UDC 003.26.09
DOI: 10.15587/1729-4061.2025.331044

IDENTIFYING THE EFFICIENCY OF APPLYING OF FINITE AUTOMATA IN ENCRYPTION AND DECRYPTION

Zhanat Saukhanova
Candidate of Physical and Mathematical Sciences,
Associate Professor*

Altynbek Sharipbay
Doctor of Technical Sciences, Professor
Department of Artificial Intelligence Technologies**

Gulmira Shakhmetova
Corresponding author
Senior Lecturer*
E-mail: sh_mira2004@mail.ru

Alibek Barlybayev
Doctor PhD, Professor
Department of Artificial Intelligence Technologies
L.N. Gumilyov Eurasian National University
Satbayev str., 2, Astana, Republic of Kazakhstan, 010008

Sayat Raykul
Student*

Altay Khassenov
Student*
*Department of Information Security**
**L.N. Gumilyov Eurasian National University
Satbayev str., 2, Astana, Republic of Kazakhstan, 010008

The contemporary cryptographic field is marked by efforts to enhance traditional methods through the integration of novel mathematical concepts. This fusion seeks to address the shortcomings of classical cryptography, tackle emerging security challenges, and devise more sophisticated data protection systems. Among these innovations is the application of finite automata, or CryptoAutomata, used as encoders and decoders. The object of this research is the use of finite automata, specifically CryptoAutomata, in cryptographic systems. The study addresses the problem of vulnerabilities in classical cryptographic methods, which include susceptibility to emerging cryptanalytic attacks and inefficiencies in computational overhead.

The essence of the obtained results lies in demonstrating the practical implementation and cryptographic advantages of reversible finite automata, including surjective and Mealy automata, integrated into encryption systems. Due to the inherent properties of these automata, such as reversibility, composability, and computational efficiency, the authors were able to increase the security of encryption, significantly complicating cryptanalysis attempts. These results are primarily explained by the compositional approach, which involves combining multiple finite automata to form complex encryption structures. Rigorous statistical evaluations were carried out, including NPCR and UACI, which yielded NPCR values ranging between 99.56% to 99.61% and UACI values around 33%, affirming strong resistance to differential attacks. Additionally, noise resilience was confirmed through PSNR evaluations, achieving values above 35 dB even under significant noise conditions, thereby validating robustness in practical scenarios. Furthermore, the cryptographic strength was substantiated by NIST statistical randomness tests

Keywords: finite automata, mealy automata, cryptography with finite automata, automata composition, statistical cryptanalysis

Received 06.03.2025
Received in revised form 21.04.2025
Accepted date 22.05.2025
Published date 25.06.2025

How to Cite: *Saukhanova, Z., Sharipbay, A., Shakhmetova, G., Barlybayev, A., Raykul, S., Khassenov, A. (2025). Identifying the efficiency of applying of finite automata in encryption and decryption. Eastern-European Journal of Enterprise Technologies, 3 (9 (135)), 65–78. https://doi.org/10.15587/1729-4061.2025.331044*

1 Introduction

In modern conditions, the necessity for scientific research on cryptographic systems using finite automata arises from the increasing sophistication and frequency of cyber-attacks, coupled with the growing computational power available to attackers. Classical cryptographic methods, while reliable historically, now exhibit vulnerabilities and limitations due to advances in computational technology, making previously secure algorithms susceptible to cryptanalysis. Research into CryptoAutomata addresses these limitations by leveraging automata theory, providing cryptographic solutions that are reversible, computationally efficient, and robust against advanced cryptanalytic attacks. Given the proliferation of IoT devices, embedded systems, and environments with constrained resources, lightweight yet secure cryptographic methods based on finite automata offer practical solutions that classical, computation-intensive cryptosystems cannot effectively provide.

Currently, there are a wide range of cryptosystems that ensure the secure storage and transmission of data. Each of these cryptosystems has its own advantages and disadvantages. For example, symmetric cryptosystems are easy to implement in hardware and are faster in execution compared to asymmetric ones. However, these cryptosystems face challenges in securely distributing keys [1]. Asymmetric cryptosystems require a lot of computing power to implement, but they provide integrity and non-repudiation, which gives them a greater advantage over symmetric cryptosystems. In terms of key size, symmetric encryption has an advantage over asymmetric encryption, as its key sizes are much smaller [2].

The drawbacks of cryptographic algorithms drive the development of fundamentally new ciphers or the improvement of existing ones. As an alternative approach to designing cryptosystems, automata theory has been proposed. Nowadays some cryptosystems based on CryptoAutomata have been developed. They applied different various of automata,

Copyright © 2025, Authors. This is an open access article under the Creative Commons CC BY license

such as Glushkov automata, cellular automata, Mealy/Moore machines, Rabin-Scott models and others [3].

Automata theory is a branch of theoretical computer science that studies abstract computing devices. An automaton is a mathematical model that represents an abstract machine that performs calculations and data transformations depending on their state and input data [4]. Automata theory is used in various scientific and applied research. This theory is fundamental to the advancement of algorithms, compilers, cryptosystems, and various other fields within computer science.

The motivation for using cryptosystems based on finite automata lies in their ability to provide reversible, composable, and computationally lightweight encryption mechanisms. Unlike traditional number-theory-based cryptosystems, finite automata can be efficiently implemented via state transitions and lookup tables, avoiding heavy arithmetic operations. This makes them suitable for hardware-constrained environments such as embedded systems and IoT. Furthermore, finite automata offer structural diversity (Mealy, surjective, and information lossless types), which can be exploited to increase cryptographic complexity and reduce the risk of successful cryptanalysis. By composing multiple automata, it becomes possible to expand the key space and construct more obfuscated encryption schemes. The practical results of research into cryptographic systems based on finite automata are significant. They offer robust, secure, and computationally efficient encryption methods suitable for real-world applications, particularly in resource-constrained environments such as embedded systems and IoT devices. The results can enhance data security by significantly increasing the difficulty of cryptanalysis, demonstrated through high NPCR (approximately 99.56–99.61%) and optimal UACI values (~33%), indicating strong resistance to differential attacks. Also, the results can provide effective resilience against noise attacks, confirmed by high PSNR values (exceeding 35 dB), ensuring data integrity even in noisy transmission conditions. The research results can contribute to the development of modular cryptographic systems validated by empirical statistical tests (NIST tests, NPCR, UACI, PSNR), ensuring cryptographic reliability and real-world applicability.

2. Literature review and problem statement

There are various cryptosystems that are based on finite automata. The cryptosystems under study can be classified into two classes: some are based on transducer-automata (finite automata with output), and others are based on recognizer-automata (finite automata without output). In this paper, the foundation for the study of CryptoAutomata is cryptosystems such as FAPKC [5], DAFA, FSAaCIT and others.

Finite Automaton Public Key Cryptosystem [6] focuses on the development and presentation of a public key cryptosystem and associated digital signature scheme that utilizes finite automata as the underlying mathematical structure. The paper proposes using the properties and operations of finite automata as the basis for constructing a public key cryptosystem. The complexity of problems related to finite automata, such as state equivalence or language recognition for certain types of automata, might be leveraged to create the one-way functions or trapdoor functions necessary for public key cryptography. The public key would likely be derived from some description of an automaton or a related structure, while the private key would consist of secret information about the automaton's internal structure or a related transformation that allows for efficient decryption or signing.

The DAFA [7] cryptosystem aims to provide a secure and efficient method for encrypting data. It combines the strengths of the Data Encryption Standard with the flexibility of finite automata to create a novel encryption scheme. The DAFA cryptosystem is designed to be lightweight, making it suitable for resource-constrained environments. However, this study does not provide a precise analysis of its security properties, especially when compared to more modern and widely used cryptographic algorithms.

FSAaCIT [8] proposed system or technique designed for secure data de-duplication specifically within cloud computing environments. It achieves this by combining a symmetric cryptographic method based on Finite State Automata for security with a chunk-based technique for processing and indexing data to identify and eliminate redundancy. The system aims to provide the storage and bandwidth efficiency benefits of de-duplication while ensuring the confidentiality and integrity of data stored in the cloud through its integrated FSA-based one-key cryptosystem. The chunk-based indexing facilitates the de-duplication process by allowing the system to identify and manage duplicate data segments at a granular level. But, simply encrypting data can complicate the de-duplication process, as identical plaintext chunks will result in different ciphertext chunks if standard encryption modes are used with unique initial vectors or random padding.

This work [9] focuses on developing a framework that integrates the properties of finite automata with authenticated encryption schemes, aiming to enhance both security and performance. The authors outline specific design principles for constructing an AE scheme based on finite automata. They emphasize the importance of ensuring that the system can withstand various attacks while maintaining efficiency.

[10] describes a one-key (symmetric) cryptosystem where both encryption and decryption operations are based on the state transitions and output functions of a finite nonlinear automaton. The key of the cryptosystem is used to define or parameterize the specific finite nonlinear automaton used. The encryption process involves feeding the plaintext through the automaton, potentially using the automaton's state and input to determine the output (ciphertext). The decryption process, using the same key and thus the same automaton, reverses this operation to recover the original plaintext from the ciphertext. The nonlinearity of the automaton is intended to provide cryptographic strength, making it difficult for an adversary to predict the output or determine the key based on observed plaintext-ciphertext pairs. The security analysis presented in the paper would typically discuss the system's resistance to various cryptographic attacks, such as known-plaintext attacks, chosen-plaintext attacks, and state recovery attacks, based on the properties of the chosen nonlinear automaton. An extended Mealy automaton was considered. The secret key included the state transition functions of the automaton and the value of internal and external variables. Rounds' number and the size of blocks plaintext and the key length were arbitrary and were set by the users themselves. However, the key length had to be even.

In cryptography, FSMs [11] can be utilized to model the behavior of cryptographic algorithms and protocols, ensuring that they adhere to specified security properties. FSMs can represent the operational flow of cryptographic algorithms, allowing researchers to analyze their security properties systematically. The integration of finite state machines and recursive functions into cryptosystems enhances our understanding of algorithmic behavior and security properties.

In the system FAPKC weakly reversible linear and nonlinear FA with input-output memory with finite delay τ was used as the key space. This cryptosystem is asymmetric, which means that a public key is used to encrypt the plaintext. The public key in FAPKC consists of a sequential composition of the FA, the initial encryption state, and a finite delay τ. A private key is applied for decryption of cipher text. Inverse FA, states are elements of this secret key. Decomposition of composition automata is challenging, which contributes the cryptosystem's reliability [12]. The FAPKC cryptosystem was improved to version FAPKC3 [13] and to FAPKC4 [14], in which a FA with pseudo-memory was added.

More modern works on the use of automata in cryptography include [8, 15, 16]. In [15] a Symmetric Key Cryptosystem based on Sequential State Machine is shown. In this cryptosystem, the open text is transformed using a permutation function, then fed to a weakly reversible finite state machine. The encrypted text is passed through a reverse finite state machine, then the reverse permutation function is applied and the original text is obtained. The proposed cryptosystem is more efficient and reduces the time complexity by 30% compared to DES.

The paper [16] describes a new method for using finite automata in image encryption. The presented technology consists of the following: the original image is passed through a permutation automaton, and then a compositional automaton is applied to the intermediate data. The presented statistical data demonstrate the effectiveness of this method. This enhancement is achieved through the application of cryptographic processes, namely encryption and decryption, which are standard techniques for protecting information confidentiality. Encryption transforms data into an unreadable format, while decryption reverses this process using a key, making the data accessible only to authorized parties. The distinguishing characteristic of the methodology presented in this paper its foundation on FSMs. FSMs are mathematical models of computation used to design systems that transition between a finite number of states in response to inputs. The paper explores how an FSM-based approach can be utilized to develop a new system or algorithm for encrypting and decrypting images, aiming to provide a robust method for protecting visual information from unauthorized access or tampering.

In the field of cryptographic protocol evaluation, the paper [17] provides a robust approach through the development of a 9-tuples abstract model based on Finite State Machine (FSM), illustrating its practical application in simulating network behaviors on the OMNeT++ platform. Their research notably highlights the impact of protocols like the Internet Key Exchange (IKEv2) on network communication efficiency, demonstrating an average increase of 12% in time delay under simulated Denial of Service attack scenarios. This study substantiates the utility of FSM in cryptographic analysis and advances our understanding of protocol performance under adversarial conditions, offering a valuable framework for assessing the resilience and overhead of cryptographic protocols within communication networks. But, the complexity of cryptographic protocols, involving multiple participants, concurrent actions, and cryptographic operations, necessitates a systematic approach to modeling to avoid state explosion and accurately capture the protocol's logic and potential interactions, including those with a potential adversary.

The article [18] proposes a novel FPGA-based implementation of the AES cryptographic algorithm that incorporates a two-layered defense strategy against power analysis attacks, utilizing the structure of a finite state machine combined with a random number generator. Their approach not only masks intermediate variables but also randomizes operation sequences and incorporates dummy computations to enhance security. Cryptographic algorithms are essential for securing data in various applications, including communications, banking, and personal privacy. However, they are vulnerable to side-channel attacks that can reveal sensitive information through indirect means, such as timing information, power consumption, or electromagnetic leaks. These vulnerabilities necessitate robust countermeasures to protect against potential exploits.

The paper [19] describes the finite-size effects on the performance of continuous-variable measurement-device-independent quantum key distribution, offering a critical evaluation under practical conditions. Their study applies refined parameter estimation techniques to assess how finite data blocks impact the security key rate, showing a decrement in performance with reduced block sizes but maintaining operational viability over metropolitan distances with sufficiently large data sets. In the context of quantum cryptography, finite-size analysis refers to the study of the security of quantum key distribution protocols when the number of transmitted signals (or the size of the data set) is finite. In practice, the number of signals that can be transmitted is always limited, and this limitation can have significant implications for the security of the protocol.

In the domain of cryptographic security, the work [20] stands out for its innovative approach to enhancing the nonlinearity of S-boxes, which are critical components in thwarting differential, linear, and algebraic attacks in modern cipher systems. This research introduces a novel method for constructing 8-bit S-boxes by leveraging the properties of smaller 4-bit S-boxes combined with finite field multiplication. This technique not only addresses the challenge of generating S-boxes with nearly optimal cryptographic properties but also achieves an impressive nonlinearity value of up to 108. This development is significant as it contributes to the ongoing refinement of S-box construction methodologies, offering a promising avenue for developing more secure cryptographic systems. While the study claims high nonlinearity values, it does not extensively compare the performance of the proposed S-boxes with widely adopted S-boxes such as those in AES or Camellia. Without empirical benchmarking, it's difficult to evaluate practical superiority. The analysis heavily emphasizes nonlinearity but gives limited quantitative treatment to differential uniformity and avalanche criteria. These are equally crucial for resisting differential and statistical attacks. A broader set of metrics (e.g., algebraic degree, linear approximation table) would enhance credibility.

The [21] publication explores the integration of quantum mechanics with cryptography, focusing on the construction of robust cryptosystems using quantum spinning, rotation, and finite state machines. The authors suggest that by using the principles of quantum mechanics, specifically quantum spinning and rotation, and the mathematical model of FSM, it is possible to create a secure communication system. The proposed method involves using quantum spinning and rotation to encode and decode information. The authors suggest that by using the spin of particles to represent information, it is possible to create a secure communication system. The FSM is used to model the behavior of the quantum system and to ensure that the information is transmitted securely. In practice, this method is difficult to implement in real time.

In the study [22], the authors explore cryptographic protocols in non-interactive settings using noisy channels. They extend previous work, focusing on the completeness of finite channels in cryptographic protocols where only one party speaks. Key findings from this work include demonstrating the completeness of bit-ROT (Randomized Oblivious Transfer) with inverse polynomial error, proving that no finite channel can realize string-ROT with negligible error, and characterizing finite channels capable of enabling zero-knowledge proofs. The assumption that bit-ROT can be complete under inverse polynomial error may be too lenient for practical applications, where negligible error (e.g., exponentially small) is often the benchmark. This raises questions about the applicability of the completeness result in cryptographic systems requiring stronger guarantees.

In [23], authors address the critical issue of fault detection in cryptographic systems, particularly those that utilize finite field multipliers. While the paper acknowledges both accidental and malicious faults, it does not clearly differentiate between the fault models used for testing or how the proposed architecture performs under targeted fault attacks (e.g., differential fault analysis or glitch attacks). Although fault resilience is the main focus, real-world implementations must also account for side-channel attacks, especially in FPGA environments. The omission of any side-channel resistance assessment weakens the security robustness claim.

In this work [24], authors present an innovative algebraic system called the Generalized Triangular Dynamical System to construct cryptographic permutations over finite fields. This algebraic framework aims to systematically explore and optimize symmetric-key cryptographic functions, particularly over large odd prime fields, which are crucial in multi-party computation and zero-knowledge proofs. By integrating and extending various iterative design strategies like Substitution-Permutation Networks, Feistel networks, and Lai-Massey constructions, their approach provides a versatile tool for developing more efficient cryptographic primitives. While the system is theoretically well-structured, the paper lacks a rigorous, empirical cryptanalytic evaluation of the generated permutations. The study does not provide detailed performance benchmarks (e.g., computational complexity, cycle count, gate area) for implementations of GTDS-based permutations. This omission makes it difficult to assess its real-world viability compared to existing lightweight and high-throughput ciphers.

In the article [25], authors introduce a novel image cryptography algorithm known as the Three-tier Image Encryption Algorithm (TIEA), which is designed to meet the rigorous demands of confidentiality, integrity, and authenticity in image information security. Their approach utilizes finite field theory to apply Shannon's cryptographic principles of confusion and diffusion effectively. The distinctiveness of TIEA lies in its intricate key stream generation pattern, which supports the creation of two subkeys aimed at enhancing the permutation processes associated with the crypto key. Despite invoking Shannon's principles, the paper does not present measurable results such as NPCR (Number of Pixels Change Rate), UACI (Unified Average Changing Intensity), entropy analysis, or correlation coefficients standard metrics used to validate the effectiveness of image encryption.

In summary, although numerous cryptographic schemes have utilized finite automata, ranging from transducer-based models like FAPKC to hybrid schemes such as DAFA and FSAaCIT. Such hybrid schemes several limitations persist. Many previous systems either lack formal reversibility guarantees, have not demonstrated practical implementations for image encryption, or rely heavily on non-composable automaton structures, limiting scalability and security strength. A variant of overcoming the corresponding difficulties can be conducting research using comprehensive empirical evaluation using standardized statistical methods such as NPCR, UACI, PSNR, or the NIST random set. Therefore, a gap remains in designing a modular, symmetric cryptosystem based on reversible, information-preserving automata with validated performance through quantitative experimentation.

3. The aim and objectives of the study

The aim of this study is to identify the efficacy of finite automata in cryptographic systems, with a particular focus on enhancing the security, robustness, and reliability of encryption and decryption processes.

To achieve this aim, the following objectives are accomplished:

– to perform detailed statistical evaluations using measures such as NPCR and UACI;

– to evaluate the algorithm's resistance to noise attacks using the PSNR test with the addition of Salt and Pepper noise intensities of 0.01, 0.05, and 0.1 to encrypted images;

– to investigate of resilience to occlusion attacks;

– to analysis of cryptographic strength via NIST tests.

4. Materials and methods

4. 1. Object and hypothesis of the study

The object of this study is the use of finite automata, specifically CryptoAutomata, in cryptographic systems. This includes various forms such as Mealy automata, surjective finite automata, and information lossless automata, which are collectively referred to in the research as CryptoAutomata. The research focuses on studying their structural and functional properties, in particular reversibility and composability, to improve the reliability, security and efficiency of encryption and decryption processes.

Research hypothesis of this study is the proposed symmetric cryptographic system based on finite automata, specifically using Mealy, surjective, and information lossless automata will demonstrate superior encryption robustness, statistical randomness, and resilience to common cryptographic attacks (differential, noise, occlusion), as evaluated by standard quantitative metrics such as NPCR, UACI, PSNR, and NIST tests, without incurring computational overhead.

In conducting this study, several key assumptions were made to guide the design and evaluation of the proposed cryptographic system. It is proposed that reversible finite automata, in particular Mealy, surjective and lossless types, can serve effectively as cryptographic keys due to their deterministic and invertible structures. The reversibility property ensures that encrypted data can be accurately decrypted without information loss. Furthermore, it is presumed that the composition of multiple finite automata increases the encryption system's complexity and key space, thereby enhancing resistance to cryptanalysis. The method assumes minimal computational overhead, as encryption and decryption are implemented via table lookups instead of arithmetic operations, supporting efficient execution. Standard grayscale images (e.g., Lena, Peppers, Mandrill) are considered representative benchmarks for evaluating system performance and robustness. It is also assumed that established statistical metrics such as NPCR, UACI, PSNR, and the NIST randomness test suite are sufficient for validating the security properties of the encryption system. The study adopts a symmetric encryption model, assuming that the same key can be reliably and securely used for both encryption and decryption within the automata-based framework.

To ensure the feasibility and focus of the proposed cryptographic system, several simplifications were adopted in the study. Image encryption and decryption experiments were conducted exclusively on standardized grayscale images with a resolution of 512 × 512 pixels, simplifying the processing of input data. The encryption process is based entirely on lookup tables derived from automata transitions, avoiding arithmetic computations and thereby reducing computational complexity. Additionally, encryption mechanisms employ sequential composition of reversible automata, assuming that such a structure maintains overall reversibility and avoids the need for designing single, highly complex automata. A fixed bit-delay is introduced during encryption and removed during decryption, providing an added layer of transformation without complicating synchronization. All evaluations rely on a consistent test dataset and standardized statistical metrics (NPCR, UACI, PSNR, and NIST randomness tests), and the cryptosystem is assessed in a controlled offline environment without real-time communication protocols. These simplifications collectively allowed for a focused exploration of the automata-based cryptographic model while maintaining clarity in implementation and analysis.

4. 2. Materials

The software implementation of the cryptosystem is written in the Python programming language. Various combinations of surjective finite automata, Mealy automata, and lossless automata were considered in this research work. For encryption, a composition was used different combinations of considered FA. To obtain experimental data, grey images with a size of 512 × 512 pixels were taken from the database (https://sipi.usc.edu/database): Mandrill, Peppers, Lena, Airplane.

The example is a Lena.tiff image with a size of 512 × 512 pixels. This image contains large areas with the same color. Fig. 1 shows that the encryption and decryption of images were successful.

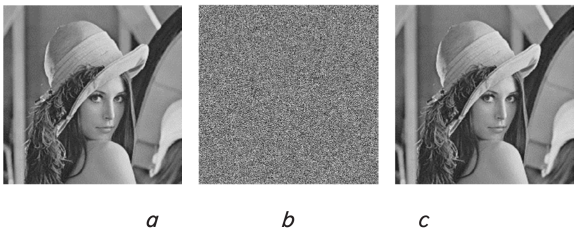

Fig. 1. Converting an image: *a* — original image; *b* — encrypted image; *c* — decrypted image

Fig. 1 illustrates the encryption and decryption process applied to a grayscale image (Lena.tiff) of resolution 512 × 512 pixels. Subfigure (*a*) depicts the original image, characterized by uniform color regions, making it suitable for testing visual data encryption. Subfigure (*b*) shows the encrypted version, which appears as noise-like and visually unrecognizable, indicating strong obfuscation of image features. Subfigure (*c*) presents the successfully decrypted image, which closely matches the original, thereby confirming the effectiveness and reversibility of the proposed cryptographic method.

4. 3. Methods

4. 3. 1. CryptoAutomata

This section is devoted to the considered finite automata with output. Definitions of surjective automata, Mealy automata and information losslessness automata will be given. As is known, the main task of encryption is reversible transformations of open text using keys. In our case, such keys are CryptoAutomata. Therefore, this class of automata must have the property of reversibility, in other words, the ability to restore the original sequence of symbols, knowing the output sequence. Due to this property, it is possible to construct a reverse CryptoAutomaton, which will serve as a decoder. It is worth noting that finite automata can be subjected to a sequential composition operation and a completely new compositional finite automaton can be obtained that hides the original finite automata. The use of FA compositions allows increasing the reliability of finite-automaton cryptosystems by increasing the number of key states.

4. 3. 1. 1. Finite automata with outputs

Formally, a FA with output can be represented as a quintuplet (1), where (2) is a finite alphabet of input symbols; (3) is a finite alphabet of output symbols; (4) is a set of internal states; (5) is the transition function; (6) is the output function:

$$A = \langle Q, X, Y, \delta, \lambda \rangle, \tag{1}$$

$$X = \{x_1, x_2, ..., x_n\}, \tag{2}$$

$$Y = \{y_1, y_2, ..., y_n\}, \tag{3}$$

$$Q = \{q_1, q_2, ..., q_n\}, \tag{4}$$

$$\delta : Q \times X \to Q, \tag{5}$$

$$\lambda : Q \times X \to Y. \tag{6}$$

This formalism is typical for Mealy machines, where the output depends both on the current state and the current input. The model is fundamental in automata theory and finds applications in various areas such as sequential logic design, formal language processing, and control systems.

4. 3. 1. 2. Mealy automata

An automaton is an abstract device that operates in discrete time $t = 1, 2,...$ and so on. It turns out that at each moment of time t the automaton is in a certain state $q_1 \in Q$, receives a signal $x_1 \in X$ at the input, outputs a signal $y_1 \in Y$ according to the formula (7) and goes into a new state $q_{1+1} \in Q$ according to the formula (8):

$$y_t = \lambda(q_t, x_t), \tag{7}$$

$$q_{t+1} = \delta(q_t, x_t). \tag{8}$$

In other words, the FA A (1), receiving the sequence (9) at the input, starting from initial state q_1, goes through the sequence of internal states (10) and as a result of the machine operation, the output sequence (11) is obtained:

$$\alpha = x_1, x_2, \ldots, x_n, \tag{9}$$

$$\gamma = q_1, q_2, \ldots, q_{n+1}, \tag{10}$$

$$\beta = y_1, y_2, \ldots, y_n. \tag{11}$$

Therefore, in the context of the system, the FA can be represented in the following form (12), this FA is the Mealy Automata [26]

$$\begin{cases} q_{t+1} = \delta(q_t, x_t), \\ y_t = \lambda(q_t, x_t). \end{cases} \tag{12}$$

It is convenient to represent such finite automata in tabular form Table 1. The current state (CS) is listed in the rows, the input symbols are shown in the columns, and at the intersection of each row and column, the next state (NS) is indicated, with the output symbol separated by a comma.

Table 1

Finite automata with output

CS	NS, y_n		
	x_1	…	x_n
q_1	$\delta(q_1,x_1)$, $\lambda(q_1,x_1)$	…	$\delta(q_1,x_n)$, $\lambda(q_1,x_n)$
…	…	…	…
q_n	$\delta(q_n,x_1)$, $\lambda(q_n,x_1)$	…	$\delta(q_n,x_n)$, $\lambda(q_n,x_n)$

Table 1 provides a tabular representation of a finite automaton with output, a Mealy machine. The table is structured to illustrate how the automaton transitions between states and generates outputs in response to given input symbols. This matrix form enables a compact and intuitive visualization of the behavior of the automaton for every possible state and input combination. It is particularly useful for simulation, implementation, or analysis of sequential systems in fields such as digital logic design and automata-based modeling.

4. 3. 1. 3. Surjective FA

A finite automaton (1) is called surjective if for any output sequence $y \in Y^*$ there exists an input sequence $x \in X^*$ such that, for the initial state $q_0 \in Q$, the automaton A, when reading the sequence x, produces the output sequence y. It's mean, that for any $y \in Y^*$ there exists $x \in X^*$ such that: (13), where $\lambda^*(q_0, x)$ is the output sequence of the automaton for the initial state q_0 and the input sequence x [27]

$$\lambda^*(q_0, x) = y. \tag{13}$$

In other words, surjective automata are finite automata that satisfy the conditions of surjective function, i. e. it is necessary and sufficient that in each row of the output table each output symbol occurs at least once.

4. 3. 1. 4. Information lossless finite automata

A lossless finite automaton is a type of finite automaton that has the property of reversibility. In such an automaton, for any state and input symbol of the next state, the previous state and input symbol can be uniquely determined. This means that the automaton can be "rewound" without losing information about previous states and input symbols.

A finite automaton is said to be *lossless* (*IL*) if there is no state q_i and no two different input sequences x^n and w^n (for $n \geq 1$) such that (14), (15) [28]:

$$\lambda(q_i, x^n) = \lambda(q_i, w^n), \tag{14}$$

$$\delta(q_i, x^n) = \delta(q_i, w^n). \tag{15}$$

Lossless automata with delay L are reversible automata where information about transitions is stored but can be restored with some delay L, where $L \leq N/2$.

4. 3. 1. 5. Weakly reversible FA

If (16) for (17) of FA (1), it is mean that $\gamma = \gamma'$ consequently this FA is called reversible. That is to say, FA A is reversible if and only if any input sequences $\forall\gamma \in X^*$ can be uniquely retrieved by $\lambda(q,a)$ for $\forall q \in Q$ [29]:

$$\lambda(q, \gamma) = \lambda(q, \gamma'), \tag{16}$$

$$\forall q \in Q, \forall \gamma, \gamma' \in X^*. \tag{17}$$

A FA (1) is called reversible with delay τ, or τ-reversible, where τ – non-negative integer, if (18) the outputs coincide, i. e. (19), then it follows that $x = x'$. In other words, it is possible to say that for $\forall q \in Q$, $x \in X$, and $\forall \alpha \in X^\tau$, the input x can be uniquely determined using the state q and $\lambda(q, x\alpha)$:

$$\forall q \in Q, \forall x, x' \in X, \forall \alpha, \alpha' \in X^\tau, \tag{18}$$

$$\lambda(q, x\alpha) = \lambda(q, x'\alpha'). \tag{19}$$

Theorem 1 [30]: Let (1) be a Finite Automata. A is reversible if and only if G_A (testing graph of A) has no circuit. Moreover, if G_A has no circuit and the level of G_A is $\rho - 1$, then A is reversible with a delay of $\rho+1$ and not invertible with a delay of τ for any $\tau \leq \rho$.

4. 3. 1. 6. Invert of FA

There are two FA (1) and (20), for (21), if for $\forall \alpha \in X^*$, there exists $\alpha_0 \in X^\tau$ such that (22) and (23), then (q^{-1},q) is called a pair with delay τ (a τ-pair) [12]. From this can be concluded that, automaton A^{-1} is called the inverse with delay τ to the automaton A if for $\forall q \in Q$, there exists $q^{-1} \in Q^{-1}$ such that (q^{-1},q) is a τ-pair in A^{-1}×A:

$$A^{-1} = \left\langle Q^{-1}, X, Y, \delta^{-1}, \lambda^{-1} \right\rangle, \tag{20}$$

$$\forall q \in Q, q^{-1} \in Q^{-1}, \tag{21}$$

$$\lambda^{-1}\left(q^{-1}, \lambda(q, \alpha)\right) = \alpha_0 \alpha, \tag{22}$$

$$|\alpha_0| = \tau. \tag{23}$$

These expressions formalize the concept of an inverse automaton with delay, which plays a significant role in reversible computing, error correction, and information retrieval systems. It ensures that the behavior of the original automaton can be reconstructed, within a bounded lag, by an appropriately defined inverse system.

4. 3. 1. 7. FA composition

Let two automata be given A_1 automata (24) and A_2 automata (25), where input for second automata is output of first automata (26). The composition of two automata is then defined as follows: $C(A_1, A_2)$ (27), where automaton permutation functions (28) and (29):

$$A_1 = \langle Q_1, X_1, Y_1, \delta_1, \lambda_1 \rangle, \tag{24}$$

$$A_2 = \langle Q_2, X_2, Y_2, \delta_2, \lambda_2 \rangle, \tag{25}$$

$$X_2 = Y_1, \tag{26}$$

$$C(A_1, A_2) = \langle Q_1 \times Q_2, X_1, Y_2, \delta, \lambda \rangle, \tag{27}$$

$$\delta(< q_1, q_2 >, x) = \langle \delta_1(q_1, x), \delta_2(q_2, \lambda_1(q_1, x)) \rangle, \tag{28}$$

$$\lambda(\langle q_1, q_2 \rangle, x) = \lambda_2(q_2, \lambda_1(q_1, x)),$$

$$x \in X_1, q_1 \in Q_1, q_2 \in Q_2. \tag{29}$$

This process defines how two automata can be combined into a single composite system, allowing for sequential processing of input and intermediate output symbols.

4. 3. 2. Symmetric cryptosystem based of CryptoAutomata

The framework of a symmetric cryptosystem within the context of finite automata will be outlined. Symmetric encryption is an encryption method that uses the same secret key to encrypt/decrypt information. Key generation, encryption, and decryption are main phase of cryptographic process [31].

Formally, a cryptosystem is a quintuplet [27] (30), where K – a finite set of keys, X^* and Y^* – a finite set of public and ciphertexts, respectively. Encryption is a mapping of (31), for $k \in K^*$. Decryption is a mapping of (32) for $k \in K^*$:

$$C = \langle K, X^*, Y^*, E_k, D_k \rangle, \tag{30}$$

$$E_k : x \to y(x \in X^*, y \in Y^*), \tag{31}$$

$$D_k : y \to x(y \in Y^*, x \in X^*). \tag{32}$$

In addition, the following properties must be met:

- the mapping must be injective, i. e. (33);
- (34), where the union is taken over all (35):

$$\forall x \in X^*, \forall k \in K^* : D_k(E_k(x)) = x, \tag{33}$$

$$Y^* = \cup E_k(x), \tag{34}$$

$$k \in K, x \in X^*. \tag{35}$$

In our case, the keys are reversible finite automata. The key generation process is described below.

4. 3. 2. 1. Generation of surjective FA

According to their definition, surjective FA have the property of reversibility without delay.

The method of their construction is based on simple conditions, which allows for the rapid generation of even large FA. Additionally, due to its structure, the finite automaton exhibits randomness, which over time enhances the quality of encryption:

1) generate a set *NS* for each element (*NS*, *y*) taking into account that the object, being in state *Q*, does not move to the same state *Q*;

2) generate a set y for elements (*NS*, *y*) such that both 0 and 1 can exit from state *Q*.

That is, it is possible to exclude the case when an object in state *Q*, both at $x = 1$ and at $x = 0$, returns the same element *y* – only 1 or only 0.

An automaton with the elements listed in Table 2, which meet the specified conditions, is surjective and can be employed in a composition for subsequent encryption.

Table 2

Finite automata with output

CS	NS, y_n	
	$x = 0$	$x = 1$
0	1.0	2.1
1	3.1	0.0
2	0.1	2.0
3	1.1	3.0

The algorithm for constructing an inverse automaton A^{-1} to a surjective one is quite simple: (36), (37), where x is an arbitrary element from the set $\lambda^{-1}(q, y)$, which, due to surjectivity, is not empty:

$$\lambda^{-1}(q, y) = x, \tag{36}$$

$$\delta^{-1}(q, y) = \delta(q, x). \tag{37}$$

An example of an inverse automaton to the automaton presented in Table 2 is shown in Table 3.

Table 3

Finite automata with output

CS	NS, y_n	
	$x = 0$	$x = 1$
0	1.0	2.1
1	0.1	3.0
2	2.1	0.0
3	3.1	1.0

Table 3 exemplifies a well-structured inverse FA derived from a surjective automaton, maintaining reversibility, deterministic behavior, and enhanced randomness, all critical features for secure computational models, especially in cryptographic contexts.

4. 3. 2. 2. Generation of a reversible Mealy automata

As is known, not all Mealy automata can have the property of reversibility. In order to check the generated machine for reversibility, it is necessary to apply the algorithm "Reversibility test" described in [4, 32].

The essence of this test is as follows:

1) an automaton is constructed in tabular form, with a given number of states;

2) a testing table is constructed, consisting of 2 parts. The description of the construction of the testing table is given in [4];

3) a testing directed weighted graph *G* is constructed using the testing table from step 2;

4) the graph *G* from step 3 is checked for the presence of a cycle. If there is a cycle, then the FA is not a reversible au-

tomaton with finite memory; if there is no cycle, then the FA is a reversible automaton with finite memory;

5) find the delay $\mu = l + 2$, where l is the longest path of graph G.

The resulting reversible Mealy automaton is preserved and can be used as a component of a composite FA. The inverse automaton is constructed using the Kohavi algorithm [4].

4. 3. 2. 3. Generating information lossless FA

Lossless automata of order $L = N/2$ are generated according to the algorithm presented by Olson [28]:

$$\delta(q_i,0) = q_{i+2} \quad \lambda(q_i,0) = 1, \tag{38}$$

$$\delta(q_{i+1},0) = q_{i+2} \quad \lambda(q_i,0) = 0, \tag{39}$$

$$\delta(q_i,1) = q_{i+3} \quad \lambda(q_i,1) = 0, \tag{40}$$

$$\delta(q_{i+1},1) = q_{i+2} \quad \lambda(q_i,1) = 1, \tag{41}$$

for $i = 1 \ldots N$.

In the case when $i = N - 1$, then the output and input functions are calculated as follows:

$$\delta(q_{N-1},0) = q_1 \quad \lambda(q_{N-1},0) = 1, \tag{42}$$

$$\delta(q_{N-1},1) = q_2 \quad \lambda(q_{N-1},1) = 0, \tag{43}$$

If $i = N$, then:

$$\delta(q_N,0) = q_1 \quad \lambda(q_N,0) = 0, \tag{44}$$

$$\delta(q_N,1) = q_2 \quad \lambda(q_N,1) = 1. \tag{45}$$

The value $N = 2L$, where L is set arbitrarily by the user.

Next, let's obtain a general representation of the automaton without loss of information according to Olson according Table 4.

Table 4

Information lossless FA

CS	NS, *y*	
	0	1
q_1	q_3,1	q_4,1
q_2	q_3,0	q_4,0
q_3	q_5,1	q_6,0
q_4	q_5,0	q_6,1
…	…	…
q_i	q_{i+2},1	q_{i+3},0
q_{i+1}	q_{i+2},0	q_{i+3},1
…	…	…
$q_{n\text{-}1}$	q_1,1	q_2,0
q_n	q_1,0	q_2,1

The inverse automaton had been constructed using Olson's algorithm [28].

4. 3. 2. 4. Construction of the composition of the FA

The main point of the composition of finite automata is that it allows connect two or more finite automata, representing another, separate automaton. The peculiarity of this automaton is that the passage of an object through this automaton is comparable to the same as if the object passed sequentially through those automata from which the composition is built. An example of constructing a composition will be shown.

Two reversible finite automata are constructed in tabular form. The following FA were selected for this purpose and presented in Tables 5, 6.

Table 5

Finite Automata A_1

CS	NS, *y*	
	$x = 0$	$x = 1$
0	1.0	0.0
1	0.1	1.1

Table 6

Finite Automata A_2

CS	NS, *y*	
	$x = 0$	$x = 1$
0	0.1	1.1
1	1.0	0.0

According to the algorithm for constructing the composition of FA described above, let's obtain $C(A_1, A_2)$, shown in Table 7.

Table 7

FA $C(A_1, A_2)$ composition

CS	NS, *y*	
	$x = 0$	$x = 1$
0	2.1	0.1
1	3.0	1.0
2	1.1	3.1
3	0.0	2.0

Table 7 exemplifies a systematic approach to automata composition, serving as a foundation for the design of higher-order automata-based systems.

4. 3. 2. 5. The process of encryption and decryption

A key advantage of a cryptosystem based on finite automata is that encryption and decryption can be implemented without the need for calculations. In the process of data encryption, the computer only needs to go through certain indices of the FA table.

As a result, to implement the encryption or decryption function, the following main parameters are fed to the input:

– the data to be encrypted or decrypted (denoted as a bit stream. Example: 110101100101);

– finite automata table (types of finite automata are selected arbitrarily to construct a composite finite automata);

– delay of finite automata;

– initial states for data encryption.

And a bit stream representing the encrypted bit sequence is obtained at the output.

The pseudocode for the data encryption algorithm using a finite automaton is presented below (Algorithm 1):

```
Algorithm 1. Data Encryption

Input:
P – plaintext
```

```
$L_d$ – number of delay
$S_0$ – initial state
$M(A_0,A_1,..A_m)$ – set of invertible automata represented as matrix Nx4 (N-number of state)
m – number of automata
Output:
C – ciphertext
Start
1. Select number of FA m that will participate in encryption
2. Choose m FA from set M
3. Calculate number of delay $L_d = L_0+L_1+...+L_m$
3. Construct composition $C(A_0,A_1,..A_m)$
4. Randomly generate w bits with length $= L_d$
5. Add w end to P ($P_w = P+w$)
6. Encrypt $P_w$ by $C(A_0,A_1,..A_m)$ with initial state $S_0$
Return ciphertext $C_w$
End
```

The decryption algorithm is not very different from the encryption. The sole distinction lies in the delay stage. In the encryption algorithm, the delay introduces additional bits at the end of the data before encryption, whereas during decryption, these extra bits are removed after the data has been decrypted.

Data decryption algorithm based on CrypoAutomata using pseudocode had been described in Algorithm 2. As is seen, the input parameters are the same as in the encryption algorithm:

Algorithm 2. Data decryption

```
Input:
 $C_w$ - ciphertext
$L_d$ – number of delay
$S_0$ – initial state
$C(A_0,A_1,..A_m)$ – composition of FA
Output:
P – plaintext
 Start
1. Construct invert of $C(A_0,A_1,..A_m)$
2. Decrypt $C_w$ by invert of $C(A_0,A_1,..A_m)$ with initial state $S_0$
3. Cut from decrypted $P_w$ w bits
Return plaintext P;
End
```

Algorithm 2 leverages the principles of finite automata to systematically decrypt data by utilizing pre-defined state transitions. This decryption process is essentially an inversion of the corresponding encryption method, aiming to retrieve the original data from its encrypted form efficiently. The algorithm's emphasis on removing delay bits during the decryption phase ensures that the output precisely mirrors the pre-encrypted input, highlighting the deterministic nature of finite automata in cryptographic applications.

5. Results of the development of the CryptoAutomata

5. 1. Differential attack resistance analysis using NPCR and UACI metrics

The statistical measures known as NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity) are utilized to assess the robustness of image encryption techniques against various forms of attacks [33]. Differential attacks exploit the sensitivity of encryption methods to minor alterations in the input image. A substantial visual difference between the original and encrypted images enhances the difficulty for an attacker to distinguish between them. These metrics can be calculated as follows:

$$\text{NPCR} = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{i=1}^{H} D\left(C1_{i,j}, C2_{i,j}\right), \tag{46}$$

$$\text{UACI} = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} \left| C1_{i,j} - C2_{i,j} \right|, \tag{47}$$

$C1$ and $C2$ are two encrypted images, W and H are image's size. $D\left(C1_{i,j}, C2_{i,j}\right)$ can be expanded as

$$D\left(C1_{i,j}, C2_{i,j}\right) = \begin{cases} 0, \text{if } C1_{i,j} = C2_{i,j}, \\ 1, \text{if } C1_{i,j} \neq C2_{i,j}. \end{cases} \tag{48}$$

Table 8 presents the NPCR and UACI values for the input images, demonstrating the proposed method's values between the proposed method and existing approaches.

Table 8

This analysis compares the NPCR and UACI values of this algorithm with other algorithms to assess its resistance to differential attacks

Image	Algorithms	NPCR	UACI
Lena	Proposed method	99.6117	33.4843
	Ref [34]	99.6091	33.4598
	Ref [35]	99.597	28.07
	Ref [36]	99.5893	33.5541
Mandrill	Proposed method	99.6151	33.5042
	Ref [34]	99.6161	33.4693
	Ref [35]	99.688	29.284
	Ref [36]	99.5893	33.5541
Peppers	Proposed method	99.5960	33.4882
	Ref [34]	99.6063	33.4626
	Ref [35]	99.489	31.934
	Ref [36]	99.5893	33.5541
Airline	Proposed method	99.5590	33.2348
	Ref [34]	99.5987	33.4582
	Ref [35]	99.596	19.904
	Ref [36]	99.5893	33.5541

This Table 8 compares the proposed encryption method with three other referenced methods [34–36] across four different images: Lena, Mandrill, Peppers, and Airline. For Lena the proposed method shows an NPCR of 99.6117 and a UACI of 33.4843, indicating strong resistance to pixel change attacks. [35] shows a notably lower UACI of 28.07, suggesting lesser resistance compared to the proposed method and other references. For Mandrill the proposed method and [34] show very similar NPCR values, with [34] slightly higher, implying very subtle differences in performance. [35] records the highest NPCR of 99.688 but a lower UACI of 29.284, indicating high sensitivity to pixel changes but less average intensity variation. For Peppers the proposed method has an NPCR slightly below that of [34], which suggests a marginally lesser sensitivity to differential changes. [35] shows significantly lower values for both NPCR and UACI, indicating the weakest resistance among the tested algorithms for this image. For Airline the proposed method shows the lowest NPCR and UACI for this image set, suggesting a need for further optimization to enhance its resistance to differential attacks. [36] again shows a notably low UACI of 19.904, significantly lower than other algorithms, underscoring its lower performance in modifying pixel intensity on average. This analytical summary highlights the relative performance of each algorithm in resisting differential cryptographic attacks, providing essential insights into their efficacy. Such comparisons are crucial for understanding algorithmic strengths and weaknesses, guiding further development and refinement in cryptographic techniques. This comparative analysis is crucial for understanding the relative performance of different encryption algorithms in resisting differential attacks, providing insights into their effectiveness in real-world applications where security and data integrity are critical.

5. 2. Robustness evaluation under Salt-and-Pepper noise attack

A noise attack is a common type of adversarial strategy employed to assess the robustness of image encryption algorithms. In a noise attack, random noise is intentionally introduced into the encrypted image, for example salt and pepper noise. In our experiment, different densities noise attacks are shown. The intensity of 0.01, 0.05 and 0.1 of Salt and Pepper Noise are added to the encrypted images. Table 9 presents the PSNR values for the decrypted images. The results of this test indicate that the PSNR value exceeds 30 dB when subjected to Salt and Pepper Noise. The formula PSNR defined following

$$\mathrm{PSNR} = 10\lg \frac{255\times 255}{\left(1/W\times H\right)\sum_{i=1}^{W}\sum_{j=1}^{H}\left(P(i,j)-P'(i,j)\right)^2}, \tag{49}$$

where $P(i, j)$ – the pixel of the original image in position i and j, $P'(i, j)$ – the pixel of the distorted or restored image in position i and j. Fig. 2 shows the experimental results of Lena's plain image and decrypted image with Salt and Pepper noise.

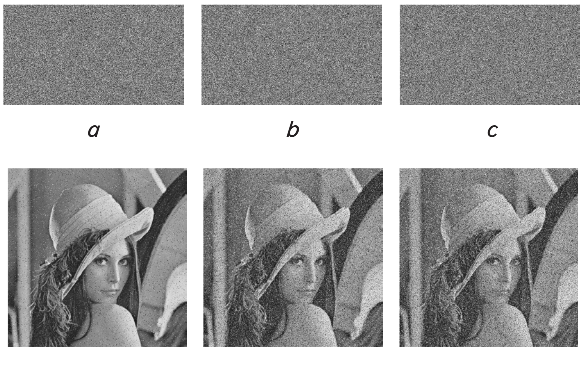

Fig. 2. Robustness against noise attack: *a* – encrypted image with 0.01 salt and pepper noise; *b* – encrypted image with 0.05 salt and pepper noise; *c* – encrypted image with 0.1 salt and pepper noise; *d* – decrypted image with 0.01 salt and pepper noise; *e* – decrypted image with 0.05 salt and pepper noise; *f* – decrypted image with 0.1 salt and pepper noise

Table 9 presents the results of an experimental evaluation designed to assess the robustness of an image encryption and decryption system against noise attacks, specifically Salt and Pepper Noise. In this type of attack, random black-and-white pixels are introduced into the encrypted image to simulate adversarial perturbations. The primary objective of the experiment is to determine how well the decryption process can recover the original image when subjected to varying levels of noise.

Table 9

Show the PSNR values when salt and pepper noise are added to the decrypted image

Image	0.01	0.05	0.1
Lena	44.8438	36.5759	35.0634

5. 3. Occlusion attack resilience assessment through block-wise data loss simulation

Fig. 3 shows decrypted images after lost data. An Occlusion Attack in image processing typically involves deliberately obscuring parts of an image to test or manipulate the behavior of image processing algorithms, particularly those used in security or data recovery. When applying this to decrypted images that have lost data, the aim could be to evaluate how robust decryption algorithms are to data loss, or to simulate how such images might be reconstructed or recovered.

Fig. 3 illustrates the effects of data loss in encrypted images upon decryption, categorized by varying block sizes. The images are decrypted versions of an original image that has been subjected to simulated data loss in blocks of sizes 8 × 8, 16 × 16, and 32 × 32 pixels. Top Row (*a*, *b*, *c*) represents complete image data loss with noise-like patterns, indicating total corruption or the absence of recoverable data. Second row of *a* shows the decrypted results from data loss at 8 × 8 pixel blocks.

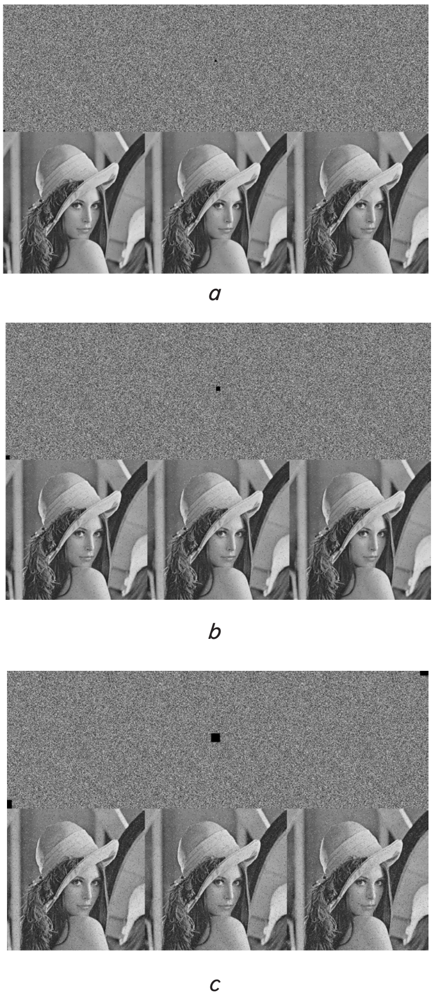

Fig. 3. Illustration of decrypted images after lost data: *a* – with blocks 8 × 8; *b* – with blocks 16 × 16; *c* – with blocks 32 × 32

Each image progressively displays the increasing impact of occlusion. While a1 has minimal visible occlusion, b1 and c1 display single pixel occlusions in different locations, highlighting the precise impact of data loss on decryption. First row of *b* similar to the top row, it shows complete image data loss at a noise level but with larger block sizes (16 × 16). Second row of *b* depicts 16 × 16 pixel block occlusions upon decryption. Compared to the 8x8 blocks, these occlusions are more prominent, demonstrating a more significant degradation in the image quality and decipherability. First row of *c* displays further scaled up noise patterns representing total data loss for the largest block size (32 × 32). Second row of *c* showcases the decrypted images with 32 × 32 pixel blocks of occlusion. The depicted results clearly demonstrate the scale of impact depending on the size of the data loss blocks. As the block size increases, the occlusion becomes more disruptive, thus affecting the image's usability and visual integrity post-decryption. This experiment can be critical for understanding and improving cryptographic resilience against data corruption or targeted data removal attacks.

5. 4. NIST test results

The NIST statistical tests were developed by the Information Technology Laboratory, a part of the National Institute of Standards and Technology. The suite consists of 15 different tests that evaluate the randomness of binary sequences. Based on various statistical properties of random sequences, passing which, positive results of these tests indicate good cryptographic resistance [37]. In other terms, NIST statistical tests are adept at evaluating the randomness of encrypted data, which is a primary sign of robust encryption.

Table 10 contains the results of NIST statistical tests on the experimental image named Lena.

Table 10

NIST results

Test name		P-Value	Conclusion
1. Frequency test		0.0459339227971131	True
2. Block frequency test		0.2906437702767687	True
3. Run test		0.3290546165467799	True
4. Run test (longest run of ones)		0.413555884378768	True
5. Binary matrix rank test		0.6923433155597949	True
6. Discrete Fourier transform (spectral) test		0.9414774452839101	True
7. Non-overlapping template matching test		0.0153780652805539	True
8. Overlapping template matching test		0.7651577376589505	True
9. Universal statistical test		0.5766279701371697	True
10. Linear complexity test		0.0493598386854056	True
11. Serial test		0.7462922803679235	True
12. Approximate entropy test		0.505780758515081	True
13. Cumulative sums (forward)		0.0553307724029172	True
13. Cumulative sums (backward)		0.0553307724029172	True
14. Random excursion test			
STATE	xObs	P-Value	Conclusion
–4	7.718450645564349	0.1724502217745767	True
–3	7.523284210526316	0.1845393715420106	True
–2	5.124756335282651	0.4008454081449354	True
–1	3.1578947368421053	0.6756579921494642	True
1	3.5263157894736845	0.6194095092280941	True
2	5.63417803768681	0.3434569605505082	True
3	5.22117894736842	0.3894879881686620	True
4	3.883864179398935	0.5662550544355305	True
15. Random excursion variant test			
STATE	COUNTS	P–Value	Conclusion
–9.0	211	0.0079131790048760	False
–8.0	155	0.0980314574802094	True
–7.0	136	0.1770917561891871	True
–6.0	125	0.2307869488479882	True
–5.0	120	0.2341943048792145	True
–4.0	113	0.2566654676647206	True
–3.0	108	0.2457387003398492	True
–2.0	106	0.1600573462319449	True
–1.0	90	0.2561449666035268	True
+1.0	76	1.0	True
+2.0	95	0.3735966374564359	True
+3.0	94	0.513802293806963	True
+4.0	80	0.9024017855981159	True
+5.0	86	0.7868763596160389	True
+6.0	81	0.9026780651217505	True
+7.0	65	0.8045547988441902	True
+8.0	62	0.7693710146499217	True
+9.0	79	0.952938798134652	True

The results of all tests confirm that the encrypted image has a high degree of randomness and meets the cryptographic strength criteria.

6. Discussion on the security, robustness, and randomness performance of the proposed CryptoAutomata encryption system

The presented CryptoAutomata encryption method was evaluated through rigorous experimentation, focusing on its resistance to differential attacks, robustness against noise perturbations, occlusion attack resilience, and compliance with statistical randomness standards. The differential attack resistance, measured by NPCR and UACI demonstrated high resilience. As shown in Table 8, NPCR values ranged between 99.5590% and 99.6151% across different test images, indicating exceptional sensitivity to input variations. The UACI values ranged from 33.2348 to 33.5042, affirming strong intensity variation responses. Compared with existing algorithms, the proposed method showed competitive results, particularly outperforming reference [35] significantly in UACI metrics, indicating enhanced cryptographic security against differential cryptanalysis.

Robustness evaluation under Salt-and-Pepper noise further highlighted the encryption method's reliability. As shown in Table 9, PSNR values recorded were 44.8438 dB, 36.5759 dB, and 35.0634 dB for noise intensities of 0.01, 0.05, and 0.1 respectively. All results remained above the acceptable threshold of 30 dB, confirming that the decryption process effectively recovers the original image, maintaining a high level of fidelity even under significant noise interference. Occlusion resilience testing via simulated block-wise data loss demonstrated the method's vulnerability to larger occlusion blocks. As shown in Fig. 3, minimal degradation was observed at smaller occlusions (8 × 8 blocks), but a noticeable deterioration in image quality and decipherability appeared with larger occlusion blocks (16 × 16 and 32 × 32 pixels). This outcome underscores the need for further optimization of the method to handle extensive data loss effectively.

The comprehensive randomness assessment using the NIST test suite provided strong evidence of cryptographic strength. As shown in Table 10, proposed method passed all fundamental statistical randomness tests, affirming that encrypted outputs possess sufficient randomness and unpredictability, essential attributes for secure encryption.

Overall, the results validate the CryptoAutomata method as a robust encryption solution, emphasizing its suitability for secure image transmission and storage, while also highlighting areas for improvement, specifically in enhancing resilience to substantial data loss scenarios.

While the proposed CryptoAutomata-based encryption method demonstrates high levels of statistical robustness, noise resistance, and differential attack resilience, several limitations were identified during the evaluation process that provide clear guidance for future research directions. Performance inconsistencies were observed across different test images. For example, the image "Airline" yielded the lowest NPCR and UACI values among the dataset, suggesting that the algorithm's effectiveness may depend on specific image characteristics. Such variability limits the general applicability of the method without further adaptation.

To address limitations, several future research directions are proposed. First, enhancing the algorithm's robustness against occlusion attacks through the integration of redundancy mechanisms or error correction codes could improve its resilience in adverse conditions. Second, implementing adaptive parameter tuning based on the structural properties of input images may standardize encryption quality across diverse visual datasets. Transitioning from a simulation-based evaluation to real-time and hardware-oriented testing on platforms such as FPGA or microcontrollers would provide insights into the algorithm's practical feasibility, power efficiency, and scalability for embedded and IoT systems.

7. Conclusions

1. The proposed CryptoAutomata encryption algorithm demonstrated high resistance to differential attacks, as confirmed by NPCR and UACI metrics. The NPCR values consistently exceeded 99.55% across tested images, indicating strong sensitivity to pixel alterations, essential for robust encryption. The UACI metrics, generally above 33%, further confirmed the algorithm's effectiveness in producing significant average intensity variation, thus enhancing resistance to differential cryptanalysis. However, variability in NPCR and UACI across different images, notably the relatively lower performance observed for the "Airline" image, suggests further optimization is needed to achieve uniformly robust security performance.

2. The evaluation of robustness against Salt-and-Pepper noise attacks revealed that the CryptoAutomata algorithm maintained strong image recovery capabilities. With PSNR values consistently exceeding the 30 dB threshold, including notable performances at 44.84 dB, 36.58 dB, and 35.06 dB for respective noise densities of 0.01, 0.05, and 0.1, the method exhibited significant resilience. These findings underscore the practical applicability of the proposed algorithm in noisy transmission environments, affirming its reliability in maintaining decrypted image integrity despite external perturbations.

3. The assessment of resilience against occlusion attacks through block-wise data loss simulations demonstrated clear limitations in the proposed method's performance. While minimal degradation was observed for small occlusion blocks (8 × 8 pixels), the visual quality and decipherability significantly deteriorated with larger block sizes (16 × 16 and 32 × 32 pixels). This vulnerability indicates an essential direction for future development, emphasizing the need for the integration of advanced error-correcting or redundancy strategies to enhance algorithm robustness against extensive data corruption.

4. The proposed encryption method exhibited strong cryptographic strength according to NIST statistical randomness tests. Successfully passing 14 out of 15 rigorous statistical tests confirmed the high randomness and unpredictability of the encrypted data, critical for secure encryption. Nevertheless, the failure of the Random Excursion Variant Test specifically at state –9.0 highlights a potential area for improvement. Achieving full compliance with all NIST test criteria would reinforce the algorithm's credibility and suitability for stringent cryptographic applications, ensuring comprehensive randomness and security.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

This work was supported by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan under Grant No. AP19677422.

Data availability

Manuscript has no associated data.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the current work.

References

1. Al Busafi, S., Kumar, B. (2020). Review and Analysis of Cryptography Techniques. 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), 323–327. https://doi.org/10.1109/smart50582.2020.9336792
2. Salami, Y., Khajevand, V., Zeinali, E. (2023). Cryptographic algorithms: a review of the literature, weaknesses and open challenges. Journal of Computer & Robotics, 16 (2). https://doi.org/10.22094/JCR.2023.1983496.1298
3. Sharipbay, A., Saukhanova, Z., Shakhmetova, G., Barlybayev, A. (2023). Development of Reliable and Effective Methods of Cryptographic Protection of Information Based on the Finite Automata Theory. The Eurasia Proceedings of Science Technology Engineering and Mathematics, 26, 19–25. https://doi.org/10.55549/epstem.1409285
4. Kohavi, Z., Jha, N. K. (2009). Switching and Finite Automata Theory. Cambridge University Press. https://doi.org/10.1017/cbo9780511816239
5. Lotfi, Z., Khalifi, H., Ouardi, F. (2023). Efficient Algebraic Method for Testing the Invertibility of Finite State Machines. Computation, 11 (7), 125. https://doi.org/10.3390/computation11070125
6. Tao, R., Chen, Sh. (1985). A finite automaton public key cryptosystem and digital signatures. Chinese Journal of Computers, 8 (6), 401–409.
7. Abubaker, S., Wu, K. (2013). DAFA - A Lightweight DES Augmented Finite Automaton Cryptosystem. Security and Privacy in Communication Networks, 1–18. https://doi.org/10.1007/978-3-642-36883-7_1
8. Kodada, B. (2022). FSAaCIT: Finite State Automata based One-Key Cryptosystem and Chunk-based Indexing Technique for Secure Data De-duplication in Cloud Computing. https://doi.org/10.36227/techrxiv.20443653.v1
9. Salas Pena, P. I., Ernesto Gonzalez Torres, R. (2016). Authenticated Encryption based on finite automata cryptosystems. 2016 13th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE), 1–6. https://doi.org/10.1109/iceee.2016.7751254
10. Gysin, M. (1996). A one-key cryptosystem based on a finite nonlinear automaton. Cryptography: Policy and Algorithms, 165–173. https://doi.org/10.1007/bfb0032356
11. Lakshmi, S. (2012). On finite state machines and recursive functions – applications to cryptosystems. Jawaharlal Nehru Technological University.
12. Meskanen, T. (2001). On finite automaton public key cryptosystems. TUCS Technical Report.
13. Tao, R., Chen, S., Chen, X. (1997). FAPKC3: A new finite automaton public key cryptosystem. Journal of Computer Science and Technology, 12 (4), 289–305. https://doi.org/10.1007/bf02943149
14. Tao, R., Chen, S. (1999). The generalization of public key cryptosystem FAPKC4. Chinese Science Bulletin, 44 (9), 784–790. https://doi.org/10.1007/bf02885019
15. Kodada, B. B., D'Mello, D. A. (2021). Symmetric Key Cryptosystem based on Sequential State Machine. IOP Conference Series: Materials Science and Engineering, 1187 (1), 012026. https://doi.org/10.1088/1757-899x/1187/1/012026
16. Shakhmetova, G., Barlybayev, A., Saukhanova, Z., Sharipbay, A., Raykul, S., Khassenov, A. (2024). Enhancing Visual Data Security: A Novel FSM-Based Image Encryption and Decryption Methodology. Applied Sciences, 14 (11), 4341. https://doi.org/10.3390/app14114341
17. Zhang, M., Dong, S., Kong, H., Liu, X., Guan, H. (2016). Modeling and Simulation Strategies of Cryptographic Protocols Based on Finite State Machine. Information Technology and Intelligent Transportation Systems, 541–551. https://doi.org/10.1007/978-3-319-38789-5_62
18. Attari, S., Shahmirzadi, A. R., Salmasizadeh, M., Gholampour, I. (2017). Finite State Machine Based Countermeasure for Cryptographic Algorithms. 2017 14th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), 58–63. https://doi.org/10.1109/iscisc.2017.8488336
19. Papanastasiou, P., Ottaviani, C., Pirandola, S. (2017). Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables. Physical Review A, 96 (4). https://doi.org/10.1103/physreva.96.042332
20. de la Cruz Jiménez, R. A. (2019). Generation of 8-Bit S-Boxes Having Almost Optimal Cryptographic Properties Using Smaller 4-Bit S-Boxes and Finite Field Multiplication. Progress in Cryptology – LATINCRYPT 2017, 191–206. https://doi.org/10.1007/978-3-030-25283-0_11
21. Waseem, H. M., Khan, M. (2018). Information Confidentiality Using Quantum Spinning, Rotation and Finite State Machine. International Journal of Theoretical Physics, 57 (11), 3584–3594. https://doi.org/10.1007/s10773-018-3872-6

22. Agrawal, S., Ishai, Y., Kushilevitz, E., Narayanan, V., Prabhakaran, M., Prabhakaran, V., Rosen, A. (2020). Cryptography from One-Way Communication: On Completeness of Finite Channels. Advances in Cryptology – ASIACRYPT 2020, 653–685. https://doi.org/10.1007/978-3-030-64840-4_22
23. Cintas-Canto, A., Kermani, M. M., Azarderakhsh, R. (2023). Reliable Architectures for Finite Field Multipliers Using Cyclic Codes on FPGA Utilized in Classic and Post-Quantum Cryptography. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 31 (1), 157–161. https://doi.org/10.1109/tvlsi.2022.3224357
24. Roy, A., Steiner, M. J. (2025). Generalized Triangular Dynamical System: An Algebraic System for Constructing Cryptographic Permutations over Finite Fields. Selected Areas in Cryptography – SAC 2024, 139–165. https://doi.org/10.1007/978-3-031-82841-6_6
25. Lavanya, M., Sundar, K., Saravanan, S. (2025). Finite Field-Based Three-Tier Cryptography Algorithm to Secure the Images. Defence Science Journal, 75 (1).
26. Sharipbay, A. (2016). Automata models in cryptography. KazNU Bulletin. Mathematics, Mechanics, Computer Science Series, 3 (1 (90)), 94–104.
27. Bogachenko, N. (2007). Application of automata-theoretic models in cryptography. Mathematical Structures and Modeling, 1 (17), 112–120.
28. Olson, R. (1970). On the invertibility of finite state machines. No. TR-EE-703.
29. Tao, R. (2009). Finite Automata and Application to Cryptography. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-78257-5
30. Shakhmetova, G., Saukhanova, Z., Udzir, N. I., Sharipbay, A., Saukhanov, N. (2021). Application of Pseudo-Memory Finite Automata for Information Encryption. Proceedings of the 2nd International Workshop on Intelligent Information Technologies & Systems of Information Security with CEUR-WS.
31. Noura, H. N., Chehab, A., Couturier, R. (2020). Overview of Efficient Symmetric Cryptography: Dynamic vs Static Approaches. 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 1–6. https://doi.org/10.1109/isdfs49300.2020.9116441
32. Shakhmetova, G., Saukhanova, Z., Sharipbay, A., Ulyukova G. (2020). Using Reversible Finite-State Machines In Asymmetrical Cryptosystems. Journal of Almaty University Of Power Engineering And Communications, 1, 118.
33. Abed, Q. K., Al-Jawher, W. A. M. (2024). Enhanced Hyperchaotic Image Encryption with CAW Transform and Sea-Lion Optimizer. Journal of Cyber Security and Mobility, 13 (5), 1207–1238. https://doi.org/10.13052/jcsm2245-1439.13517
34. Setiadi, D. R. I. M., Rijati, N. (2023). An Image Encryption Scheme Combining 2D Cascaded Logistic Map and Permutation-Substitution Operations. Computation, 11 (9), 178. https://doi.org/10.3390/computation11090178
35. Abusham, E., Ibrahim, B., Zia, K., Rehman, M. (2023). Facial Image Encryption for Secure Face Recognition System. Electronics, 12 (3), 774. https://doi.org/10.3390/electronics12030774
36. Khan, S., Peng, H. (2024). A secure and adaptive block-based image encryption: a novel high-speed approach. Nonlinear Dynamics, 112 (18), 16445–16473. https://doi.org/10.1007/s11071-024-09870-8
37. Pareschi, F., Rovatti, R., Setti, G. (2012). On Statistical Tests for Randomness Included in the NIST SP800-22 Test Suite and Based on the Binomial Distribution. IEEE Transactions on Information Forensics and Security, 7 (2), 491–505. https://doi.org/10.1109/tifs.2012.2185227