
[47] A. K. Jain, D. Deb, and J. J. Engelsma, "Biometrics: Trust, but verify," *IEEE Trans. Biom. Beha. Ident. Scien*. **4**, 303-323, (2021).
[48] B. Zhang and L. Liu, "Chaos-based image encryption: Review, application, and challenges," *Mathematics* **11**, 2585, (2023).
[49] U. Kumar, M. Garg, and G. Kaushik, "Development and analysis of attack-resilient three party authenticated key agreement scheme based on chaotic maps for secure communication," *Clust. Comput*. **27**, 1-15, (2024).
[50] J. J. Ang'udi, "Security challenges in cloud computing: A comprehensive analysis," *Worl. Jour. Advan. Eng. Tech. Scien*. **10**, 155-181, (2023).
[51] R. Termanini, "Biomedical Defense Principles to Counter DNA Deep Hacking," *Academ. Press*, (2022).
[52] J. Hwang et al., "Machine learning in chaos-based encryption: Theory, implementations, and applications," *IEEE Access* **11**, 125749-125767, (2023).
[53] K. Kawabata, A. Kulkarni, J. Li, T. Numasawa, and S. Ryu, "Symmetry of open quantum systems: Class. Dissip. Quant. chaos," *PRX Quant*. **4**, 030328, (2023).
[54] M. M. Khayyat, M. M. Khayyat, S. Abdel-Khalek, and R. F. Mansour, "Blockchain enabled optimal Hopfield Chaotic Neural network based secure encryption technique for industrial internet of things environment," *Alex. Eng. Jour.* **61**, 11377-11389, (2022).
[55] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review," *Sensors, vol*. **23**, 4117, (2023).
[56] B. Paul and G. Trivedi, "Post Quantum Cryptography Algorithms: A Review and Applications," Intern. Conf. Intellig. Tech., *Springer*, 3-17, (2022).
[57] C. V. Anikwe et al., "Mobile and wearable sensors for data-driven health monitoring system: State-of-the-art and future prospect," *Exp. Sys. Appl*. **202**, 117362, (2022).
[58] T. Zhang, J. Shen, H. Yang, V. Pandi, B. B. Gupta, and V. Arya, "Sustainable Authentication and Key Agreement Protocol Using Chaotic Maps for Industry 5.0," *IEEE Trans. Consu. Electr*. **70**, 1580-1589, (2023).
[59] A. Chaoub et al., "Hybrid self-organizing networks: Evolution, standardization trends, and a 6G architecture vision," *IEEE Commun. Stand. Mag*. **7**, 14-22, (2023).
[60] M. Thakur, "Cyber Security Threats and Countermeasures in Digital Age," *Jour. Appl. Scien. Educat. (JASE)*, 1-20, (2024).