Qeios

A Unified Framework for Cyber Oriented Digital Engineering using Integration of Explainable Chaotic Cryptology on Pervasive Systems

Devisha Arunadevi Tiwari*[1,2] | Bhaskar Mondal[1]

[1]Department of Computer Science and Engineering, National Institute of Technology, Patna, Bihar, 800005, India
[2]Department of Computer Science Engineering(Data Science), Ace Engineering College (Autonomous), Hyderabad, Affiliated to Jawaharlal Nehru Technological University Hyderabad, Telangana, 501301, India

Correspondence
*Devisha Arunadevi Tiwari. Email: devishaarunadevitiwari@gmail.com

Present Address
Department of Computer Science and Engineering, National Institute of Technology,Patna, Bihar, 800005, India.

Abstract

Cyber Oriented Digital Engineering (CODE) aims to safeguard pervasive systems, cyber physical systems (CPS), internet of things (IoT) and embedded systems (ES) against advanced cyberattacks. Cyber oriented digital engineering pilots are earnestly required to secure transmission and credential exchanges during machine to machine (M2M) zero trust (ZT) communication. In order to construct the CODE pilot as a pivot of zero trust (ZT) communication, systems engineering employing chaotic cryptology primitives has been investigated. The empirical results with analysis of findings on its integration on real life platforms are presented as a pervasive framework, in this work. The focus was bestowed in developing an explainable approach, addressing both ante hoc and post hoc explanation needs. Ante hoc explanation ensures transparency in the encryption process, fostering user trust, while post hoc explanation facilitates the understanding of decryption outcomes.

The properties of explainable approaches are investigated, emphasizing the balance between security and interpretability. Chaotic systems are employed to introduce a dynamic layer of complexity, enhancing encryption robustness. The article aims to contribute to the evolving field of explainable chaotic cryptology, bridging the gap between cryptographic strength and user comprehension in CODE pilot based zero trust (ZT) exchanges in multimedia content protection.

Thus, this research is a communication brief case containing significant early findings and groundbreaking results studied as a part of a longer, multi-year analysis. Innovative techniques and pragmatic investigations have been discussed as a part of result dissemination in the empirical findings.

KEYWORDS:
multimedia content protection; CODE pilot; chaotic cryptology primitives; ante hoc explanation; post hoc explanation.

1 | INTRODUCTION

Chaotic Cryptology (CC) refers to a series of nonlinear dynamical systems that multimedia systems use to secure the transmission of multimedia content and protect its integrity. It is fundamental to recent advances in data security, and has been successfully

https://doi.org/10.32388/60NK7H

integrated into security-relevant systems, such as, Industry Control Systems, Optical Ethernet, RFID Security and Industrial Ethernet in healthcare, biomedical and medical sectors through Wireless Body Area Network (WBAN), Smart Body Area Network (SBAN) wherein chaotic cryptology algorithms encode confidential data to unreadable form for security, confidentiality and integrity. Chaotic primitives are non-linear components or cryptographic constructs. Without the need to explicitly design a cryptographic model and output the results, Chaotic Cryptology techniques provide security applications with the capability to automatically provide confidentiality, integrity and availability through homomorphic encoding. But due to the fact that there is no clear explanation, the security sector faces a number of difficulties:

1. **Problem 1**

   Multimedia systems are high susceptible to cyberthreats. There is no way to detect the origins of attack and profile of the intruder. Existing systems use machine learning and neural networks for the design of multimedia content protection algorithms which work on statistical approaches, hence they can be easily compromised using reverse engineered statistical models.

2. **Problem 2**

   Multimedia content protection systems use several techniques such as multimedia encryption, digital rights management, digital watermarking and multimedia fingerprinting. but these systems have their own limitations and weaknesses. Eventhough amicable integration of advanced approaches such as blockchain smart contract, proof-of-work (PoW), proof-of-concept (PoC) in modern security constructs deter cyber assaults but they are not efficient to be adopted in technology these being highly complex for pretty good privacy used in secure transmission and secure communications.

3. **Problem 3**

   Promotion and adoption of technology and security vulnerabilities due to improvised decentralization to trusted third party systems have induced threats to the access control mechanisms thus increasing the possibility of becoming single point of failure.

4. **Problem 4**

   Moreover, interoperability is an essential concern because there are no universal standards. According to a 2006 report from the Computer Emergency Response Team (CERT), there has been a significant increase in security vulnerabilities that endanger multimedia big content. According to Li et al. 2006,[1], these attacks target multimedia big data originating from heterogeneous cyber physical and social computing (CPSC) platforms.

In order to meet the requirements of explainable chaotic cryptology (CC), a deep intensive research on improvising the capability of providing explanations of CC methods. To meet the needs of explainable Chaotic Cryptology (CC), more and more intensive research on improving the capability of providing explanations of CC methods. It has been proven that various explainable methods can help the target users to make them understand how do they work. These methods help them decide whether they can trust the security provided by the chaotic cryptology primitives. Therefore, to demonstrate the explanations given by chaotic cryptology in the domain of multimedia security, we validate the behaviour of secured systems to assist the chaotic cryptology developers revive their methods to deter inconsistencies, integration errors and precision errors to safeguard the target model. In chaotic cryptography, thousands of schemes to secure multimedia content exists, providing multi-factor security explanations through vivid security constructs such as multimedia watermarking, multimedia digital rights management, multimedia fingerprinting etc. The users of these security constructs are able to focus and pay more attention on integration of these constructs and incorporating their control variables into target systems wherein the explanations let them think about the questions that:

RQ1: Which security construct is more suitable and is promising on practical platforms?

RQ2: What requirement necessitates these systems to meet the security expectations from the end users?

RQ3: Will the end user accept the reliability and trustworthiness of the security assurance provided by chaotic multimedia ciphers?

Explanations provide trust in chaotic cryptology methods, that exemplify the importance of explainable chaotic cryptology (XCC). Explainable chaotic cryptology (XCC) plays a pivotal role because it fosters trust towards chaotic cryptology solutions.

Computational intelligence approaches such as swarm intelligence, fuzzy logic, artificial neural networks, evolutionary algorithms, genetic algorithms and differential algorithms when used into the construction of chaotic cryptology primitives, they re-instantiate the intellects of human cryptography professionals, as a paradigm of transfer learning. In this work, a careful research on computational intelligence inspired chaotic cryptology (XCC) is shared alongwith a detailed discussion and setup on how it may be used for security, privacy, and trust as a model of workable computational intelligence in chaotic cryptology. Many approaches to the explanation of security systems have been investigated recently. Experts in multimedia security have begun to create models to comprehend chaotic cryptology (CC) in multimedia security, such as identifying weaknesses in data transmission, detecting security loopholes, and detecting probable attacks on chaotic cryptology based integrated systems. In order to better comprehend the decision-making process, these explainable techniques can assist in tracing the weakness in security solutions made by chaotic cryptology primitives back to the security input.

1.1 | Our Contribution

1. In this review, we outline the process for creating explainable methods as well as the two main categories of explainable chaotic cryptology techniques used in multimedia security: ante-hoc and post-hoc explanations.
2. Additionally, we provide a detailed explanation techniques of the description of the two groups along with their advantages and disadvantages to assist in the selection of approaches on a variety of real-world commercial domains, including banking, financial transactions, and cloud-based multimedia storage solutions.
3. The three concepts of cryptography—confidentiality, integrity, and availability, or the CIA triads—that this paper addresses and provides a foundation for the implementation and trust in the strength of non-linear chaotic primitives.

1.2 | Paper Organization

To assist researchers in selecting the most explainable methodologies for their work, comparative studies based on rigorous evaluation metrics are presented. Furthermore, using a particular occurrence timeline, we methodically summarize and analyze any unresolved issues. This will make it easier for readers to comprehend milestones, essential problems, and clarifying things. This is how the remainder of the survey is structured. Section 2 provides an overview of the role of explanations in multimedia content protection major four domains. We discuss the ante-hoc and post-hoc explanation setup; taxonomy of explainers and their approaches in multimedia content protection. In section 3, we discuss the desirable properties of ante-hoc explanation versus post-hoc explanation with respect to the idealistic characteristics of any explainable software systems. Then in its subsection, we discuss, the very specific properties expected from chaotic cryptology based implementation constructs (XCC) for multimedia security, as a part of ante-hoc versus post-hoc approaches used within them. In section 4 we discuss well-tested ante-hoc approaches studied and analysed in the literature survey process, whereas in section 5, we discuss the same but for post-hoc approaches. In section 6 we perform a strict and vigorous feasibility analysis, security assurance, practicability and applicability of the ante-hoc versus post-hoc approaches studied in the literature survey. In section 7, we discuss timeline and open issues in the prevailing systems and in section 8, we discuss the provable design principles as the vigorous study in this survey. We present a discussion on the proposed solution and mitigation approaches in section 9 and discuss the usability of the proposed explainers in section 10, in realistic domains for future research. Finally in section 11, we summarize the findings and present the concluding remarks of the proposed survey.

2 | EXPLANATIONS IN MULTIMEDIA CONTENT PROTECTION

2.1 | Role of Explanations in Multimedia Security

If data, scripts or other artefacts used to generate the analyses presented in the article are available via a publicly available data repository, please include a reference to the location of the material within the article. Numerous studies looked at various security concerns and attempted to determine where they originated; however, the findings did not show a discernible decrease in vulnerabilities. In the security domain, explanations are crucial for assisting users in making decisions and determining the root reasons. When it comes to security systems, chaotic cryptology explanations help users comprehend three key concepts: (1) the construction of the security system model; (2) what makes a particular case malevolent and why it can be exploited; and

(3) how to utilize a system safely. While explanations for chaotic cryptology (CC) have been investigated and proven effective in a number of application domains, such as as blockchain transactions, multimedia broadcast and secure transmission, but chaotic cryptology has not yet given multimedia security a considerable thought.Explainable chaotic cryptology has been used in multimedia security in the areas shown in figure 1 . The following classifications of applications in the multimedia security sector are specifically covered in this study:

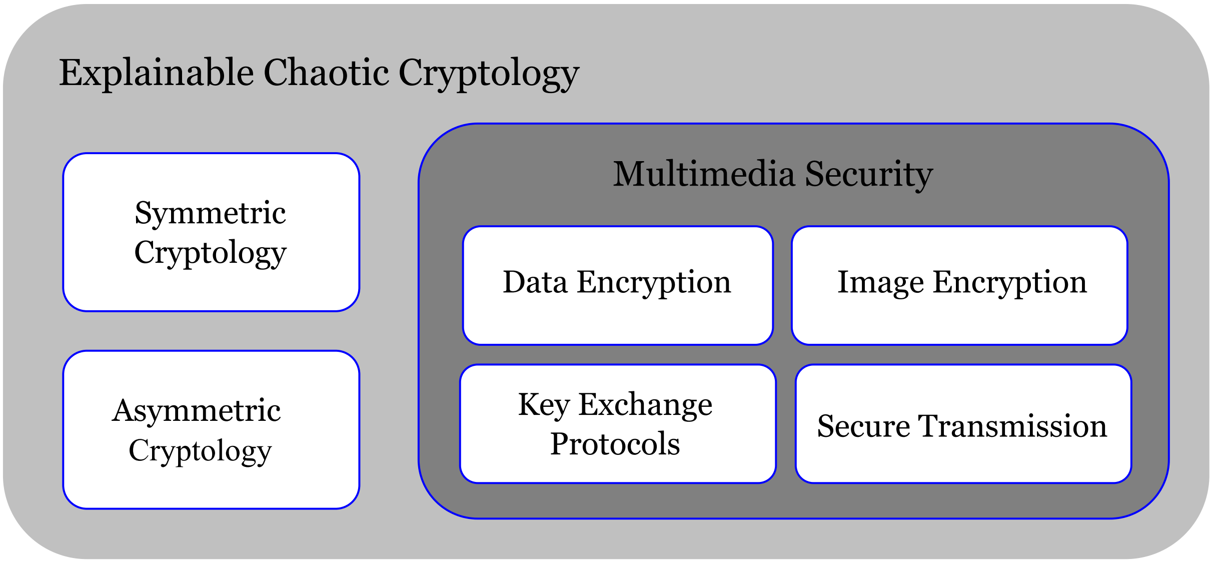

FIGURE 1 Explainable Chaotic Cryptology (XCC) for Multimedia Security. The four major broad domain where chaotic cryptology have been successfully applied are data encryption, image encryption, cryptographic key generation and key exchange and multimedia secure broadcast.

1. *Data Encryption*

   Multimedia content is dynamic in nature and has huge voluminous information within it. To secure multimedia transmission, chaos dynamics are applied into the design of multimedia security algorithms. Several researchers have proven in their works[2,3,1,4], the practical relevance of chaos inspired cryptology and the crypto-friendly properties provided by them. Real-time multimedia encryption uses stochastic properties of chaotic systems to synchronize the data transmission alongwith signal transmission. Radha et.al[3] devised an effective chaotic shuffler function using non-linear key-dependent transformation which encrypts 512 bit stream bitstream over a blocksize of 512 bits each. Hasimoto Rogelio[2] constructed an N-map chaotic array using three level perturbation scheme. Li et.al[1] discussed the transcodability, video on demand property, syntax-aware multimedia encryption, electronic codebook (ECB) and cipher block chaining (CBC) modes off encryption using chaotic cryptology and their practical relevance in multimedia security. Li et.al[1] addressed several issues of chaotic diffusion and the time taken for iterative chaotic diffusion schemes to encrypt bulky multimedia content. Li et.al[1] differentiated between traditional image processing based methods and classical cryptographic algorithms in multimedia security versus need of advanced chaotic cryptology primitives for high end task such as video and audio multimedia encryption. Li et.al, 2022[4] constructed a chaotic oscillation based multimedia cryptosystem to be used on IoT platforms.

2. *Image Encryption*

   Image encryption versus data encryption are completely different task and there exist no algorithm to do both with complete assurance and same level of security expectations. Traditional approaches used wavelet decomposition and pixel position scrambling methods to encrypt the images But chaotic cryptology has proven very beneficial to be the best candidate for image encryption. Masuda N,Jakimoski G., Kazuyuki A. and Kocarev L. et. al[5] derived a uniform structure having key addition, SBox substitution, permutation and linear mixing layer to implement block cipher for image encryption. Chaotic block ciphers, chaotic non-linear transformation, chaotic feistel cipher, chaotic uniform cipher 128 bit using

16 active SBoxes and their practical security concerns have been discussed in[5]. Masuda N,Jakimoski G., Kazuyuki A. and Kocarev L. et. al[5] prove the practical reliability of chaotic ciphers as a competent security construct in image encryption. Authors[5] illustrate the provable security of these chaotic cryptology constructs and the desirable degree of randomness associated with them. Xiaoling Huang in 2012[6] proved the cryptographic properties of Chebyshev Chaotic map that it is orthogonal, recursive, it has a chaotic behaviour and has a chaotic state within (-1, 1) and can generate pseudorandom sequences since its largest lyapunov exponent λ is 1.25 >0.

3. *Key Exchange*

   Secure multi party computation requires assured key exchange. In past decades, there have been several key exchange modalities such as privacy-aware end-to-end authenticated key exchange (PAE2EAKE), Client-to-Client Password-Authenticated Key Exchange (C2C-PAKE) in the cross-realm setting where two clients are in two different realms and hence two servers involved, one-way authenticated key agreement scheme (OWAKE) based on chaotic maps with multi-server architecture. The OWAKE scheme is widely used to no need for mutual authentication environment on Internet, such as consumer-to-trader model in online commodity exchange. Zhu et. al[7] illustrated the limitations and issues in traditional key exchange mechanisms and their inherent weakness causing key-theft and password leakage attacks. Zhu et.al[7] derived PAKE using Chebyshev Chaotic Maps and their cryptographic hardness in breaking them in a given episode. Traditional schemes require restricting access to multimedia multi-casts and the necessity of distribution of the rekeying messages and the key management problem.

4. *Multimedia Secure Broadcast*

   Ren et. al[8] discussed the troubles of using traditional multimedia secure broadcast scheme such as 3GPP. For multicast contents, 3GPP developed the key management mechanism (KMM) in evolutionary multimedia broadcast/multicast service (eMBMS) to offer both bidirectional security. Ren et.al[8] highlighted that KMM may result in rekeying and re-authentication problems often because of the features of eMBMS, specifically due to a large number of group members, a dynamic group topology and unforeseen wireless disconnections. User equipment (UE) interfaces and mobile carriers continue to be impacted with these issues. It seems reasonable to extend the rekeying period in order to mitigate the difficulties. However, a long rekeying period is not seen as the best operational choice because content providers lose out on revenue thereby affecting their business. Trappe et. al[9] illustrated that the problems of maintaining and distributing keying information in traditional schemes is necessary to address the issue of restricting access to multimedia multi-casts. Usually, the distribution of the rekeying messages and the key management problem should be taken into consideration independently. Two methods for disseminating the rekeying messages related to secure group communication are offered by multimedia sources. The most traditional method uses a media-independent channel to provide signals about rekeying. However, the authors Ren et.al[8] illustrated a different strategy that uses a media-dependent channel and is accomplished for multimedia through the application of data embedding techniques. A chaotic cryptography system has subsequent essential features that define a good quality keystream produced by a cryptographic system. Necessarily it obeys randomness, repeatability, unpredictability and long period. Randomness: It should have strong statistical features and pass the majority of widely used standard randomness tests. Repeatability: Using the same seed results in the same output sequence. So, the chaotic keystream is re-initialized in every iteration. Unpredictability: Regardless of prior knowledge of the bits sequence, the next output bit is unpredictable if the seed is unknown. Long Period: The pseudo-random sequence is produced by a deterministic algorithm with a predetermined period that needs to be as long as feasible.

2.2 | Explanation Setup in Multimedia Security

Differentiable approaches for chaotic cryptology in multimedia security may be identified based on whether the explanations are produced by cryptographically designed secure models (post hoc) or by a self-explanatory chaotic map based secure models (ante hoc). In multimedia security, ante hoc and post hoc explanations are dependent upon distinct design processes. Figure 2 and figure 3 depict the processes involved in providing users with explanations in ante hoc and post hoc scenarios, respectively.

2.2.1 | Ante-hoc Explanation Setup

The explanatory models incorporate explanation-generating modules into their design to provide reasoning of their security assurance, as seen in the ante hoc explanation workflow in Figure 2 . These models use a variety of chaotic cryptology primitives

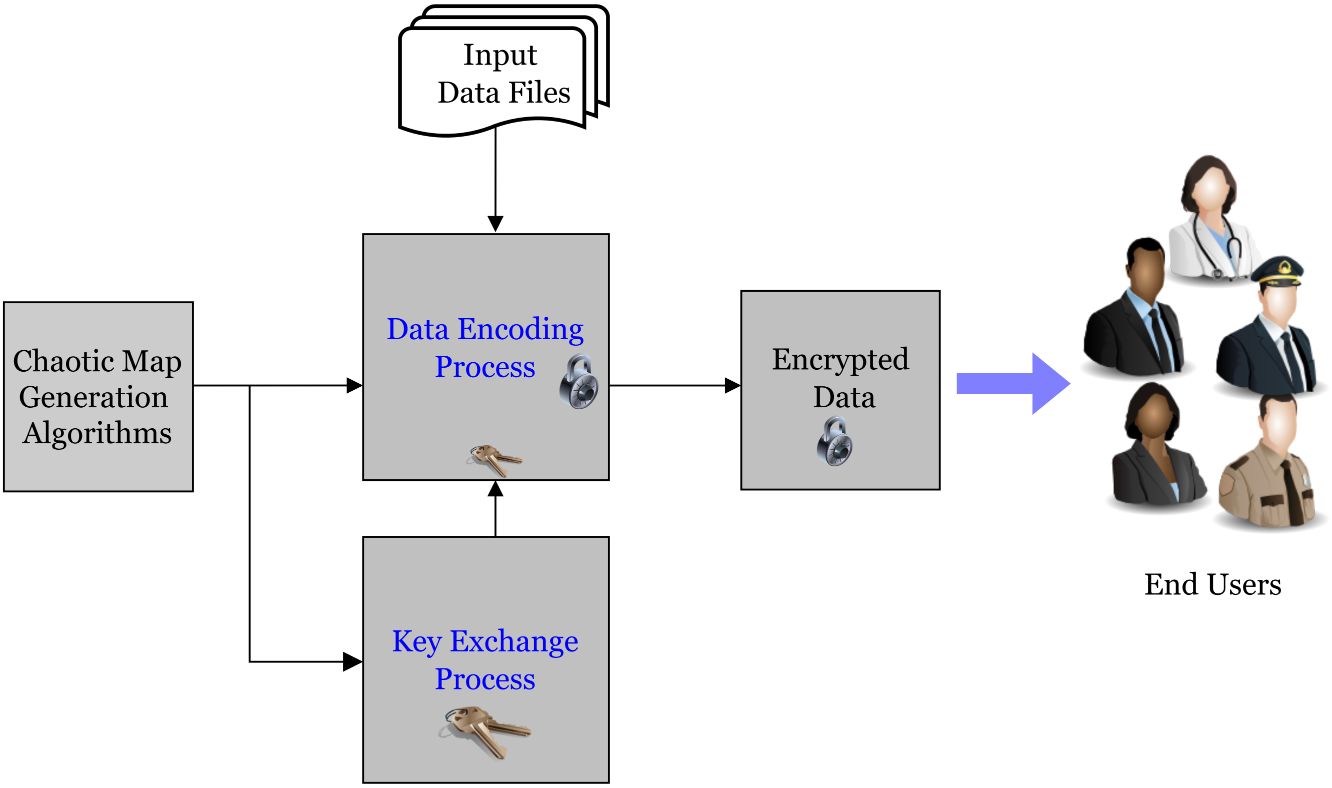

FIGURE 2 Ante hoc explanation workflow in multimedia security: chaotic systems with well tested crypto-friendly primitives produce secured outputs and explanations on security coverage.

and operations to induce cryptographic complexity related to explainable models. The functionalities of these models have the power to impose security measures for non-repudiation, secrecy, integrity, and authentication. They could also offer a justification for the security assurances. Additional data controls appear in the explainable output, which provides significant context for understanding the logic behind the security restrictions. With the use of explainable modeling, ante hoc explanations limit the complexity of the model. It creates models that are more explicable by nature. Anthropomorphic or humanistic explanations are utilized for inherently comprehensible modeling.

2.2.2 | Post-hoc Explanation Setup

Applying an explainable method to a target model—typically a black-box model—is known as a post-hoc explanation. After multimedia reshaping and compression as well as data transformation and reduction, post hoc explanations concentrate on interpretable techniques (such as pixel permutation, shuffling, scrambling, row-column transformation, and replacement). In addition to being utilized as surrogate or proxy models, post hoc explainable procedures are employed to obtain explanations for pre-developed models but for those target systems which cannot be fixated with ante-hoc models. In order to provide explainable security assurance and the security controls employed within them, post hoc explanations might be used in systems who wish to maintain privacy and their system architecture cannot be made transparent publicly such as online banking systems and online trading.

The workflow for the post hoc explainable techniques is depicted in Figure 3 and consists of three interconnected modules: (1) the non-linearity adder module, which eliminates statistical relationships to protect guess-work by the adversary for the current multimedia data, (2) the data encoding process to mask the original data and (3) the key-exchange module, which makes accomplishment of security assurance. Information encoding (IC) for security assurance is the process of concealing the information to make it readable only to the authorized user. It can make use of several mathematical constructs to enable rule based data access control. The encodings generated by the chaotic non-linearity module are independent of the explanation module. The target recipient can only assess the security but cannot explain how the data/information is protected.

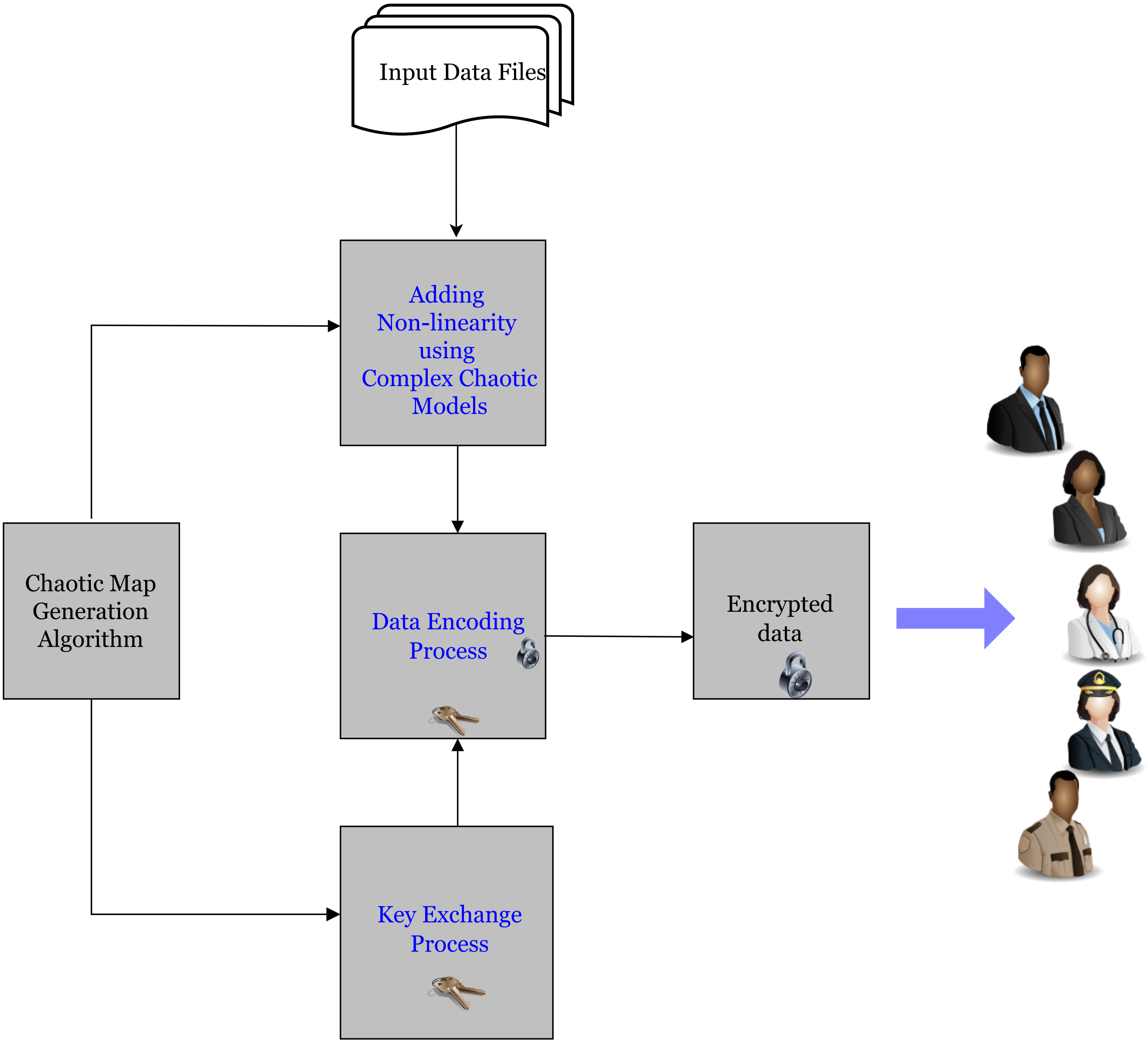
Input Data Files
Adding Non-linearity using Complex Chaotic Models
Chaotic Map Generation Algorithm
Data Encoding Process
Encrypted data
Key Exchange Process

FIGURE 3 Post hoc explanation workflow in multimedia security: the well tested cryptographically designed security model outputs security coverage, and the joint chaotic cryptology primitive acts as an explainable method and outputs explanations results.

2.3 | Taxonomy of explanations in multimedia security

Figure 4 displays the classification of the explanation approaches used in multimedia security at present. The entire spectrum of ante hoc and post hoc explanation is studied. Several classification criteria are used for the two categories depending on the target models and the underlying structural characteristics of the models.

2.3.1 | Ante hoc explanation type

Human-interpretable methods and algorithmic transparency characterize the ante-hoc explanation models. An ante hoc explanation model must be able to be broken down into its component fragments, which include the model's structure, control parameters, input arguments, and dimension features that provide intuitive explanation.

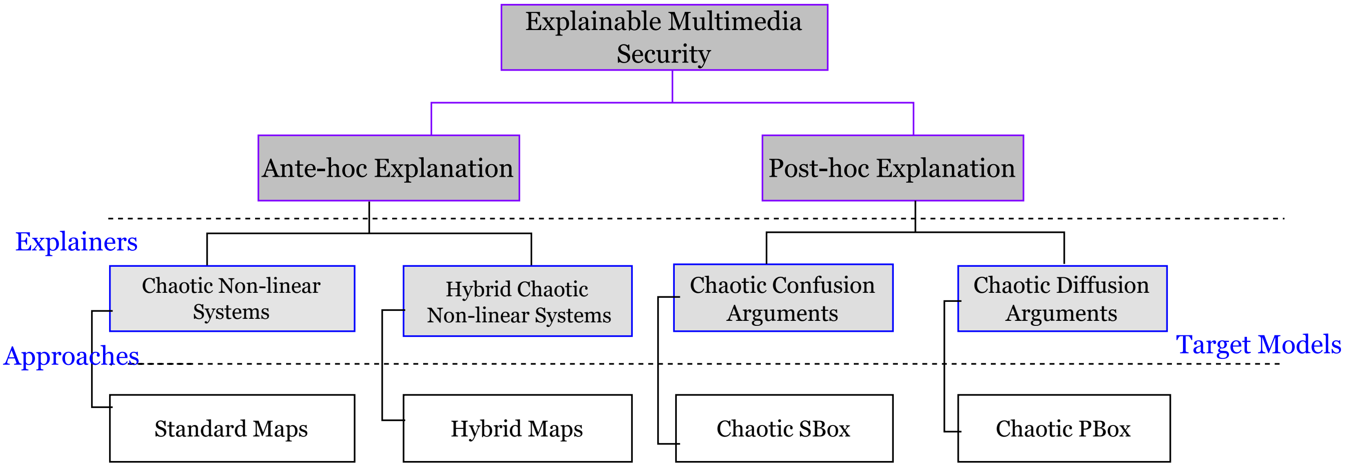
Explainable Multimedia Security
Ante-hoc Explanation
Post-hoc Explanation
Explainers
Chaotic Non-linear Systems
Hybrid Chaotic Non-linear Systems
Chaotic Confusion Arguments
Chaotic Diffusion Arguments
Approaches
Target Models
Standard Maps
Hybrid Maps
Chaotic SBox
Chaotic PBox

FIGURE 4 Taxonomy of explainable approaches in multimedia security: post hoc explanations are categorized by the target model type, whereas ante hoc explanations are categorized by the type of explainers models. The ante hoc models include derivations of chaotic non-linear systems using several standard chaotic maps such as Logistic map, Lorenz Map, Sine Map, Henon Map, Tent Map, Arnold's Map, Chirikov-Taylor's Map, Chen's Map. In the ante hoc explanations, the hybrid chaotic non-linear systems are derived from the standard maps using coupling and cascading and map expansion. The post hoc models include chaotic confusion arguments and chaotic diffusion arguments. The chaotic SBoxes are constructed from chaotic confusion arguments whereas chaotic PBoxes are constructed from chaotic diffusion arguments.

2.3.2 | Post hoc explanation type

Chaotic SBoxes and Chaotic Substitution Permutation Networks (SPN) are widely used in multimedia content protection in chaotic cryptology. In order to introduce non-linearity into the computation and prevent the adversary from determining the required functionality used in the security scheme, these constructions are required to include chaotic confusion diffusion arguments. One of the most significant advantage of these primitives is that they themselves are well tested and cryptographically designed. However, the deployment of these models still needs flexible design in order to make them integrable in existing multimedia transmission protocols.

3 | PROPERTIES OF EXPLANATION IN MULTIMEDIA CONTENT PROTECTION

Explainability refers to the capability of a system or process to provide clear and understandable reasons for its decisions or outputs. In the context of chaotic cryptology for multimedia content protection, explainability becomes crucial for transparency and user trust.

3.1 | Properties of Explainable Approaches

1. **Ante Hoc Explanation:**

    - **Transparency:** Ante hoc explanation in chaotic cryptology ensures transparency in the encryption process. Users can comprehend how their multimedia content is being secured, fostering a sense of trust in the system.
    - **User Understanding:** The properties of chaotic systems are communicated in a clear manner, allowing users to understand how the cryptographic algorithms manipulate their data before the encryption process begins.
    - **Parameter Accessibility:** Users have access to key parameters and variables involved in the chaotic encryption, enabling them to grasp the intricacies of the cryptographic operations applied to their multimedia content.

2. **Post Hoc Explanation:**

- **Outcome Interpretability:** Post hoc explanation focuses on clarifying the results of the decryption process. Users can understand why certain outcomes occurred and gain insights into the decrypted multimedia content.
- **Error Analysis:** In case of decryption errors or unexpected outcomes, post hoc explanation provides a means for users to analyze and comprehend the reasons behind such occurrences, enhancing system diagnostics.
- **Traceability:** Users can trace the cryptographic steps taken during decryption, aiding in the reconstruction of the original multimedia content. This traceability enhances the recovery process and overall system reliability.

3.2 | Characteristics of Explainable Software Systems

In chaotic cryptology for multimedia content protection, the properties of explainable approaches ensure not only robust security through chaotic systems but also a user-friendly interface where individuals can comprehend and validate the encryption and decryption processes. The integration of ante hoc and post hoc explanation contributes to a holistic understanding of the cryptosystem's functionality and outcomes. The characteristics of Explainable Software Systems are synthesized as follows,

1. **Interpretability:** - Example: The ability of a system to provide clear and understandable descriptions of its processes. - In Multimedia Content Protection: Chaotic cryptology systems should offer interpretability, explaining how chaotic dynamics are applied to encrypt and decrypt multimedia content.

2. **Traceability:** - Example: Keeping a record or trace of decisions and processes made by the system. - In Multimedia Content Protection: Users should be able to trace the steps of chaotic cryptology to understand how their multimedia content is transformed and reconstructed.

3. **User Understanding:** - Example: Ensuring that users, even without a deep technical background, can comprehend the system's actions. - In Multimedia Content Protection: Chaotic cryptology should be presented in a way that users can understand the role of chaotic dynamics in securing their multimedia data.

4. **Parameter Accessibility:** - Example: Providing access to relevant parameters and variables that influence the system's behavior. - In Multimedia Content Protection: Users should have access to key parameters of chaotic cryptology algorithms, allowing them to assess the security and functionality of the encryption process.

3.3 | Properties of Explanations in Multimedia Content Protection using Chaotic Cryptology:

By integrating these characteristics and properties, multimedia content protection systems utilizing chaotic cryptology can enhance both security and user comprehension, aligning with the principles of explainable software systems.

1. **Global explanation:**

   Definition 1. Global explanation refers to an overall understanding of the chaotic cryptology model's behavior across the entire system or dataset.

   - In Multimedia Content Protection: Understanding how the chaotic dynamics influence the encryption and decryption processes at a high-level across various scenarios and content types.

2. **Local explanation:**

   Definition 2. Local explanation focuses on explaining the behavior of the chaotic cryptology model for a specific instance or subset of instances within the dataset.

   - In Multimedia Content Protection: Explaining why the chaotic cryptology model made specific decisions or produced particular outcomes for a specific piece of multimedia content.

3. **Model-agnostic:**

   Definition 3. Model-agnostic explanations are applicable across different types of models, providing insights into the model's behavior without relying on its specific architecture.

- In Multimedia Content Protection:Providing explanations for how chaotic cryptology, irrespective of its specific algorithm, influences the security and transparency of multimedia content protection.

4. **Model-specific:**

   Definition 4. Model-specific explanations are tailored to the particular characteristics and decisions of a specific cryptographic model.

   - In Multimedia Content Protection:Explaining the nuances and intricacies of how the chosen chaotic cryptology algorithm specifically protects multimedia content, considering its unique properties.

5. **Security:** Explainers threaten the security of their target systems. Due to increasing use of AI automated systems and intensive machine learning methods, statistical analysis and breaking of cryptosystems have been recently witnessed and has posed its reliability. Security issues such transmission accuracy versus system compromise is on speculations on high end platforms such as industry 4.0 and social media sites. Moreover, cyber-physical systems have no standard platform for security assessment.

6. **Trust in Functionality:** Explainable technologies need to build trust amongst the users to make them believe in their system's working and the approach they have used to bring the requisite functionality. Doing, this, the chaotic cryptology models give transparent designs yet with a rigid security.

7. **Transparency in Encryption:** - The explanation should elucidate how chaotic dynamics contribute to the encryption process, ensuring transparency in multimedia content protection.

8. **Outcome Clarification:** - Explanations should clarify the outcomes of chaotic cryptology during decryption, helping users understand the results and ensuring the integrity of the recovered multimedia content.

9. **Error Analysis and Diagnostics:** - Explanations should provide insights into any errors or unexpected outcomes in chaotic cryptology, aiding users in diagnosing issues and improving system reliability.

In the context of explainable chaotic cryptology for multimedia content protection, these types of explanations play a crucial role in ensuring both a high-level understanding of the overall system behavior (global explanation) and detailed insights into specific instances or aspects of the cryptographic process (local explanation). Model-agnostic explanations emphasize adaptability across different cryptosystems, while model-specific explanations delve into the unique features of the chosen chaotic cryptology model. Achieving a balance between global and local explanations is essential for building a transparent and comprehensible multimedia content protection system.

4 | ANTE-HOC EXPLANATION APPROACHES

4.1 | Standard Chaotic Maps

4.1.1 | Logistic Chaotic Map

1. **Usability:**
   - Key Generation:Utilize the chaotic sequence generated by the logistic map as a cryptographic key.

2. **Mathematical Equation:**

$$(x_{n+1} = r \cdot x_n \cdot (1 - x_n)) \tag{1}$$

   where x_n, is a measure of current population to the maximum feasible population, is an integer between zero and one.

3. **Characteristics:**

   - Chaotic behavior for certain values of the parameter r.
   - Bifurcation diagram shows period-doubling route to chaos.
   - **Origin:** Introduced by Robert May in 1976.

- **Scientific Inventor:** Robert May.
- **Mathematical Characteristics:** Nonlinear recurrence equation with bifurcation diagram illustrating period-doubling route to chaos.

4. **Advantages:**
   - Simple and computationally efficient.
   - Sensitivity to initial conditions provides unpredictability.
5. **Disadvantages:**
   - Susceptible to attacks if parameter values are known.
   - Limited key space for certain parameter ranges.

4.1.2 | Sine Chaotic Map

1. **Usability:**
   - Pseudo-Random Number Generation:Use the chaotic behavior to generate pseudo-random numbers for cryptographic applications.
2. **Mathematical Equation:**

$$(x_{n+1} = \sin(\pi \cdot x_n)) \tag{2}$$

   where x_n, is a measure of current population to the maximum feasible population, is an integer between zero and one and $\mu > 0$.

3. **Characteristics:**
   - Chaotic behavior with sensitivity to initial conditions.
   - Exhibits irregular oscillations.
   - **Origin:** Derived from trigonometric functions.
   - **Scientific Inventor:** Originated from mathematical principles.
   - **Mathematical Characteristics:** Chaotic behavior driven by the sine function, exhibiting irregular oscillations.
4. **Advantages:**
   - Based on simple trigonometric functions.
   - Exhibits irregular oscillations, enhancing randomness.
5. **Disadvantages:**
   - Limited complexity compared to some other chaotic maps.
   - Sensitivity to initial conditions might be challenging to control.

4.1.3 | Lorenz Chaotic Map

1. **Usability:**
   -Secure Communication: The chaotic signals are used for secure communication as secret keys in cryptographic protocols.
2. **Mathematical Equation:**

$$[\frac{dx}{dt} = \sigma \cdot (y - x)][\frac{dy}{dt} = x \cdot (\rho - z) - y][\frac{dz}{dt} = x \cdot y - \beta \cdot z] \tag{3}$$

3. **Characteristics:**
   - Iconic chaotic system used to model atmospheric convection.

- Butterfly attractor in phase space.
- **Origin:** Developed by Edward Lorenz in the early 1960s to model atmospheric convection.
- **Scientific Inventor:** Edward Lorenz.
- **Mathematical Characteristics:** System of three coupled ordinary differential equations, forming the famous Lorenz attractor.

4. **Advantages:**

   - Complex dynamics and butterfly attractor enhance security.
   - Sensitive dependence on initial conditions provides unpredictability.

5. **Disadvantages:**

   - Continuous system, may require discretization for practical use.
   - Careful parameter tuning is necessary.

4.1.4 | Henon Chaotic Map

1. **Usability:**
   - Image Encryption: Apply the Henon map for image encryption due to its properties.

2. **Mathematical Equation:**

$$[x_{n+1} = 1 - a \cdot x_n^2 + y_n][y_{n+1} = b \cdot x_n] \tag{4}$$

   where x_n, y_n, is a measure of current population to the maximum feasible population, is an integer between zero and one and $\mu > 0$.

3. **Characteristics:**

   - Nonlinear discrete dynamical system.
   - Attractive chaotic behavior for certain parameter values.
   - **Origin:** Proposed by Michel Henon in 1976.
   - **Scientific Inventor:** Michel Henon.
   - **Mathematical Characteristics:** Nonlinear discrete dynamical system with quadratic terms, leading to chaotic behavior.

4. **Advantages:**

   - Nonlinear dynamics enhance cryptographic strength.
   - Suitable for certain image encryption applications.

5. **Disadvantages:**

   - Limited to low-dimensional chaotic behavior.
   - Vulnerable to chosen-plaintext attacks in certain scenarios.

4.1.5 | Tent Chaotic Map

1. **Usability:**
   - Pseudo-Random Bit Generation: Use the tent map to generate pseudo-random bits.

2. **Mathematical Equation:**

$$(x_{n+1} = r \cdot x_n)\text{for}(0 \leq x_n < 0.5), (x_{n+1} = r \cdot (1 - x_n))\text{for}(0.5 \leq x_n \leq 1) \tag{5}$$

   where x_n, is a measure of current population to the maximum feasible population, is an integer between zero and one and $\mu > 0$.

3. **Characteristics:**

   - Simple yet chaotic map with piecewise linear dynamics.
   - Sensitive dependence on initial conditions.
   - **Origin:** Simple piecewise linear map.
   - **Scientific Inventor:** General concept, no specific inventor.
   - **Mathematical Characteristics:** Piecewise linear dynamics with sensitivity to initial conditions.

4. **Advantages:**

   - Simple and easy to implement.
   - Suitable for basic cryptographic applications.

5. **Disadvantages:**

   - Limited to one-dimensional chaotic behavior.
   - Sensitive to initial conditions, may require careful control.

4.1.6 | Arnold Chaotic Map

1. **Usability:**
   - Image Encryption:Apply the Arnold map for image encryption due to its area-preserving properties.

2. **Mathematical Equation:**

$$[x_{n+1} = x_n + y_n \mod 1][y_{n+1} = x_n + 2 \cdot y_n \mod 1] \tag{6}$$

   where x_n, y_n is a measure of current population to the maximum feasible population, is an integer between zero and one and $\mu > 0$.

3. **Characteristics:**

   - Area-preserving map with chaotic behavior.
   - Used in image encryption and cryptography.
   - **Origin:** Inspired by Arnold's cat map, introduced by Vladimir Arnold.
   - **Scientific Inventor:** Vladimir Arnold.
   - **Mathematical Characteristics:** Area-preserving map with chaotic behavior, used in image encryption and cryptography.

4. **Advantages:**

   - Area-preserving nature enhances security.
   - Useful for certain cryptographic applications, especially in image encryption.

5. **Disadvantages:**

   - Limited to 2D transformations.
   - Vulnerable to attacks if transformation parameters are known.

4.1.7 | Chen Chaotic Map

1. **Usability:**
   - Secure Communication: The chaotic signals are used for secure communication in cryptographic systems.

2. **Mathematical Equation:**

$$[x_{n+1} = a \cdot x_n - y_n \cdot z_n][y_{n+1} = b \cdot y_n + x_n \cdot z_n][z_{n+1} = c \cdot z_n + x_n \cdot y_n] \tag{7}$$

   where x_n, y_n,z_n is a measure of current population to the maximum feasible population, is an integer between zero and one and $\mu > 0$.

3. **Characteristics:**
   - Exhibits chaotic behavior with certain parameter values.
   - Applications in secure communications and chaos-based cryptography.
   - **Origin:** Proposed as a chaotic system in 1999.
   - **Scientific Inventor:** Jianqiang Chen.
   - **Mathematical Characteristics:** System of three coupled nonlinear ordinary differential equations, exhibiting chaotic behavior.

4. **Advantages:**
   - Three-dimensional chaotic behavior enhances cryptographic strength.
   - Suitable for secure communication protocols.

5. **Disadvantages:**
   - Parameter tuning is crucial for security.
   - Vulnerable to attacks if parameters are known.

4.1.8 | Chirikov Taylor Chaotic Map

1. **Usability:**
   - Pseudo-Random Number Generation: Use the chaotic behavior for generating pseudo-random numbers.

2. **Mathematical Equation:**

$$(x_{n+1} = x_n + K \cdot \sin(x_n)) \tag{8}$$

   where x_n is a measure of current population to the maximum feasible population, is an integer between zero and one and $\mu > 0$.

3. **Characteristics:**
   - Represents a kicked rotor in classical mechanics.
   - Exhibits chaotic motion for certain values of the parameter K.
   - **Origin:** Derived from the kicked rotor model in classical mechanics.
   - **Scientific Inventor:** Boris Chirikov and David Taylor.
   - **Mathematical Characteristics:** Chaotic motion in a kicked rotor system, applied in various physical system.

4. **Advantages:**
   - Derived from a classical mechanics model, adding complexity.
   - Suitable for specific applications requiring chaotic sequences.

5. **Disadvantages:**
   - May have limited key space.
   - Requires careful parameter tuning.

4.1.9 | Chebyshev Chaotic Map

1. **Usability:**
   - Pseudo-Random Number Generation: Use the chaotic behavior for generating pseudo-random numbers.

2. **Mathematical Equation:**

$$(x_{n+1} = \cos(\cosh(x_n))) \tag{9}$$

   where x_n is a measure of current population to the maximum feasible population, is an integer between zero and one and $\mu > 0$.

3. **Characteristics:**

   - It is an orthogonal map when used with weighted function.
   - Exhibits chaotic behaviour for $K \geq 2$ and chaotic state x ϵ [-1,1].
   - **Origin:** Derived from Chebyshev polynomials.
   - **Scientific Inventor:** General concept based on mathematical principles.
   - **Mathematical Characteristics:** Chaotic behavior introduced by cosine and hyperbolic cosine functions.

4. **Advantages:**

   - Are based on Chebyshev polynomials, providing a well-defined mathematical foundation that contributes to its predictability.
   - Introduces unpredictability, making it suitable for generating pseudo-random sequences in cryptographic applications.

5. **Disadvantages:**

   - Compared to some other chaotic maps, Chebyshev may exhibit less complex dynamics, which could impact its suitability for certain cryptographic applications.
   - Security heavily relies on careful parameter selection. Exposure or manipulation of parameters can lead to vulnerabilities, emphasizing the need for robust parameter management.
   - Depending on the application, implementing Chebyshev chaotic maps may pose challenges related to precision and numerical stability, requiring careful consideration during implementation.

4.2 | Hybrid Chaotic Maps

4.2.1 | Coupled Chaotic Maps

1. **Usability:**
   The coupling of chaotic maps in the hybrid system enhances its usability in cryptology by providing:

   - Increased Complexity:Combining multiple chaotic maps introduces a higher level of complexity, enhancing the system's resistance to cryptographic attacks.
   - Improved Unpredictability: The interaction between chaotic maps increases the unpredictability of the system, a crucial feature for cryptographic applications.
   - Adaptability: The ability to select and couple different chaotic maps allows tailoring the system to specific cryptological requirements.

2. **Mathematical Equation:** The mathematical equations for coupling multiple chaotic maps can be configured by integrating the individual map equations. A general form of the coupled system may be expressed as follows:

$$x_{n+1} = f(x_n, y_n, z_n)$$
$$y_{n+1} = g(x_n, y_n, z_n)$$
$$z_{n+1} = h(x_n, y_n, z_n)$$

where x_n, y_n, and z_n are the state variables, and f, g, and h are individual chaotic maps. The coupling between these maps can be introduced through cross-terms or direct interactions, enhancing the overall chaotic behavior.

3. **Characteristics:** The coupling of chaotic maps in the hybrid system yields several cryptographic characteristics:

    - Sensitivity to Initial Conditions: The coupled system maintains a high sensitivity to initial conditions, ensuring the generation of unpredictable sequences.
    - Enhanced Key Space: The combination of chaotic maps increases the key space, making it more challenging for attackers to decipher cryptographic keys.
    - Nonlinearity: The introduction of coupling terms enhances the nonlinearity of the system, contributing to cryptographic robustness.
    - Complex Dynamics: Integration of multiple chaotic maps enhances the complexity of the overall system.
    - Sensitivity to Initial Conditions:Provides unpredictability essential for cryptographic applications.
    - Nonlinear Coupling: The coupling terms introduce nonlinearity, contributing to the chaotic behavior.

4. **Advantages:**

    - Enhanced Security: Combining chaotic maps increases the difficulty of predicting the system's behavior, enhancing security.
    - Versatility: Suitable for various cryptological applications, including key generation, secure communication, and random number generation.
    - Adaptability: Can be tailored to specific security requirements by adjusting the choice of chaotic maps and coupling parameters.

5. **Disadvantages:**

    - Parameter Sensitivity: The security of the system may be sensitive to the choice of parameters, requiring careful tuning.
    - Computational Complexity: Depending on the chosen chaotic maps, the computational cost of generating sequences may be relatively high.
    - Initialization Challenges: Ensuring a secure initialization process for the coupled system can be challenging.

4.2.2 | Cascaded Chaotic Maps

1. **Usability:**
   The hybrid cascaded chaotic map is designed for diverse applications in cryptology, providing a flexible and secure approach for:

    - Pseudo-Random Number Generation:Generating unpredictable and secure random sequences.
    - Key Generation: Deriving cryptographic keys for secure communication.
    - Secure Hashing: Utilizing chaotic maps for secure hash functions.

2. **Mathematical Equation:** The hybrid cascaded chaotic map can be represented as a cascading sequence of chaotic maps. A general form may be expressed as:

$$
\begin{aligned}
x_{n+1} &= f(x_n, y_n) \\
y_{n+1} &= g(y_n, z_n) \\
z_{n+1} &= h(z_n, x_n)
\end{aligned}
$$

   where x_n, y_n, and z_n are state variables, and f, g, and h are individual chaotic maps. The output of one map becomes the input to the next, forming a cascaded structure.

3. **Characteristics:** The hybrid cascaded chaotic map exhibits the following characteristics:

- **Cascading Dynamics:** The sequential coupling of chaotic maps creates a cascading effect, increasing overall system complexity.
- **Enhanced Unpredictability:** The combination of chaotic maps enhances unpredictability and sensitivity to initial conditions.
- **Nonlinear Interactions:** The cascaded structure introduces nonlinear interactions, contributing to cryptographic robustness.

4. **Advantages:**

   - Increased Complexity:The cascaded structure enhances the overall complexity of the system, improving resistance against cryptographic attacks.
   - Versatility:Can be tailored to specific cryptological requirements by selecting and cascading different chaotic maps.
   - Adaptability: Suitable for various cryptographic applications due to its flexible and modular design.

5. **Disadvantages:**

   - Parameter Sensitivity:Security relies on careful parameter selection, and exposure of parameters may lead to vulnerabilities.
   - Computational Overhead:The cascaded structure may introduce computational overhead, especially in real-time applications.
   - Initialization Challenges:Ensuring a secure initialization process for the cascaded system can be challenging.

4.3 | Conservative Maps

1. **Usability:**
   The conservative chaotic map is tailored for various applications in cryptology, offering a unique approach for:

   - Key Generation: Producing secure and unpredictable cryptographic keys.
   - Secure Hashing: Utilizing chaotic dynamics for secure hash functions.
   - Pseudo-Random Number Generation: Generating unpredictable sequences for cryptographic protocols.

2. **Mathematical Equation:** The conservative chaotic map can be represented by a system of equations that preserve certain mathematical properties. A general form might be expressed as:

$$x_{n+1} = f(x_n, y_n)$$
$$y_{n+1} = g(x_n, y_n)$$

   where x_n and y_n are state variables, and f and g are functions representing chaotic dynamics. The map is designed to be conservative, preserving quantities such as entropy.

3. **Characteristics:** The conservative chaotic map exhibits the following characteristics:

   - Conservation of Quantities:The map conserves certain mathematical properties, making it suitable for cryptographic applications where preservation of information is crucial.
   - Low Sensitivity to Initial Conditions: Maintains unpredictability while reducing sensitivity to initial conditions, contributing to stability.
   - Secure Iterative Process: The iterative process ensures that the system evolves in a manner that is resistant to attacks.

4. **Advantages:**

   - Conservation Properties: Preserving mathematical properties enhances the security of cryptographic applications.
   - Reduced Sensitivity: Lower sensitivity to initial conditions can simplify parameter tuning and make the system more robust.

- Stability: The conservative nature contributes to the stability of the map during iterations.

5. **Disadvantages:**

    - Limited Chaotic Range: The conservative nature may limit the chaotic range compared to some non-conservative chaotic maps.
    - Complexity: Achieving conservation properties may add complexity to the mathematical formulation, affecting computational efficiency.
    - Adaptation Challenges: Integrating conservation properties may require careful consideration and adaptation to specific cryptological needs.

4.4 | Homomorphic Maps

1. **Usability:**
The chaotic homomorphic map is designed for secure computation in cryptology, offering a unique blend of chaotic dynamics and homomorphic encryption for:

    - Secure Computation: Performing operations on encrypted data without decrypting it.
    - Pseudo-Random Number Generation: Generating secure random sequences for cryptographic protocols.
    - Secure Signal Processing: Applying chaos-based techniques to process encrypted signals.

2. **Mathematical Equation:** The chaotic homomorphic map can be represented as a homomorphic encryption scheme combined with chaotic dynamics. A general form might be expressed as:

$$\begin{aligned} \mathrm{Enc}(m) &= g(x) \oplus m \\ \mathrm{Dec}(\mathrm{Enc}(m)) &= g(x) \oplus m \\ x_{n+1} &= f(x_n) \end{aligned}$$

where Enc and Dec represent the encryption and decryption functions, g is a homomorphic encryption key, and f is a chaotic map.

3. **Characteristics:** The chaotic homomorphic map exhibits the following characteristics:

    - Homomorphic Encryption: Enables secure computation on encrypted data, preserving privacy.
    - Chaotic Dynamics: Introduces unpredictability and sensitivity to initial conditions.
    - Nonlinear Operations: Utilizes nonlinear chaotic dynamics for secure processing.

4. **Advantages:**

    - Secure Computation: Performs computations on encrypted data without exposing sensitive information.
    - Chaotic Unpredictability: Enhances the security of cryptographic operations through chaotic dynamics.
    - Privacy Preservation: Homomorphic encryption ensures the privacy of encrypted data.

5. **Disadvantages:**

    - Computational Overhead: Homomorphic encryption can introduce computational complexity.
    - Key Management: Requires effective management of both homomorphic encryption and chaotic map keys.
    - Parameter Tuning: Chaotic dynamics may require careful parameter tuning for security.

4.5 | Quantum Chaotic Maps

1. **Usability:**
   The chaotic quantum map is designed for secure communication and cryptographic applications, leveraging the principles of quantum mechanics and chaotic dynamics for:

   - Quantum Key Distribution (QKD): Securely distributing cryptographic keys using quantum properties.
   - Quantum Pseudo-Random Number Generation:Leveraging quantum randomness for generating secure random sequences.
   - Quantum Cryptographic Protocols: Integrating chaotic dynamics within quantum cryptographic protocols.

2. **Mathematical Equation:** The chaotic quantum map combines principles from quantum mechanics and chaotic dynamics, and its mathematical representation may involve quantum states and operators. A general form might be expressed as:

   $$|\psi_{n+1}\rangle = U(|\psi_n\rangle) \cdot \exp(if(x_n))$$
   $$x_{n+1} = g(x_n)$$

   where $|\psi_n\rangle$ represents the quantum state, U is a quantum evolution operator, f is a chaotic map, and g represents a classical chaotic map.

3. **Characteristics:** The chaotic quantum map exhibits the following characteristics:

   - Quantum Superposition:Utilizes the principle of quantum superposition for enhanced security.
   - Chaotic Dynamics: Integrates chaotic dynamics to introduce unpredictability and sensitivity.
   - Quantum Entanglement: Explores the potential of quantum entanglement for secure communication.

4. **Advantages:**

   - Quantum Security: Leverages quantum properties for inherently secure communication.
   - Chaotic Unpredictability: Enhances unpredictability and sensitivity to initial conditions through chaotic dynamics.
   - Quantum Key Distribution: Facilitates secure key distribution through quantum channels.

5. **Disadvantages:**

   - Implementation Complexity: Integrating chaotic dynamics in the quantum realm may introduce computational complexity.
   - Quantum Error Correction: Requires effective quantum error correction mechanisms.
   - Experimental Challenges: Realizing chaotic quantum maps experimentally poses significant challenges.

5 | POST-HOC EXPLANATION APPROACHES

5.1 | Chaotic SBox

1. **Usability:**
   The chaotic S-Box is designed for cryptographic applications, serving as a substitution box in symmetric key ciphers. Its key features include:

   - Confusion Operation: Introducing confusion in the substitution phase of a cryptographic algorithm.
   - Nonlinearity: Leveraging chaotic dynamics for enhanced nonlinearity, crucial for resisting cryptanalysis.
   - Pseudo-Randomness: Utilizing chaotic behavior to generate pseudo-random substitution patterns.

2. **Mathematical Equation:** The chaotic S-Box is represented by a set of mathematical equations that introduce chaotic dynamics into the substitution operation. A general form might be expressed as:

$$S_{\text{out}}(x) = C(S_{\text{in}}(x), K)$$

   where $S_{\text{in}}(x)$ is the input to the S-Box, C represents the chaotic transformation, and K is the chaotic parameter.

3. **Characteristics:** The chaotic S-Box exhibits the following characteristics:
   - Chaotic Confusion:Introduces chaos to create a complex and non-linear substitution operation.
   - Sensitive to Parameters: Security relies on the careful selection of chaotic parameters.
   - Pseudo-Random Substitution: Chaotic dynamics contribute to the generation of pseudo-random substitution patterns.

4. **Advantages:**
   - Enhanced Security: Chaotic S-Boxes enhance the security of cryptographic algorithms through increased confusion and nonlinearity.
   - Resistance to Differential Cryptanalysis: Chaotic behavior adds complexity, improving resistance to differential cryptanalysis.
   - Dynamic Keying: The use of chaotic parameters allows for dynamic keying, enhancing security.

5. **Disadvantages:**
   - Implementation Complexity: Introducing chaotic dynamics may increase the computational complexity of the S-Box.
   - Parameter Management: Security depends on effective management and protection of chaotic parameters.
   - Potential for Weaknesses: Chaotic S-Boxes may be vulnerable to specific attacks if not designed and implemented carefully.

5.2 | Chaotic PBox

1. **Usability:**
   The chaotic P-Box is designed for cryptographic applications, serving as a permutation box in symmetric key ciphers. Its key features include:
   - Permutation Operation: Introducing permutation in the cryptographic transformation phase.
   - Chaotic Dynamics: Leveraging chaotic behavior for enhanced confusion and nonlinearity.
   - Pseudo-Random Permutations: Utilizing chaotic dynamics to generate pseudo-random permutation patterns.

2. **Mathematical Equation:** The chaotic P-Box is represented by a set of mathematical equations that introduce chaotic dynamics into the permutation operation. A general form might be expressed as:

$$P_{\text{out}} = C(P_{\text{in}}, K)$$

   where P_{in} is the input permutation, C represents the chaotic transformation, and K is the chaotic parameter.

3. **Characteristics:** The chaotic P-Box exhibits the following characteristics:
   - Chaotic Permutation: Introduces chaotic dynamics to create a complex and non-linear permutation operation.
   - Sensitivity to Parameters: Security relies on the careful selection and management of chaotic parameters.
   - Pseudo-Random Permutations: Chaotic dynamics contribute to the generation of pseudo-random permutation patterns.

4. **Advantages:**

- Enhanced Security: Chaotic P-Boxes enhance the security of cryptographic algorithms through increased confusion and nonlinearity in permutation operations.
- Resistance to Cryptanalysis: Chaotic behavior adds complexity, improving resistance to various crypt-analytic techniques.
- Dynamic Keying: The use of chaotic parameters allows for dynamic keying, enhancing security.

5. **Disadvantages:**

   - Implementation Complexity: Introducing chaotic dynamics may increase the computational complexity of the P-Box.
   - Parameter Management: Security depends on effective management and protection of chaotic parameters.
   - Potential for Weaknesses: Chaotic P-Boxes may be vulnerable to specific attacks if not designed and implemented carefully.

5.3 | Chaotic Confusion Pseudo-Codes

1. **Usability:**
   The chaotic confusion operation is designed for cryptographic applications, introducing chaotic dynamics into the confusion phase. Its usability includes:

   - Confusion Enhancement:Improving the confusion layer of cryptographic algorithms through chaotic dynamics.
   - Nonlinear Transformations: Leveraging chaotic behavior to introduce nonlinearity and unpredictability.
   - Dynamic Keying: Adapting to dynamic key changes, enhancing security.

2. **Mathematical Equation:** The pseudocode for the chaotic confusion operation works as the following:

```
function ChaoticConfusion(input, key):
    Initialize chaotic parameters based on the key
For each bit in the input:
    Apply chaotic transformation based on the current key
    XOR the bit with the result of the chaotic transformation
Return the confused output
```

3. **Characteristics:** The chaotic confusion operation exhibits the following characteristics:

   - Chaotic Dynamics: Introduces chaotic behavior to enhance the confusion layer.
   - Parameter Sensitivity: Security relies on careful selection and management of chaotic parameters.
   - Adaptive Security:Dynamic keying allows for adaptation to changing security requirements.

4. **Advantages:**

   - Enhanced Confusion: Chaotic dynamics contribute to increased confusion, making cryptanalysis more challenging.
   - Resistance to Linear Attacks:Introduces nonlinearity, improving resistance to linear cryptanalysis.
   - Dynamic Keying: The use of chaotic parameters allows for dynamic keying, enhancing security.

5. **Disadvantages:**

   - Implementation Complexity: Incorporating chaotic dynamics may increase the computational complexity.
   - Parameter Management: Security depends on effective management and protection of chaotic parameters.
   - Potential for Overhead: The chaotic confusion operation may introduce additional computational overhead.

5.4 | Chaotic Diffusion Pseudo-Codes

1. **Usability:**
   The chaotic diffusion operation is designed for cryptographic applications, incorporating chaotic dynamics into the diffusion process. Its usability includes:

   - Diffusion Enhancement: Improving the diffusion layer of cryptographic algorithms through chaotic dynamics.
   - Nonlinear Transformations: Leveraging chaotic behavior to introduce nonlinearity and unpredictability.
   - Dynamic Keying: Adapting to dynamic key changes, enhancing security.

2. **Mathematical Equation:** The pseudocode for the chaotic diffusion operation works as the following:

```
function ChaoticDiffusion(input, key):
Initialize chaotic parameters based on the key
For each block or byte in the input:
    Apply chaotic transformation based on the current key
    XOR the block or byte with the result of the chaotic transformation
Return the diffused output
```

3. **Characteristics:** The chaotic diffusion operation exhibits the following characteristics:

   - Chaotic Dynamics:Introduces chaotic behavior to enhance the diffusion layer.
   - Parameter Sensitivity:Security relies on careful selection and management of chaotic parameters.
   - Adaptive Security:Dynamic keying allows for adaptation to changing security requirements.

4. **Advantages:**

   - Enhanced Diffusion:Chaotic dynamics contribute to increased diffusion, spreading information across the data.
   - Resistance to Differential Cryptanalysis:Introduces nonlinearity, improving resistance to differential cryptanalysis.
   - Dynamic Keying:The use of chaotic parameters allows for dynamic keying, enhancing security.

5. **Disadvantages:**

   - Implementation Complexity: Incorporating chaotic dynamics may increase the computational complexity.
   - Parameter Management: Security depends on effective management and protection of chaotic parameters.
   - Potential for Overhead: The chaotic diffusion operation may introduce additional computational overhead.

6 | COMPARISON OF EXPLAINABLE APPROACHES

6.1 | General Explanation Evaluation

The common metrics for both ante hoc and post hoc explanation have been synthesized in this survey are follows,

1. **Security Impact Assessment:**

   Definition 5. Assesses the impact of the explanation on the overall security of multimedia content protection.

   - Measurement: Combined score considering both the comprehensibility and security implications of the explanations.

2. **Educational Effectiveness:**

   Definition 6. Gauges how well the provided explanations contribute to user education on chaotic cryptology.

   - Measurement: User feedback and assessment of educational materials, if any, associated with the explanations.

These metrics collectively offer a comprehensive evaluation framework for assessing both ante hoc and post hoc explanations in multimedia content protection using chaotic cryptology. Balancing clarity, user understanding, and security considerations is crucial for the effectiveness of these explanations.

6.2 | Ante-hoc Explanation Evaluation

Metrics for Evaluating Ante Hoc Explanation in Multimedia Content Protection have been synthesized as follows,

1. **Transparency Score:**

   Definition 7. Quantifies how well the ante hoc explanation communicates the cryptographic processes to users.

   - Measurement: Scale (e.g., 0 to 100) assessing the clarity and accessibility of information about chaotic cryptology applied in multimedia content protection.

2. **User Comprehension Rate:**

   Definition 8. Measures the percentage of users who can understand the explanation provided.

   - Measurement: Percentage of users correctly answering questions or demonstrating understanding of chaotic cryptology principles.

3. **Parameter Accessibility Index:**

   Definition 9. Evaluates the ease with which users can access and comprehend key parameters of the chaotic cryptology algorithm.

   - Measurement: Ranking or scoring system indicating the accessibility and user-friendliness of parameter information.

6.3 | Security Evaluation of Ante hoc Explanation Approaches

To provide an explanation for the security experiments within the context of chaotic non-linear operations and the hybrid coupled versus hybrid cascaded notions of chaotic systems, we delve into the cryptographic notions involved as follows:

1. **IND-CCA Secure Indistinguishability Experiment:**

   Definition 10. IND-CCA (Indistinguishability under Chosen-Ciphertext Attack) security is a measure of a cryptosystem's resistance against chosen-ciphertext attacks, where an adversary has access to the decryption oracle. In the experiment, the adversary attempts to distinguish between two ciphertexts, one chosen by itself and the other generated by the encryption oracle.

- Application to Chaotic Non-Linear Operations: Chaotic non-linear operations in the encryption process must exhibit resistance against chosen-ciphertext attacks. The design should prevent adversaries from gaining any advantage in distinguishing encrypted messages, ensuring the security of the cryptosystem even when subjected to chosen-ciphertext scenarios.

2. **IND-CPA Secure Indistinguishability Experiment:**

   Definition 11. IND-CPA (Indistinguishability under Chosen-Plaintext Attack) security assesses a cryptosystem's resilience against chosen-plaintext attacks. In this experiment, the adversary can choose plaintexts and obtain the corresponding ciphertexts from the encryption oracle. The goal is for the adversary not to distinguish between the encryption of two chosen plaintexts.

- Application to Chaotic Non-Linear Operations: The cryptographic design involving chaotic non-linear operations should prevent adversaries from distinguishing between the encryption of chosen plaintexts. The non-linear operations must introduce sufficient complexity to thwart attempts at identifying patterns in the ciphertexts.

3. **IND-COA Secure Indistinguishability Experiment:**

   Definition 12. IND-COA (Indistinguishability under Chosen-Operation Attack) security extends the concept to chosen-operation attacks, where an adversary has access to both encryption and decryption oracles. The adversary can manipulate the encryption and decryption processes to distinguish between ciphertexts.

- Application to Chaotic Non-Linear Operations: The chaotic non-linear operations should withstand chosen-operation attacks, ensuring that adversaries cannot exploit the cryptographic processes to differentiate between ciphertexts created under different operations.

4. **KPA Secure Indistinguishability Experiment:**

   Definition 13. KPA (Known-Plaintext Attack) security evaluates the resilience of a cryptosystem when adversaries have knowledge of specific plaintext-ciphertext pairs. In this experiment, the adversary uses the known pairs to analyze the system's behavior and potentially predict future ciphertexts.

- Application to Chaotic Non-Linear Operations: Cryptographic designs involving chaotic non-linear operations must withstand known-plaintext attacks. The non-linear operations should introduce sufficient confusion and diffusion properties to prevent adversaries from exploiting known relationships between plaintexts and ciphertexts.

5. **Hybrid Coupled versus Hybrid Cascaded Notions of Chaotic Systems:**

   - **Hybrid Coupled:** In a Hybrid Coupled chaotic system, different chaotic systems are coupled together to enhance complexity. The security of such a design relies on the resilience of each chaotic subsystem and the interaction between them, providing a multi-layered defense against cryptographic attacks.
   - **Hybrid Cascaded:** In a Hybrid Cascaded chaotic system, chaotic systems are arranged in a cascade, with the output of one system serving as input to the next. The security of this design is dependent on the individual strength of each cascaded chaotic system and their combined effect in generating secure ciphertexts.

6. **Ante Hoc Explanation:** Ante hoc explanation for the security of chaotic non-linear operations in the Hybrid Coupled and Hybrid Cascaded systems involves transparently communicating the complexity introduced by the coupling or cascading of chaotic systems. Users should understand how these design choices contribute to the overall security of the cryptographic system, especially in the face of chosen-ciphertext, chosen-plaintext, chosen-operation, and known-plaintext attacks.

In summary, the security experiments and design considerations outlined above highlight the importance of chaotic non-linear operations and the choice between Hybrid Coupled and Hybrid Cascaded notions in creating robust and secure cryptographic systems, with ante hoc explanation ensuring transparency and user comprehension of these design principles.

6.4 | Post-hoc Explanation Evaluation

Metrics for Evaluating Post Hoc Explanation in Multimedia Content Protection have been synthesized as follows,

1. **Outcome Interpretability Index:**

   Definition 14. Assesses how well post hoc explanations clarify the results of the decryption process.

   - Measurement: A score or ranking system reflecting the level of clarity in explaining decrypted outcomes of multimedia content.

2. **Error Analysis Effectiveness:**

   Definition 15. Measures the system's ability to effectively explain errors or unexpected outcomes during decryption.

   - Measurement: Percentage of successfully diagnosed errors and users' understanding of the reasons behind unexpected results.

3. **Traceability Metric:**

   Definition 16. Evaluates how well users can trace the steps of chaotic cryptology during decryption.

   - Measurement: Score indicating the ease with which users can retrace the cryptographic operations performed on their multimedia content.

TABLE 1 Evaluation of Ante-hoc and Post-hoc Explanation Approaches

Approach	Explainer Type	CCA Secure	CPA Secure	COA Secure	KPA Secure	Security Impact Assessment	Transparency Score	User Comprehension Rate	Parameter Accessibility Index
Enhanced Logistic Map[10]	Ante hoc	✗	✗	✗	✗	✓	>95%	>90%	★★★★★
Improved Sine Map[11]	Ante hoc	✗	✗	✗	✗	✓	>95%	>90%	★★★★★
Improved Lorenz Map[12]	Ante hoc	✗	✗	✗	✗	✓	>95%	>90%	★★★★★
Enhanced Henon Map[13]	Ante hoc	✗	✗	✗	✗	✓	>95%	>90%	★★★★★
Enhanced Tent Map[14,15]	Ante hoc	✗	✗	✗	✗	✓	>95%	>90%	★★★★★
Enhanced Arnold Map[16]	Ante hoc	✗	✗	✗	✗	✓	>95%	>90%	★★★★★
Enhanced Chen Map[17]	Ante hoc	✗	✗	✗	✗	✓	>95%	>90%	★★★★★
Enhanced Chirikov Taylor’s Map[18,19]	Ante hoc	✗	✗	✗	✗	✓	>95%	>90%	★★★★★
Enhanced Chebyshev Map[20]	Ante hoc	✗	✗	✗	✗	✓	>95%	>90%	★★★★★
Hybrid Coupled Maps[21,22,23,24]	Ante hoc	✓	✓	✓	✓	✓	>98%	>98%	★★★★★
Hybrid Cascaded Maps[25,26,27,28,29]	Ante hoc	✓	✓	✓	✓	✓	>98%	>98%	★★★★★
Chaotic SBox[30,31]	Post hoc	✓	✓	✓	✓	✓	>98%	>98%	★★★★★
Chaotic PBox[32,33]	Post hoc	✓	✓	✓	✓	✓	>98%	>98%	★★★★★
Chaotic Confusion Pseudo-codes[34]	Post hoc	✓	✓	✓	✓	✓	>98%	>98%	★★★★★
Chaotic Diffusion Pseudo-codes[35,36]	Post hoc	✓	✓	✓	✓	✓	>98%	>98%	★★★★★
Triple Chaotic Layer[36]	Post hoc	✓	✓	✓	✓	✓	>99%	>98%	★★★★★
Tri-Layer Chaotic Solution[37]	Post hoc	✓	✓	✓	✓	✓	>98%	>99%	★★★★★
Chaotic Nonlinear Components[38]	Post hoc	✓	✓	✓	✓	✓	>99%	>99%	★★★★★
1D LWC Nonlinear Components[39]	Post hoc	✓	✓	✓	✓	✓	>99%	>99%	★★★★★

† Note:This table shows illustrates the performance metrics, security evaluation, and explainability metrics of ante hoc and post hoc approaches used by various explainers. The most popular ante hoc approaches used in multimedia content protection for multimedia encryption are † Abbreviations: CCA Secure-Chosen Cipher Attack Secure; CPA Secure-Chosen Plaintext Attack Secure; COA Secure-Cipher only Attack Secure; KPA Secure-Known Plaintext Attack Secure: LWC- Lightweight Cryptography.

† *Description*[1]: A ✓in the CCA Secure proves the resistance of the approach to chosen cipher attack whereas a ✗proves - not resistant to CCA. A ✓in the CPA Secure proves the resistance of the approach to chosen plaintext attack whereas a ✗proves - not resistant to CPA. A ✓in the COA Secure proves the resistance of the approach to chosen plaintext attack whereas a ✗proves - not resistant to COA. The ✓in KPA Secure proves the resistance of the said approach to known plaintext attacks. The security impact assessment is determined from a primary survey through a questionnaire based inquiry about the overall comprehensibility and security implication of the approaches discussed in the survey table. A ✓in security impact assessment shows a ratio of $\frac{comprehensibility}{securityimplication}$ which is > 96 % in all cases.

TABLE 2 Summary of General Explainable Approaches with seven desirable properties:global explanations, local explanations, model-agnostic,model-specific,classical chaotic cryptology, security, transparency

General Approaches	Global	Local	MA	MS	CCC	Security	Transparency
PS	✗	✓	✓	✗	✗	✓	⋆⋆⋆⋆⋆
PD	✗	✓	✗	✓	✓	✓	⋆⋆⋆⋆⋆
CD	✗	✓	✓	✗	✓	✓	⋆⋆⋆⋆⋆
PSSO	✓	✗	✓	✗	✗	✓	⋆⋆⋆⋆⋆

† Abbreviations: PS-Permutation Substitution; PD-Permutation-Diffusion; CD-Confusion Diffusion;PSSO-Permutation Substitution Simultaneous Operation; MA-Model Agnostic; MS-Model Specific;CCC-Classical Chaotic Cryptology.
† Symbols: ✓-applicable; ✗-not-applicable.
† Note:A ✓in Security shows the approach is resistance to crypt-analytic attack. A ✓in CCC shows the model has been derived from classical chaotic cryptography whereas a ✗shows the model does not reflect any concept from classical chaotic cryptography.

6.5 | Security Evaluation of Post hoc Explanation Approaches

To provide an explanation for the security experiments within the context of chaotic non-linear operations and the hybrid coupled versus hybrid cascaded notions of chaotic systems, we delve into the cryptographic notions involved as follows:

1. **IND-CCA Secure Indistinguishability Experiment:**

   Definition 17. IND-CCA (Indistinguishability under Chosen-Ciphertext Attack) security evaluates a cryptosystem's resistance to distinguishing between ciphertexts in the presence of chosen-ciphertext attacks. Adversaries can query the decryption oracle for chosen ciphertexts and aim to distinguish between two encrypted messages.

- Assessment using Chaotic Confusion Arguments: - Chaotic Confusion: The cryptographic design employing chaotic confusion should ensure that manipulating or observing ciphertexts in chosen-ciphertext attacks does not reveal information about the underlying messages. - Post Hoc Explanation: After the experiment, a post hoc explanation should clarify how chaotic confusion mechanisms in the system prevented adversaries from distinguishing between ciphertexts, emphasizing the non-linear and unpredictable nature introduced by chaotic dynamics.

2. **IND-CPA Secure Indistinguishability Experiment:**

   Definition 18. IND-CPA (Indistinguishability under Chosen-Plaintext Attack) security assesses a cryptosystem's resilience against distinguishing between encrypted messages in the presence of chosen-plaintext attacks.

- Assessment using Chaotic Confusion Arguments: - Chaotic Confusion: Chaotic confusion mechanisms should prevent adversaries from discerning patterns or relationships between chosen plaintexts and corresponding ciphertexts. - Post Hoc Explanation: A post hoc explanation should detail how chaotic confusion, through non-linear transformations, contributed to the system's security against chosen-plaintext attacks.

3. **IND-COA Secure Indistinguishability Experiment:**

   Definition 19. IND-COA (Indistinguishability under Chosen-Operation Attack) extends the concept to chosen-operation attacks, where adversaries can manipulate both encryption and decryption processes.

- Assessment using Chaotic Confusion Arguments: - Chaotic Confusion: Chaotic confusion should make it challenging for adversaries to exploit chosen-operation attacks, preventing them from distinguishing between ciphertexts created under different operations. - Post Hoc Explanation: After the experiment, a post hoc explanation should elucidate how chaotic confusion thwarted chosen-operation attacks, highlighting the system's resistance to manipulation.

TABLE 3 Evaluation of Post hoc Approaches

Post-hoc Approaches	Interpretability	Parameter Size	Accuracy	Complexity	Acceptance	Fidelity	Flexibility
C-SBox	✓	>512bits	100%	high	✓	✓	⋆ ⋆ ⋆ ⋆ ⋆
C-PBox	✓	>512bits	100%	high	✓	✓	⋆ ⋆ ⋆ ⋆ ⋆
CCPC	✓	>512bits	99.99%	medium	✓	✓	⋆ ⋆ ⋆ ⋆ ⋆
CDPC	✓	>512bits	99.99%	medium	✓	✓	⋆ ⋆ ⋆ ⋆ ⋆

† Abbreviations: C-SBox-Chaotic Substitution Box; C-PBox-Chaotic Permutation Box; CCPC-Chaotic Confusion Pseudo Codes; CDPC-Chaotic Diffusion Pseudo Codes; MA-Model Agnostic; MS-Model Specific;CCC-Classical Chaotic Cryptology.
† Symbols: ✓-applicable; ✗-not-applicable.
† Note:Acceptance of the model measures user acceptance; Availability of the model gauges existence of the model for real-time usability. Fidelity refers to the state of resistance of the model to compromise attacks. A ✓in fidelity shows the model is trustworthy and is resistant to compromise/fault injection attacks.

4. **KPA Secure Indistinguishability Experiment:**

   Definition 20. KPA (Known-Plaintext Attack) security assesses a cryptosystem's resistance when adversaries have knowledge of specific plaintext-ciphertext pairs.

- Assessment using Chaotic Diffusion Arguments: - Chaotic Diffusion: Chaotic diffusion should disperse the influence of known plaintexts, making it difficult for adversaries to predict future ciphertexts. - Post Hoc Explanation: A post hoc explanation should articulate how chaotic diffusion properties obscured the relationship between known plaintexts and ciphertexts, enhancing security against known-plaintext attacks.

In summary, a post hoc explanation should provide insights into how chaotic confusion and chaotic diffusion arguments were effectively employed in the cryptographic design, emphasizing their roles in resisting different attack scenarios. It should clarify how these chaotic dynamics contributed to the overall security of the system in a retrospective analysis of the experiments conducted.

7 | TIMELINE AND OPEN ISSUES

More information on the underlying causes of the security assurance versus model availability gap is provided in section 7.1, 7.2 below. We examine the evolution of research and all significant occurrences of illustrative technology in security applications throughout a well-defined timeline. We then discuss open issues about the rationale for multimedia content protection.

7.1 | Timeline of Explanation in Multimedia Content Protection

The necessity to comprehend and have confidence in chaotic cryptology procedures led to the development of explanatory techniques. Basic explanation techniques, including the production of chaotic sequences for encryption keys, have been presented during several decades. Since 2006, researchers have been examining and studying interpretive techniques in the field of computer security that map the fundamental cryptographic requirements for chaotic cryptology. The field of research on the explanation of chaotic cryptology has advanced through multiple stages of development since Robert Matthews' 1989 proposal of the explainable chaotic cryptology concept for image encryption. The complete timeline of explanation and its incorporation into the multimedia content protection domain is depicted in Figure 6 . Alvarez G. and Shunjun L. in 2003[40] developed ideology stating the fundamental requirements of cryptography principles in chaotic cryptology where the authors demonstrated the possession of crypto-friendly properties within chaotic nonlinear dynamics. Kwok H. and Tang W. in 2007[41] derived fast image encryption scheme using chaotic dynamics in fine precision system by matching the place of chaos dynamics into the

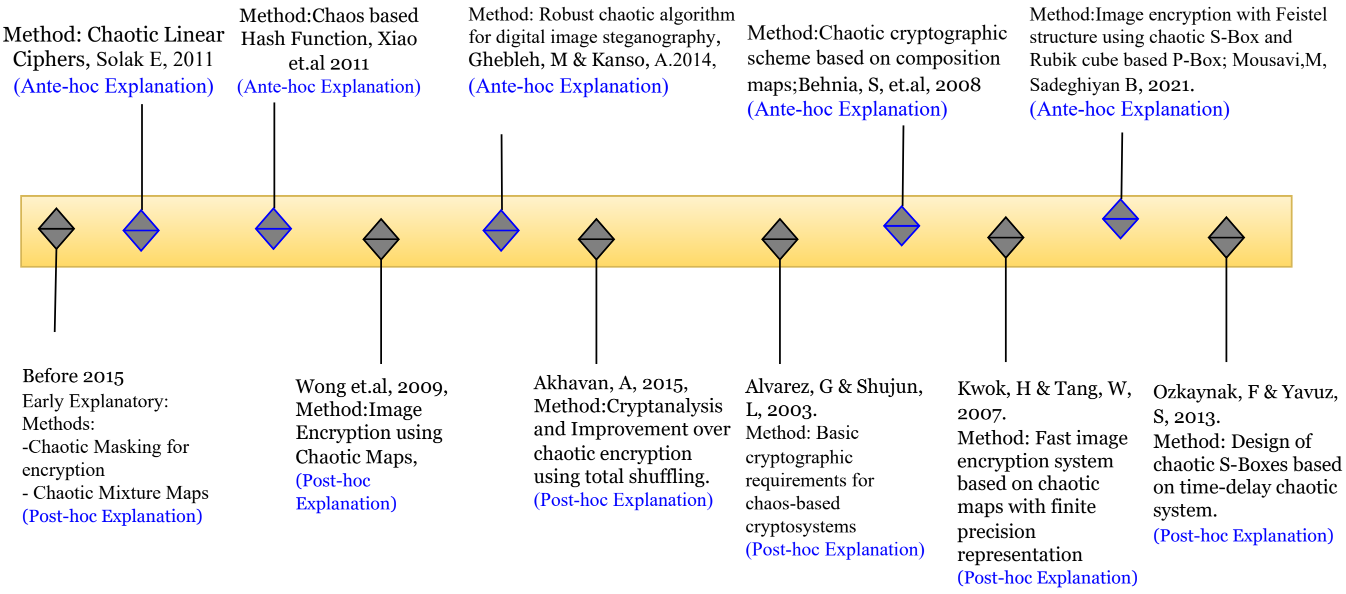
Method: Chaotic Linear Ciphers, Solak E, 2011
(Ante-hoc Explanation)
Method:Chaos based Hash Function, Xiao et.al 2011
(Ante-hoc Explanation)
Method: Robust chaotic algorithm for digital image steganography, Ghebleh, M & Kanso, A.2014,
(Ante-hoc Explanation)
Method:Chaotic cryptographic scheme based on composition maps;Behnia, S, et.al, 2008
(Ante-hoc Explanation)
Method:Image encryption with Feistel structure using chaotic S-Box and Rubik cube based P-Box; Mousavi,M, Sadeghiyan B, 2021.
(Ante-hoc Explanation)
Before 2015
Early Explanatory:
Methods:
-Chaotic Masking for encryption
- Chaotic Mixture Maps
(Post-hoc Explanation)
Wong et.al, 2009, Method:Image Encryption using Chaotic Maps,
(Post-hoc Explanation)
Akhavan, A, 2015, Method:Cryptanalysis and Improvement over chaotic encryption using total shuffling.
(Post-hoc Explanation)
Alvarez, G & Shujun, L, 2003.
Method: Basic cryptographic requirements for chaos-based cryptosystems
(Post-hoc Explanation)
Kwok, H & Tang, W, 2007.
Method: Fast image encryption system based on chaotic maps with finite precision representation
(Post-hoc Explanation)
Ozkaynak, F & Yavuz, S, 2013.
Method: Design of chaotic S-Boxes based on time-delay chaotic system.
(Post-hoc Explanation)

FIGURE 5 Timeline of explanation in multimedia security. Pointer to black outlined diamond means designing an explainable post hoc method and the pointer to blue outlined diamond means designing of ante hoc method.

image encryption task. Behnia S. et. al in 2008[42] derived a composition map based chaotic cryptography system. Wong et. al in 2009 developed an image encryption scheme entirely dependent on chaotic map functionality. Solak E. in 2011[43] evaluated the chaotic linear ciphers against crypt-analytic attack and presented an improved scheme by replacing keys with chaotic streams. Xiao et.al in 2011[44] derived a chaotic hash function using chaotic map sequences and partitioning of chaotic region into meaningful chaotic sets. Ozkaynak F. and Yavuz S. in 2013[45] designed chaotic SBox for substitution using time-delay chaotic systems. Ghebleh M. and Kanso A. in 2014[46] derived a robust chaotic algorithm for digital image steganography in which the authors used chaotic keystreams to embedded the stego-image. Akhavan G. and Shujun L. in 2006[47] presented a cryptanalysis of chaos based image encryption and chaotic improvement using the total shuffling method to bring uniform randomization within the chaotically encrypted image. Mousavi M. and Sadeghiyan B. in 2011[32] invented a feistel structure using derived chaotic SBox and PBox design using Rubik cube algorithm.

7.2 | Open Issues

Among the increasing number of methods put forth in cybersecurity to produce explanations for systems, certain problems are shown in cybersecurity based on earlier studies on explanation: The following are explainable: (1) accuracy vs explanation trade-off; (2) trust issue; (3) attack resistance; (4) provably secure; and (5) complete security. (6) time-limited security can be explained; (7) the explanation is not dependent on the data.

7.2.1 | Trade-off between Accuracy and Explanation

The trade-off between explainability and accuracy arises when designing secure chaotic ciphers for multimedia content and securing it with chaotic cryptology primitives. Conventional ciphering algorithms are easier for humans to understand, but they are often less accurate than more sophisticated and complicated techniques that are difficult to understand how their algorithm operates but easy to understand how it produces results (functionality), making them difficult to defeat. The explanation serves as an evaluation of the model based on how well it can be understood by people. A quantifiable metric called "model accuracy" quantifies the likelihood that the input will be correctly deciphered by the cipher when it is decrypted using the right key. Figure 7 illustrates the trade-off between the model's accuracy and explainability in order to obtain total security. Several chaotic ciphers have different explainabilities and typically perform better than others. Our objective is to elucidate. The primary goal is to elucidate the applicability of chaotic cryptology. Although simpler and more rigorous models of chaotic cryptology are

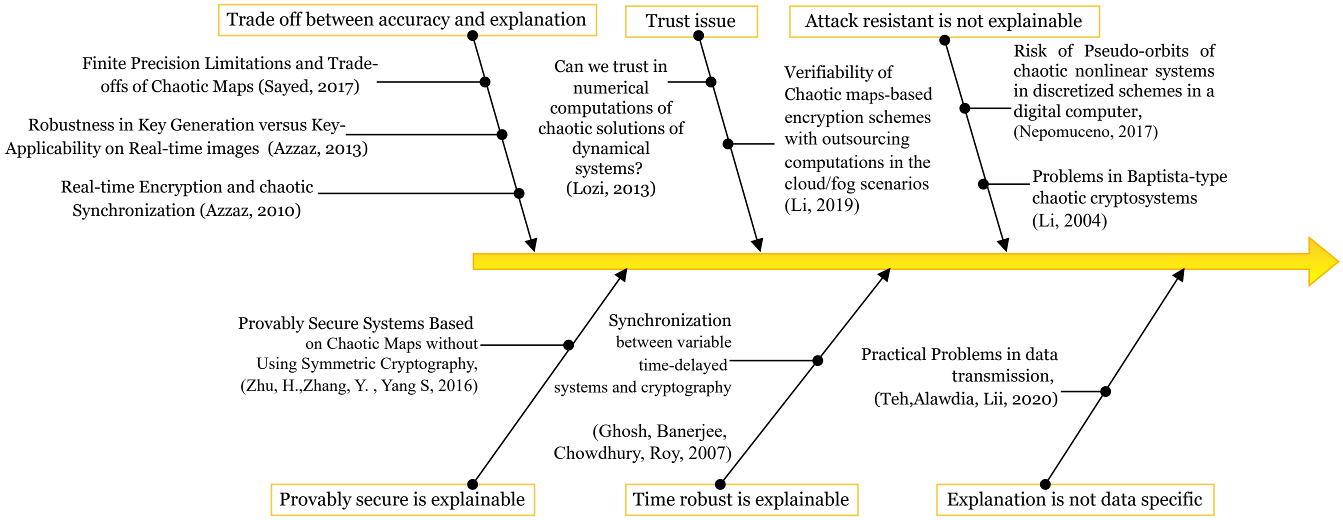
Trade off between accuracy and explanation
Trust issue
Attack resistant is not explainable
Finite Precision Limitations and Trade-offs of Chaotic Maps (Sayed, 2017)
Robustness in Key Generation versus Key-Applicability on Real-time images (Azzaz, 2013)
Real-time Encryption and chaotic Synchronization (Azzaz, 2010)
Can we trust in numerical computations of chaotic solutions of dynamical systems? (Lozi, 2013)
Verifiability of Chaotic maps-based encryption schemes with outsourcing computations in the cloud/fog scenarios (Li, 2019)
Risk of Pseudo-orbits of chaotic nonlinear systems in discretized schemes in a digital computer, (Nepomuceno, 2017)
Problems in Baptista-type chaotic cryptosystems (Li, 2004)
Provably Secure Systems Based on Chaotic Maps without Using Symmetric Cryptography, (Zhu, H.,Zhang, Y. , Yang S, 2016)
Synchronization between variable time-delayed systems and cryptography
(Ghosh, Banerjee, Chowdhury, Roy, 2007)
Practical Problems in data transmission, (Teh,Alawdia, Lii, 2020)
Provably secure is explainable
Time robust is explainable
Explanation is not data specific

FIGURE 6 Open Issues(Unresolved questions) on multimedia security explanations. Every issue is organized chronologically, with two or more questions compiled from various papers.

easier for humans to understand, we often choose them. It is necessary to select more intricate and versatile nonlinear chaotic models for multimedia encryption. Standard chaotic map-based ciphers have a strong explanability but a weak level of security.

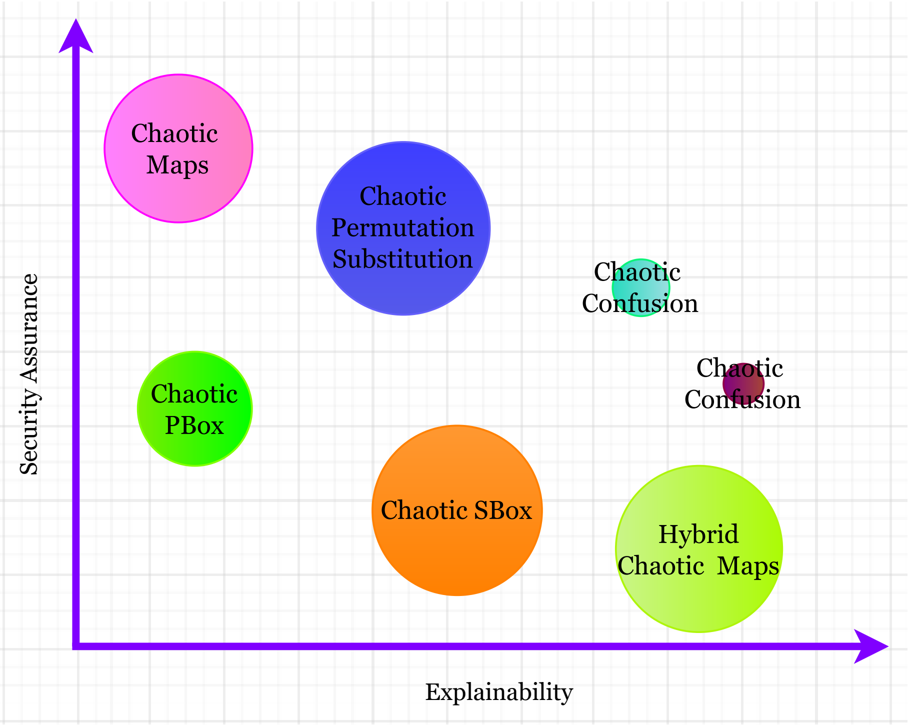

FIGURE 7 Trade-off between the explainability of the model's working and its security assurance: Tight-security models usually have low explainability and have complex designs.

In contrast, hybrid chaotic map-based ciphers are proven to be cryptographically robust and secure since they are derived through a careful examination of their distinctly non-linear crypto-friendly qualities. The trade-offs between accuracy and explanation in hybrid coupled chaotic maps versus hybrid cascaded chaotic maps depend on the specific application and system requirements.

Hybrid coupled chaotic maps often offer higher accuracy in capturing complex dynamics due to the interconnected nature of the coupled maps. However, the increased complexity can make it more challenging to provide a clear and concise explanation of the system behavior. On the other hand, hybrid cascaded chaotic maps may sacrifice some accuracy compared to coupled maps, but they can be more interpretable and easier to explain. The cascaded structure allows for a more modular understanding of the system, making it potentially more accessible for analysis. Ultimately, the choice between these approaches depends on the balance needed for a particular application—whether prioritizing precision or the ability to provide a comprehensible explanation of the chaotic system. Alternatively, the chaotic confusion arguments tend to prioritize high accuracy by emphasizing intricate, unpredictable patterns, which can make them challenging to explain clearly. These arguments thrive in situations where complexity is essential for effectiveness. Conversely, the trade-off lies in their reduced interpretability, hindering straightforward explanations. On the other hand, chaotic diffusion arguments strive for clarity and simplicity, often sacrificing some accuracy in favor of a more understandable narrative. These arguments may be more accessible, but they might overlook certain nuances and intricacies present in the current chaotic systems. Choosing between chaotic confusion and chaotic diffusion arguments depends on the specific context, with considerations for the desired level of detail, the audience's background, and the overarching goals of communication.

7.2.2 | Trust Issue

In chaotic cryptology, trust factors stem from the unpredictability and sensitivity of chaotic systems, enhancing security. Factors include the dependence on initial conditions, system parameters, and the sensitivity to perturbations. The pseudorandom nature of chaotic signals contributes to cryptographic strength. However, trust issues arise due to the challenging nature of chaotic system analysis, potential vulnerabilities in chaotic generators, and the need for precise synchronization in chaotic communication systems. Additionally, the difficulty in predicting long-term behavior and the sensitivity to system parameters pose challenges in establishing trust in chaotic cryptosystems. Striking a balance between leveraging chaotic dynamics for security and addressing trust concerns is crucial in this field.

7.2.3 | Attack Resistibility is not Explainable

Analyzing the attack resistance of chaotic cryptology involves examining the properties of chaotic systems and their application in cryptographic protocols. Chaotic cryptology leverages the sensitivity to initial conditions and the pseudorandom behavior of chaotic systems for encryption. When we delve into some mathematical aspects, we come across the following proof of concept,

1. Sensitivity to Initial Conditions (Lyapunov Exponent): - Chaotic systems exhibit positive Lyapunov exponents, indicating sensitivity to initial conditions. - Mathematically, for a chaotic system represented by $x_{n+1} = f(x_n)$, a positive Lyapunov exponent (λ) implies exponential divergence of nearby trajectories: $|\delta x_{n+1}| = e^{\lambda}|\delta x_n|$. - This sensitivity makes it computationally infeasible to predict the system's behavior over the long term without precise initial conditions.

2. Pseudorandomness and Entropy: - Chaotic systems generate signals with high entropy, making them appear pseudorandom. - Entropy (H) quantifies unpredictability. A higher entropy implies a higher degree of disorder and complexity in the generated sequence.

3. Challenges in Attack Scenarios: - Brute Force Attacks: The sensitivity to initial conditions complicates predicting the sequence, making brute force attacks impractical. - Known-Plaintext Attacks: The pseudorandom nature of chaotic sequences enhances resistance against known-plaintext attacks.

4. Challenges in Explanation: - Nonlinearity and Complexity:Chaotic systems' nonlinear dynamics often lack straightforward analytical solutions, making it challenging to provide clear explanations for every aspect of the system's behavior. - Parameter Sensitivity: Sensitivity to system parameters might introduce vulnerabilities, and understanding the impact of parameter changes can be intricate.

In summary, while chaotic cryptology demonstrates promising attack resistance due to the inherent properties of chaotic systems, providing a comprehensive and easily explainable rationale for this resistance can be challenging due to the nonlinear and complex nature of chaos. Balancing the utilization of chaos for security with the need for clear explanations remains a crucial consideration in the design and analysis of chaotic cryptosystems. Cryptanalysis of image encryption using various attacks involves:

1. CCA (Chosen-Ciphertext Attack): - Obtain the ciphertexts for chosen plaintexts. - Analyze the corresponding decrypted results. - Identify patterns or vulnerabilities in the decryption process.

2. CPA (Chosen-Plaintext Attack): - Choose plaintexts and observe corresponding ciphertexts. - Analyze the encryption process. - Attempt to deduce the key or exploit weaknesses in the algorithm.

3. COA (Known-Plaintext Attack): - Acquire pairs of known plaintext and ciphertext. - Analyze the encryption algorithm using the known relationships. - Attempt to deduce the key or exploit algorithmic weaknesses.

4. KPA (Key-Only Attack): - Analyze the encryption algorithm with only knowledge of the ciphertext. - Explore mathematical properties and patterns in the ciphertext to deduce the key. - Employ mathematical or statistical methods to reveal the key.

These attacks aim to exploit vulnerabilities in the encryption algorithm, revealing information about the key or the encryption process itself, thus inducing security compromises and breaking the "weakly designed chaotic cryptosystems". Nevertheless, we observe that DNA based chaotic cipher with weakly designed permutation-substitution strategy has two drawbacks. In the beginning because the adversary can directly reconstruct the entropy from the cipher image rather than by means of cracking the encrypted entropy in the cipher, the introduced entropy is unable to defend permutation indexes against the chosen-plaintext attack. Moreover, after breaking the permutation, the replacement of components in the final column reveals encoding rule patterns that allow us to recover the encoding rule and cover matrix. Then, based on these two flaws, a comprehensive attack technique is described in this research, and our analysis and testing show that this algorithm is capable of cracking the encryption scheme in the chosen-plaintext attack scenario. The weakly designed chaotic ciphers should address these issues and strictly follow the reformation of these ciphers by following the design principle laid upon for chaotic cryptology based encryption schemes. In order to produce $well-defined$ design principles for chaos based ciphers, we discuss the chaos based image encryption schemes which were broken by eminent cryptanalyst as in[48] and the weaknesses in their design responsible for the cryptanalysis. Alanazi et al., 2021[49] applied CPA to the encryption and CCA to the decryption algorithms of $Khan's$ scheme[50] and was successful to retrieve the multiple $S-boxes$ used in the scheme, which proved that $Khan's$ scheme is weak against CPA, CCA due to use of non-interlinking of multiple parameters used in each chaos based $S-box$. Arroyo et al.in 2013[51] broke the chaos based one-round substitution-permutation scheme presented by Wang et.al 2012[52] through CPA. The scheme has weakly designed encryption system producing insufficient level of confusion causing leakage of the keys easy enough to bypass a CPA using a good entropy "single pixel modified plain image". The pixel distribution does not meet the avalanche effect in[52]. Chen et al., 2020[53] cryptanalyzed and broke the 2D Henon Sine map based image encryption scheme presented by Wu et al., 2018[54] using CPA. The cryptanalysis procedure was applied, by identifying the weakness in the intermediate $mod256$ operations used within the diffusion process which permitted the intercepted image to percolate in the $S-boxes$. Teseleanu et al.,2022[55] broke the chaos based color image encryption scheme presented having enhanced logistic map (ELM) and enhanced Sine map (ESM) designed by Essaid et al., 2019[56] using odd and even size image inception for mounting CPA and CCA.Fan et al., 2021[57] broke Khan et al.'s scheme[50] presented in 2019, by using the circle chaotic map to breach the double diffusion of 3×3 color image through CPA and CCA. Hu et al., 2017[58] broke the Latin Square based confusion-diffusion scheme presented by Chen et al., 2015[53] using CPA and CCA through intercepted diffusion keys in both the rounds. The logistic map is used in the system to generate the latin square which is showing dense periodic windows due to improper choice of control parameter μ. Yu et al., 2021 broke the scheme presented by Hua et al., 2017[59] by constructing codebook on linear relationship between plain and cipher images in test. Wen et al., 2021[60] broke the scheme presented by Hua et al., 2017[59] through inception of like images in CPA and CCA and producing the equivalent permutation and diffusion keys. Li et al., 2002[61] broke the Chaotic key based algorithm (CKBA) presented by Guo et al., 2000[62] by intercepting one pair of CPA, CCA and COA through key captured using brute force as the bit size of the key is $2^{bitsize}$ of the computer. Wang et al., 2019[63] broke the double random polarization encryption scheme presented by Matoba et al., 2004[64] by intercepting the CPA and CCA against the polarized state. Wen et al., 2019[65] broke the DNA based image encryption algorithm presented by Song et al., 2015[66] which used spatiotemporal chaos. The scheme was broken by virtual matrix with quaternary matrices of size H X 4W where H is height and W is the width. Li et al., 2019[67] cracked the latin square based permutation diffusion presented by Hu et al., 2017[58] using CPA due the weakness that two rounds of fixed permuation diffusion network (PDN). Li et al., 2018[68] broke the scheme by Niyat et al., 2017[69] by detecting weakness in the discrete time diffusion model of DNA cell having finite number of states through intercepting duplicate lena test image by COA, KPA, CPA. Wang et al., 2018[70] broke Pak et al.'s Scheme, 2017[71] by replacing the diffusion-permutation matrix with KPA on intercepted duplicate image. Ma et al., 2020[72] broke Liu et al.'s, 2018[73] scheme block encryption of image using chaotic maps through CPA by obtaining the mask image and intercepting the encryption. Wen et al., 2019[74] broke the scheme of Shafique et al., 2018[75] of image encryption using bitplane extraction through use of multiple chaotic maps ($IEC - BPMC$) using interception of bit matrix of duplicate image using CPA as the scheme is designed at bit-level in key generation and encryption process. Zhou et al., 2019[76] broke Sheela et al.'s, 2018 scheme of two dimensional modified henon map (2D-MHM) along with hybrid chaotic shift transform (HCST). The key can be revealed after O($\lceil MNlog_c(MN)\rceil$) with duplicate image injection through CPA and CCA. A confusion operation controlled by 2D-MHM is carried out using HCST, and diffusion by the XOR operation occurs using a chaotic matrix produced by a sine map. Liu et al., 2020[77] broke the scheme of Yosefnezhad et al., 2019[78] which uses one dimensional chaotic sine coupled map. The system is intercepted by finding state mapping network for intercepted initial values of 1D sine coupled map at variants $\alpha = 19/2^5$, $\beta = 287/2^5$, $\gamma = 287/2^5$ using CPA in the intermediary state mappings through duplicate image injection. Fan et al., 2021[57] broke the scheme of Khan et al., 2019[50] which has traditional permutation diffusion structure having $one - round$ diffusion by incorporating CPA on $all - zero$ image and obtaining the diffusion matrix. Li et al., 2019[67] broke the scheme of Pak et al., 2019[79] having bitplane decomposition followed by linear transformation using mod256 operation for diffusion using the $all - zero$ image after $\lceil log_2(M \bullet 24N)\rceil$ chosen-plaintext images, therefore $\lceil log_2(M \bullet 24N)\rceil$ × of CPA. Li et al., 2021[80] broke the permutation–bit diffusion structure (PBDS) scheme presented by Mondal et al., 2021[81]. The scheme uses $2DSC3$ map for to get two random sequences R1 and R2. But the CPA attack on $all - zero$ image makes the random R1 and R2 unchanged, hence left unrandomized so can be captured after (O$\lceil log_2$ W×H$\rceil + 1$) computations where w is width and h are the height of the image. In history of chaotic ciphers, the baptista-type[82] cryptosystem was broken by creating an equivalence chaotic map and was re-iterated with a single-pixel change input image by using KPA. In modern cryptography and its cryptanalysis test, deep learning based adversarial networks[83],[84],[85] are designed to test the resistance of chaotic ciphers against CCA, CPA, COA, KPA and known attacks such as Jakimoski–Kocarev attack[86] on various design approaches used in chaotic ciphers. The Jakimoski-Kocarev attack[86] majorly deals with exploitation of the cipher using KPA and creation of equivalent key-schedules.

7.2.4 | Provably Secure is Explainable

In the realm of chaotic cryptology, we mathematically discuss the resistance to various types of attacks (CCA - Chosen Ciphertext Attack, CPA - Chosen Plaintext Attack, COA - Chosen-Or-Adaptive Attack, KPA - Known-Plaintext Attack) in the context of indistinguishability experiments.

1. Indistinguishability Experiment: The indistinguishability experiment involves an adversary trying to distinguish between two sets of ciphertexts or messages. In the context of chaotic cryptology, these sets could be related to different keys or plaintexts.

2. Chosen Ciphertext Attack (CCA): In a CCA scenario, the adversary can adaptively query the decryption oracle with chosen ciphertexts. The indistinguishability experiment tests whether the adversary can distinguish between ciphertexts encrypted under two different keys.

3. Mathematically, let $E_k(\cdot)$ represent encryption under key k and $D_k(\cdot)$ represent decryption under key k. For two keys k_0 and k_1, the indistinguishability experiment can be formulated as:

$$\Pr[\text{CCA}] = |\Pr[b = 0] - \Pr[b = 1]|$$

   Where b is a bit indicating whether the adversary guessed correctly. Resistance to CCA implies that the probabilities are indistinguishable.

4. Chosen Plaintext Attack (CPA): In a CPA scenario, the adversary can obtain encryptions of chosen plaintexts. The indistinguishability experiment tests whether the adversary can distinguish between two ciphertexts corresponding to different plaintexts. Mathematically:

$$\Pr[\text{CPA}] = |\Pr[b = 0] - \Pr[b = 1]|$$

5. Chosen-Or-Adaptive Attack (COA): COA is a hybrid scenario where the adversary has some adaptability in choosing ciphertexts or obtaining adaptive chosen ciphertexts. The indistinguishability experiment in a COA scenario extends the CCA formulation.

6. Known-Plaintext Attack (KPA):In a KPA scenario, the adversary knows the plaintext corresponding to some ciphertexts. The indistinguishability experiment tests whether the adversary can distinguish between ciphertexts encrypted under different keys. Mathematically,

   $$\Pr[\text{KPA}] = |\Pr[b = 0] - \Pr[b = 1]|$$

   For chaotic cryptology to be considered secure, it should exhibit low probabilities of success in these indistinguishability experiments across various attack scenarios as negligible < 0.1. The resistance to these attacks mathematically implies that the chaotic cryptosystem is robust and can withstand attempts to distinguish between different keys or plaintexts. Achieving indistinguishability is crucial for ensuring the confidentiality of information in the chaotic cryptosystem.

7.2.5 | Complete Security is not Explainable

In chaotic cryptology, achieving complete security is a complex challenge due to the inherent properties of chaotic systems. Chaotic systems are highly sensitive to initial conditions, making them difficult to predict. However, complete security in chaotic cryptology is not fully explainable or guaranteed, as it depends on various factors such as the design of the cryptographic algorithm, the quality of chaos used, and potential vulnerabilities. Researchers often explore chaotic systems for their pseudorandom properties, but the quest for absolute security remains an ongoing endeavor with no definitive solution.

7.2.6 | Time bounded Security is Explainable

Time-bounded security in chaotic cryptology involves considering the effectiveness of cryptographic algorithms within a specific time-frame. While chaotic systems exhibit unpredictability and complexity, achieving time-bounded security in chaotic cryptology poses challenges. The sensitivity to initial conditions in chaotic systems may introduce uncertainties in encryption/decryption processes, affecting the reliability of time constraints. Therefore, explaining and ensuring time-bounded security in chaotic cryptology requires a careful analysis of the algorithm's behavior over time and consideration of potential vulnerabilities that may arise within the specified timeframe.

7.2.7 | Explanation is not Data Specific

Achieving data-specific security in chaotic cryptology involves tailoring cryptographic mechanisms to the characteristics of specific data. In chaotic systems, the sensitivity to initial conditions and the pseudo-random behavior provide a foundation for data-specific security. However, explaining this security aspect is challenging as it depends on how well the chaotic system adapts to the unique properties of the data being encrypted. Designing a chaotic cryptosystem to cater to the specific requirements of data, such as sensitivity to certain patterns or types of information, requires a nuanced understanding of both chaotic dynamics and the nature of the data itself. While chaotic cryptology offers a potential framework, the specifics of achieving and explaining data-specific security demand careful consideration of the interplay between chaotic dynamics and the targeted data characteristics.

8 | DESIGN PRINCIPLES FOR ATTACK-RESISTANT CHAOTIC CIPHER DESIGN

i. **Dynamic Chaotic Maps:** Employ chaotic maps with dynamic properties to enhance unpredictability and resist attacks based on map analysis.

ii. **Parameter Sensitivity:** Exploit the sensitivity of chaotic systems to initial conditions and parameters, making the cipher resilient against attacks attempting to manipulate or predict parameters.

iii. **Nonlinearity and Complexity:** Introduce high nonlinearity and complexity in the cipher design to thwart linear and differential attacks.

iv. **Key Space Exploration:** Ensure a large and well-explored key space, making exhaustive search attacks computationally infeasible.

v. **Confusion and Diffusion:** Incorporate confusion and diffusion elements to obscure the relationship between the key and the ciphertext, enhancing the cipher's resistance against various attacks.

vi. **Multiple Chaotic Layers:** Employ multiple layers of chaotic transformations to increase the overall security of the cipher and resist attacks targeting specific layers.

vii. **Randomness Injection:** Integrate mechanisms for injecting true randomness into the cipher to counteract statistical attacks.

viii. **Adaptive Parameters:** Implement parameters that adapt over time or based on specific conditions, enhancing resistance against attacks attempting to exploit fixed parameters.

ix. **Key Management:** Establish robust key management practices, including secure key generation, distribution, and storage, to prevent key-based attacks.

x. **Cryptographic Hash Functions:** Integrate secure cryptographic hash functions to strengthen the overall security of the chaotic cipher, providing additional layers of protection.

9 | PROPOSED SOLUTION AND MITIGATION STRATEGY

9.1 | Time-Delay-Based Chaotic Cryptology for Multimedia Encryption

The science of developing and deciphering codes is known as cryptology. Whereas, the practice of composing codes is called cryptography. Time-delay-based cryptography leverages time lock puzzles and time-lock encryption in conjunction with chaotic ciphers to enhance security in multimedia encryption, providing resistance against various attacks. Tang et al. in 2010[87] invented chaotic coupled map lattices to produce time-bounded confusion-diffusion effect in chaotic cryptography implemented multimedia ciphers. Sprott J. C in 2007[88] invented a chaotic delay differential equation in which they configured the brownian's motion for the probability distribution function along the x-axis and get a time lapse of 4×10^3 with a time delay $\tau = 20$ over $N = 100$ iterations. Ozkaynak F and Yavuz S in 2013[45] designed a time delay based chaotic SBox where they used first order delay difference equation to transform logistic map attractor into first time derivative of x on three different chaotic maps namely the ikeda map, logistic map and the sinusoidal map. The method generates n-bit × n-bit S-boxes which operates by converting the outputs of the one-dimensional chaotic maps into integers between 0 and 2^n. We describe below the process to further concretize and extend similar methods and simplify their explanability into the context of time-delay based chaotic cryptology.

9.1.1 | Time Lock Puzzles

1. **Puzzle Generation:** Create time lock puzzles based on mathematical problems that require significant computational effort to solve.

2. **Time Constraint:** Set a time delay for puzzle solution, making it computationally infeasible to decipher the multimedia content before the predefined time elapses.

3. **Integration with Chaotic Cipher:** Embed the solution of the time lock puzzle as a key component in the chaotic cipher, ensuring synchronized decryption upon puzzle resolution.

9.1.2 | Time-Lock Encryption

1. **Temporal Constraints:** Implement temporal constraints in the encryption process, making decryption feasible only after a specified time period.

2. **Chaotic Cipher Integration:** Incorporate a chaotic cipher into the time-lock encryption scheme, enhancing the security of multimedia content by introducing chaotic dynamics.

3. **Dynamic Key Evolution:** Introduce time-based evolution of cryptographic keys within the chaotic cipher to resist attacks attempting to exploit static key information.

9.1.3 | Multimedia Encryption with Chaotic Cipher

1. **Chaotic Transformations:** Utilize chaotic maps for the encryption of multimedia content, introducing unpredictability and resistance against attacks.
2. **Dynamic Parameters:** Incorporate time-based parameters within the chaotic cipher to adapt to evolving security requirements and thwart potential attacks.
3. **Key Synchronization:** Ensure synchronization between time lock puzzle solutions, time-lock encryption constraints, and the chaotic cipher to achieve a coherent and secure multimedia encryption system.

The combination of time-delay-based cryptography, time lock puzzles, time-lock encryption, and chaotic ciphers forms a robust framework for multimedia encryption, providing enhanced resistance against various cryptographic attacks.

10 | FUTURE RESEARCH DIRECTIONS

Future research in chaotic cryptology holds exciting opportunities for advancing the security and resilience of cryptographic systems. Key areas of exploration include the reformulation of existing chaotic ciphers, integration of time delay time lock puzzles, and the development of testbeds using adversarial neural networks and deep learning adversarial networks. Furthermore, these prospects for improving the security and robustness of cryptographic systems through future research in chaotic cryptology are

10.1 | Reforming Chaotic Ciphers

1. **Dynamic Chaotic Mapping:** Investigate the use of dynamically evolving chaotic maps to enhance the unpredictability and resistance against attacks in chaotic ciphers.
2. **Key Evolution Mechanisms:** Explore novel techniques for introducing time-dependent key evolution mechanisms within chaotic ciphers to counteract adversarial attempts at exploiting static keys.
3. **Hybrid Encryption Schemes:** Consider hybrid encryption schemes that combine chaotic ciphers with other cryptographic primitives to achieve a balance between chaos-driven security and conventional cryptographic methods.

10.2 | Time Delay Time Lock Puzzles

1. **Puzzle Complexity Analysis:** Research and analyze the complexity of time lock puzzles to ensure they provide a robust time-bound security mechanism.
2. **Integration with Chaotic Ciphers:** Investigate methods for seamlessly integrating time delay time lock puzzles as a fundamental component of chaotic ciphers, ensuring synchronization and coherency in decryption.
3. **Adaptive Time Constraints:** Explore adaptive time constraints in time delay time lock puzzles, dynamically adjusting decryption times based on evolving security requirements.

10.3 | Testbed Design with Adversarial Neural Networks

1. **Adversarial Training:** Develop adversarial neural network models specifically designed to challenge and evaluate the security of chaotic ciphers with time delay time lock puzzles.
2. **Real-world Scenario Simulations:** Create realistic testbed scenarios that emulate practical usage conditions, allowing for a comprehensive assessment of the proposed chaotic cryptosystems.
3. **Deep Learning Adversarial Networks:** Investigate the application of deep learning adversarial networks to identify potential vulnerabilities and weaknesses in the integrated chaotic cryptographic schemes.

The future research landscape in chaotic cryptology presents a unique opportunity to advance the field by combining the strengths of chaotic dynamics, time delay time lock puzzles, and advanced adversarial network evaluations.

11 | CONCLUSION

Chaotic cryptography has emerged as a promising avenue for enhancing the security of multimedia content protection systems. The exploration of chaotic dynamics in cryptographic algorithms offers unique advantages in terms of unpredictability and resistance against various attacks. The choice between ante-hoc explanation and post-hoc explanation in chaotic cryptography presents a nuanced consideration. Ante-hoc explanation, where the rationale behind the cryptographic design is explained before its use, provides transparency and facilitates trust. On the other hand, post-hoc explanation allows for keeping certain design aspects confidential initially, potentially thwarting attackers who rely on a priori knowledge. Striking a balance between transparency and confidentiality becomes crucial in designing robust chaotic multimedia ciphers. The integration of time-delay time-lock puzzles into chaotic multimedia ciphers represents a futuristic approach to bolstering security. By introducing temporal constraints and dynamic key components, these ciphers become resilient against attacks attempting to exploit static parameters. The fusion of chaotic dynamics with time-bound cryptographic elements not only adds a layer of complexity but also aligns with the evolving nature of multimedia content protection needs. As we look to the future, research in chaotic cryptography for multimedia content protection should focus on refining existing chaotic ciphers with adaptive mechanisms, seamlessly integrating time-delay time lock puzzles, and employing advanced adversarial evaluations. This multifaceted approach ensures that the cryptographic systems are not only resistant to known attacks but also resilient against emerging threats. Conclusively, the synergy between chaotic dynamics, temporal constraints, and advanced cryptographic evaluations holds immense potential for the development of futuristic attack-resistant chaotic multimedia ciphers. This research not only contributes to the theoretical foundations of chaotic cryptography but also paves the way for practical implementations that address the evolving challenges in securing multimedia content. Thus, this paper presented research on a real use-case of AI-automated cyber-oriented digital engineering (CODE-pilot), which provides a unified framework for efficient integration across cyber-physical embedded IoT platforms. It also provides additional insight into standardization through DevSecOps as a research outcome.

Author contributions

Devisha Tiwari: review and editing (equal); Conceptualization (in supervision); writing – original draft (lead); formal analysis (equal); writing – review and editing (equal); Methodology (lead); Conceptualization (lead). Bhaskar Mondal: formal analysis(supervision);writing – review and editing (supervision); resources-gathering and analysis(supervision).

DATA AVAILABILITY

The data used in the research is available freely and need no permission for use. The code is conceptually designed and developed in Matlab R2018a and is available with the authors, will be shared upon request.

FUNDING

No research grant was availed for pursuing the stated research. No funding is received from any research support bodies.

ACKNOWLEDGMENT

I owe a deepest gratitude to Dr. Bhaskar Mondal Sir my doctoral supervisor, for his wise counsel, unwavering encouragement, and adherence. Throughout all of the presented scientific work, his vast knowledge and wealth of experience have captivated to work over the proposed concept.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CONFLICT OF INTEREST

- **Disclosure of potential conflicts of interest**
  We declare that we have no conflict of interest in relation to the proposed work and we oblige to our roles as authors of the work. We undertake to carry our duties with the highest degree of objectivity and integrity.

- **Research involving Human Participants and/or Animals**
  We certify that no human subject or biological material has ever been used in any of the studies in the proposed work. We declare that no research was done for the planned task that would be considered an infraction of animal protection legislation.

- **Informed Consent**
  We attest that the planned work is completed utilising the viewpoints, plans, and technique that have been previously discussed and finalized. We concurred on every point on the manner the work would be done.

References

1. Li S, Chen G, Zheng X, others . Chaos-based encryption for digital image and video. *Multimedia Encryption and Authentication Techniques and Applications* 2006; 129.

2. Hasimoto-Beltrán R. High-performance multimedia encryption system based on chaos. *Chaos: An Interdisciplinary Journal of Nonlinear Science* 2008; 18(2).

3. Radha N, Venkatesulu M. A chaotic block cipher for real-time multimedia. *Journal of Computer Science* 2012; 8(6): 994.

4. Li L, Abd El-Latif AA, Jafari S, Rajagopal K, Nazarimehr F, Abd-El-Atty B. Multimedia cryptosystem for IoT applications based on a novel chaotic system around a predefined manifold. *Sensors* 2022; 22(1): 334.

5. Masuda N, Jakimoski G, Aihara K, Kocarev L. Chaotic block ciphers: from theory to practical algorithms. *IEEE Transactions on Circuits and Systems I: Regular Papers* 2006; 53(6): 1341–1352.

6. Huang X. Image encryption algorithm using chaotic Chebyshev generator. *Nonlinear Dynamics* 2012; 67: 2411–2417.

7. Zhu H, Zhang Y, Sun Y. Provably Secure Multi-server Privacy-Protection System Based on Chebyshev Chaotic Maps without Using Symmetric Cryptography.. *Int. J. Netw. Secur.* 2016; 18(5): 803–815.

8. Ren Y, Chen JC, Chin JC, Tseng YC. Design and analysis of the key management mechanism in evolved multimedia broadcast/multicast service. *IEEE Transactions on Wireless Communications* 2016; 15(12): 8463–8476.

9. Trappe W, Song J, Poovendran R, Liu KR. Key management and distribution for secure multimedia multicast. *IEEE transactions on Multimedia* 2003; 5(4): 544–557.

10. Luo Y, Yu J, Lai W, Liu L. A novel chaotic image encryption algorithm based on improved baker map and logistic map. *Multimedia Tools and Applications* 2019; 78: 22023–22043.

11. Belazi A, Kharbech S, Aslam MN, et al. Improved Sine-Tangent chaotic map with application in medical images encryption. *Journal of Information Security and Applications* 2022; 66: 103131.

12. Ye G, Wu H, Liu M, Shi Y. Image encryption scheme based on blind signature and an improved Lorenz system. *Expert Systems with Applications* 2022; 205: 117709.

13. Ping P, Xu F, Mao Y, Wang Z. Designing permutation–substitution image encryption networks with Henon map. *Neurocomputing* 2018; 283: 53–63.

14. Essaid M, Akharraz I, Saaidi A, Mouhib A. A new image encryption scheme based on confusion-diffusion using an enhanced skew tent map. *Procedia Computer Science* 2018; 127: 539–548.

15. Ramasamy P, Ranganathan V, Kadry S, Damaševičius R, Blažauskas T. An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—Tent map. *Entropy* 2019; 21(7): 656.

16. Zhu H, Zhao C, Zhang X, Yang L. An image encryption scheme using generalized Arnold map and affine cipher. *Optik* 2014; 125(22): 6672–6677.

17. Chen G, Mao Y, Chui CK. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals* 2004; 21(3): 749–761.

18. Chen H, Tanougast C, Liu Z, Blondel W, Hao B. Optical hyperspectral image encryption based on improved Chirikov mapping and gyrator transform. *Optics and Lasers in Engineering* 2018; 107: 62–70.

19. Zhang Y, Xiao D. Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform. *Optics and Lasers in Engineering* 2013; 51(4): 472–480.

20. Liu L, Jiang D, Wang X, Rong X, Zhang R. 2D Logistic-Adjusted-Chebyshev map for visual color image encryption. *Journal of Information Security and Applications* 2021; 60: 102854.

21. Hua Z, Jin F, Xu B, Huang H. 2D Logistic-Sine-coupling map for image encryption. *Signal Processing* 2018; 149: 148–161.

22. Wang X, Guan N, Zhao H, Wang S, Zhang Y. A new image encryption scheme based on coupling map lattices with mixed multi-chaos. *Scientific reports* 2020; 10(1): 9784.

23. Khalil N, Sarhan A, Alshewimy MA. An efficient color/grayscale image encryption scheme based on hybrid chaotic maps. *Optics & Laser Technology* 2021; 143: 107326.

24. Saravanan S, Sivabalakrishnan M. A hybrid chaotic map with coefficient improved whale optimization-based parameter tuning for enhanced image encryption. *Soft Computing* 2021; 25: 5299–5322.

25. Farah MB, Farah A, Farah T. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. *Nonlinear Dynamics* 2020; 99(4): 3041–3064.

26. Patro KAK, Acharya B. An efficient dual-layer cross-coupled chaotic map security-based multi-image encryption system. *Nonlinear Dynamics* 2021; 104(3): 2759–2805.

27. Setiadi DRIM, Rijati N. An Image Encryption Scheme Combining 2D Cascaded Logistic Map and Permutation-Substitution Operations. *Computation* 2023; 11(9): 178.

28. Pourjabbar Kari A, Habibizad Navin A, Bidgoli AM, Mirnia M. A new image encryption scheme based on hybrid chaotic maps. *Multimedia Tools and Applications* 2021; 80: 2753–2772.

29. Wang T, Ge B, Xia C, Dai G. Multi-image encryption algorithm based on cascaded modulation chaotic system and block-scrambling-diffusion. *Entropy* 2022; 24(8): 1053.

30. Lambić D. A novel method of S-box design based on discrete chaotic map. *Nonlinear dynamics* 2017; 87: 2407–2413.

31. Özkaynak F. On the effect of chaotic system in performance characteristics of chaos based s-box designs. *Physica A: Statistical Mechanics and Its Applications* 2020; 550: 124072.

32. Mousavi M, Sadeghiyan B. A new image encryption scheme with Feistel like structure using chaotic S-box and Rubik cube based P-box. *Multimedia Tools and Applications* 2021; 80: 13157–13177.

33. Zhang X, Zhao Z, Wang J. Chaotic image encryption based on circular substitution box and key stream buffer. *Signal Processing: Image Communication* 2014; 29(8): 902–913.

34. Irawan C, Rachmawanto EH, Sari CA, Doheir M, others . Hybrid encryption using confused and stream cipher to improved medical images security. In: . 1201. IOP Publishing. ; 2019: 012022.

35. He P, Sun K, Zhu C. A novel image encryption algorithm based on the delayed maps and permutation-confusion-diffusion architecture. *Security and Communication Networks* 2021; 2021: 1–16.

36. Praveenkumar P, Amirtharajan R, Thenmozhi K, Rayappan JBB. Fusion of confusion and diffusion: a novel image encryption approach. *Telecommunication Systems* 2017; 65: 65–78.

37. Praveenkumar P, Amirtharajan R, Thenmozhi K, Rayappan JBB. Medical data sheet in safe havens–A tri-layer cryptic solution. *Computers in biology and medicine* 2015; 62: 264–276.

38. Hussain I, Shah T. Literature survey on nonlinear components and chaotic nonlinear components of block ciphers. *Nonlinear Dynamics* 2013; 74: 869–904.

39. Janakiraman S, Thenmozhi K, Rayappan JBB, Amirtharajan R. Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller. *Microprocessors and Microsystems* 2018; 56: 1–12.

40. Alvarez G, Li S. Cryptographic requirements for chaotic secure communications. *arXiv preprint nlin/0311039* 2003.

41. Kwok H, Tang WK. A fast image encryption system based on chaotic maps with finite precision representation. *Chaos, solitons & fractals* 2007; 32(4): 1518–1529.

42. Behnia S, Akhshani A, Mahmodi H, Akhavan A. Chaotic cryptographic scheme based on composition maps. *International Journal of Bifurcation and chaos* 2008; 18(01): 251–261.

43. Solak E. Cryptanalysis of chaotic ciphers. In: Springer. 2011 (pp. 227–256).

44. Xiao D, Liao X, Deng S. Chaos based hash function. *Chaos-Based Cryptography: Theory, Algorithms and Applications* 2011: 137–203.

45. Özkaynak F, Yavuz S. Designing chaotic S-boxes based on time-delay chaotic system. *Nonlinear Dynamics* 2013; 74: 551–557.

46. Ghebleh M, Kanso A. A robust chaotic algorithm for digital image steganography. *Communications in Nonlinear Science and Numerical Simulation* 2014; 19(6): 1898–1907.

47. Akhavan A, Samsudin A, Akhshani A. Cryptanalysis of "an improvement over an image encryption method based on total shuffling". *Optics Communications* 2015; 350: 77–82.

48. Li C, Zhang Y, Xie EY. When an attacker meets a cipher-image in 2018: A year in review. *Journal of Information Security and Applications* 2019; 48: 102361.

49. Alanazi AS, Munir N, Khan M, Asif M, Hussain I. Cryptanalysis of novel image encryption scheme based on multiple chaotic substitution boxes. *IEEE Access* 2021; 9: 93795–93802.

50. Khan M, Masood F. A novel chaotic image encryption technique based on multiple discrete dynamical maps. *Multimedia Tools and Applications* 2019; 78: 26203–26222.

51. Arroyo D, Diaz J, Rodriguez F. Cryptanalysis of a one round chaos-based substitution permutation network. *Signal Processing* 2013; 93(5): 1358–1364.

52. Wang X, Teng L, Qin X. A novel colour image encryption algorithm based on chaos. *Signal Processing* 2012; 92(4): 1101–1108.

53. Chen Jx, Zhu Zl, Fu C, Zhang Lb, Zhang Y. An efficient image encryption scheme using lookup table-based confusion and diffusion. *Nonlinear Dynamics* 2015; 81: 1151–1166.

54. Wu J, Liao X, Yang B. Image encryption using 2D Hénon-Sine map and DNA approach. *Signal processing* 2018; 153: 11–23.

55. Teseleanu G. Security Analysis of a Color Image Encryption Scheme Based on Dynamic Substitution and Diffusion Operations. *Cryptology ePrint Archive* 2022.

56. ESSAID M, AKHARRAZ I, SAAIDI A, MOUHIB A. A new approach of image encryption based on dynamic substitution and diffusion operations. In: IEEE. ; 2019: 1–6.

57. Fan H, Zhang C, Lu H, Li M, Liu Y. Cryptanalysis of a New Chaotic Image Encryption Technique Based on Multiple Discrete Dynamical Maps. *Entropy* 2021; 23(12): 1581.

58. Hu G, Xiao D, Wang Y, Li X. Cryptanalysis of a chaotic image cipher using Latin square-based confusion and diffusion. *Nonlinear Dynamics* 2017; 88: 1305–1316.

59. Hua Z, Zhou Y. Design of image cipher using block-based scrambling and image filtering. *Information sciences* 2017; 396: 97–113.

60. Wen H, Zhang C, Huang L, Ke J, Xiong D. Security analysis of a color image encryption algorithm using a fractional-order chaos. *Entropy* 2021; 23(2): 258.

61. Li S, Zheng X. Cryptanalysis of a chaotic image encryption method. In: . 2. IEEE. ; 2002: II–II.

62. Guo JI, others . A new chaotic key-based design for image encryption and decryption. In: . 4. IEEE. ; 2000: 49–52.

63. Wang L, Wu Q, Situ G. Chosen-plaintext attack on the double random polarization encryption. *Optics express* 2019; 27(22): 32158–32167.

64. Matoba O, Javidi B. Secure holographic memory by double-random polarization encryption. *Applied optics* 2004; 43(14): 2915–2919.

65. Wen H, Yu S, Lü J. Breaking an image encryption algorithm based on DNA encoding and spatiotemporal chaos. *Entropy* 2019; 21(3): 246.

66. Song C, Qiao Y. A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos. *Entropy* 2015; 17(10): 6954–6968.

67. Li M, Lu D, Xiang Y, Zhang Y, Ren H. Cryptanalysis and improvement in a chaotic image cipher using two-round permutation and diffusion. *Nonlinear Dynamics* 2019; 96: 31–47.

68. Li M, Lu D, Wen W, Ren H, Zhang Y. Cryptanalyzing a color image encryption scheme based on hybrid hyper-chaotic system and cellular automata. *IEEE access* 2018; 6: 47102–47111.

69. Niyat AY, Moattar MH, Torshiz MN. Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Optics and Lasers in Engineering* 2017; 90: 225–237.

70. Wang H, Xiao D, Chen X, Huang H. Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map. *Signal processing* 2018; 144: 444–452.

71. Pak C, Huang L. A new color image encryption using combination of the 1D chaotic map. *Signal Processing* 2017; 138: 129–137.

72. Ma Y, Li C, Ou B. Cryptanalysis of an image block encryption algorithm based on chaotic maps. *Journal of Information Security and Applications* 2020; 54: 102566.

73. Liu L, Hao S, Lin J, Wang Z, Hu X, Miao S. Image block encryption algorithm based on chaotic maps. *IET Signal Processing* 2018; 12(1): 22–30.

74. Wen H, Yu S. Cryptanalysis of an image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps. *The European Physical Journal Plus* 2019; 134: 1–16.

75. Shafique A, Shahid J. Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps. *The European Physical Journal Plus* 2018; 133(8): 331.

76. Zhou K, Xu M, Luo J, Fan H, Li M. Cryptanalyzing an image encryption based on a modified Henon map using hybrid chaotic shift transform. *Digital Signal Processing* 2019; 93: 115–127.

77. Liu Y, Qin Z, Liao X, Wu J. Cryptanalysis and enhancement of an image encryption scheme based on a 1-D coupled Sine map. *Nonlinear Dynamics* 2020; 100: 2917–2931.

78. Yosefnezhad Irani B, Ayubi P, Amani Jabalkandi F, Yousefi Valandar M, Jafari Barani M. Digital image scrambling based on a new one-dimensional coupled Sine map. *Nonlinear Dynamics* 2019; 97(4): 2693–2721.

79. Pak C, An K, Jang P, Kim J, Kim S. A novel bit-level color image encryption using improved 1D chaotic map. *Multimedia Tools and Applications* 2019; 78(9): 12027–12042.

80. Li M, Wang P, Yue Y, Liu Y. Cryptanalysis of a secure image encryption scheme based on a novel 2D sine–cosine cross-chaotic map. *Journal of Real-Time Image Processing* 2021: 1–15.

81. Mondal B, Behera PK, Gangopadhyay S. A secure image encryption scheme based on a novel 2D sine–cosine cross-chaotic (SC3) map. *Journal of Real-Time Image Processing* 2021; 18(1): 1–18.

82. Li S, Chen G, Wong KW, Mou X, Cai Y. Baptista-type chaotic cryptosystems: problems and countermeasures. *Physics Letters A* 2004; 332(5-6): 368–375.

83. Maghrebi H, Portigliatti T, Prouff E. Breaking cryptographic implementations using deep learning techniques. In: Springer. ; 2016: 3–26.

84. Coutinho M, Oliveira Albuquerque dR, Borges F, Garcia Villalba LJ, Kim TH. Learning perfectly secure cryptography to protect communications with adversarial neural cryptography. *Sensors* 2018; 18(5): 1306.

85. Esposito C, Su X, Aljawarneh SA, Choi C. Securing collaborative deep learning in industrial applications within adversarial scenarios. *IEEE Transactions on Industrial Informatics* 2018; 14(11): 4972–4981.

86. Li S, Mou X, Ji Z, Zhang J, Cai Y. Performance analysis of Jakimoski–Kocarev attack on a class of chaotic cryptosystems. *Physics Letters A* 2003; 307(1): 22–28.

87. Tang Y, Wang Z, Fang Ja. Image encryption using chaotic coupled map lattices with time-varying delays. *Communications in Nonlinear Science and Numerical Simulation* 2010; 15(9): 2456–2468.

88. Sprott J. A simple chaotic delay differential equation. *Physics Letters A* 2007; 366(4-5): 397–402.

AUTHOR BIOGRAPHY

Devisha Arunadevi Tiwari is currently working as an Assistant Professor in Computer Science Engineering(Data Science) department at Ace Engineering College, affiliated to Jawaharlal Nehru Technological University, Hyderabad, Telangana, India. She is pursuing PhD in Computer Science and Engineering from NIT Patna. She received her Master's Degree in Computer Science and Engineering from Rashtrasant Tukodoji Maharaj Nagpur University. She has qualified Bachelor's in Engineering in Computer Technology (Industry Collaborated).She is an Axelos Certified Project Manager and has qualified Data Scientist Masters Program from SimpliLearn Pvt Ltd in Apache Alliance partnership under the Apache Software Foundation. She worked as a Software Engineer(offshore) for four years.She is a member of ACM, IAENG and CSTA. Her research interest includes Deep Learning Architectures, AI and Robotics, Fuzzy Neural Networks and Social Networks Mining Algorithms, Cryptography and Information Security.

Bhaskar Mondal (Ph.D) serves as an Assistant Professor in the Department of Computer Science and Engineering at the National Institute of Technology (NIT) Patna. He has nearly 10 years of experience in academics and research during which he had worked at NIT Patna, Xavier University Bhubaneswar (XUB), Orisha, India. BIT Sindri, Dhanbad, and NIT Jamshedpur. He was conferred with PhD from the National Institute of Technology Jamshedpur, India in 2018 followed by M. Tech. (CSE) from Kalyani Government Engineering. He has published more than 40 research papers in reputed journals and international conferences. He is senior member of IEEE and ACM, Life member of Computer Society of India (CSI) and Cryptology Research society of India (CRSI). He is a book series editor titled Cyber Security of CRC Press. He acted as Lead Guest Editor for a special issue in CAEE, Elsevier. He has served several international conferences as session chair, advisory committee member and technical committee member. He has also reviewed articles in journals include Artificial Intelligence Review, Scientific Reports, Security and Communication Networks, Innovations in Systems and Software Engineering, ICT Express, IEEE Access, etc. His research interests include lightweight cryptography and machine learning.