Journal of Engineering and Technology for Industrial Applications

ITEGAM-JETIA

Manaus, v.12 n.58, p.686-695. March/April, 2026.
DOI: https://doi.org/10.5935/jetia.v12i58.2908

ISSN ONLINE: 2447-0228

RESEARCH ARTICLE OPEN ACCESS

ENHANCING PLAYFAIR CIPHER SECURITY USING CHAOTIC MAPS: A COMPARATIVE ANALYSIS OF LOGISTIC, HÉNON, AND ARNOLD CAT MAPS

Radhika Patel[1], Isha Patel[2], Mahek Vira[3], Stevina Dias[4]

[1,2,3,4]Dwarkadas J Sanghvi College of Engineering, Mumbai, India.

[1]https://orcid.org/0009-0003-0304-7285, [2]https://orcid.org/0009-0009-4586-7373,
[3]https://orcid.org/0009-0004-9873-3807, [4]https://orcid.org/0000-0001-6915-9712

Email:*radhappatel2004@gmail.com, ishap572@gmail.com, mahekvira@gmail.com, Stevina.Dias@djsce.ac.in

ARTICLE INFO

Article History
Received: November 8, 2025
Reviewed: December 19, 2025
Accepted: March 10, 2026
Published: April 30, 2026

Keywords:
Encryption,
Playfair Cipher,
Chaos Theory,
Chaotic Maps,
Cryptographic Security

ABSTRACT

Today, classical encryption systems such as the Playfair cipher are easily broken in the current computing environment. Traditional ciphers based on digraph interactions cannot resist attacks using frequency analysis and pattern recognition, making them unsuitable for modern security. This work presents an improved Playfair cipher by integrating three chaotic maps—Logistic, Hénon, and Arnold Cat—to generate encryption keys dynamically and distort ciphertext. This integration creates a hybrid system that is highly secure yet computationally efficient. Experimental results using Shannon entropy and Lyapunov exponent metrics show clear performance advantages. The Hénon Map proves superior in randomness, achieving a Shannon entropy of 4.11257. The Arnold Cat Map, with a Lyapunov exponent of 0.89813, demonstrates strong sensitivity to initial conditions, preventing brute-force attacks. The Logistic Map provides a balanced compromise (entropy: 3.97695, Lyapunov: 0.63663) between security and resource efficiency. This approach augments the traditional Playfair cipher into a robust modern security solution, showing how classical cryptographic techniques combined with chaos theory can effectively meet contemporary digital security demands.

I. INTRODUCTION

Classical cryptography can be divided into two types: transposition ciphers and substitution ciphers. The transposition cipher is that the letters remain unchanged, but the position changes. The substitution cipher is to replace the letters in the plain text with other letters. Playfair cipher is a typical classical cipher, which is a symmetric substitution encryption cipher. Playfair cipher was invented in 1854 by British scientist Charles Wheatstone Playfair. For a long period, the Playfair algorithm was considered an unbreakable encryption method. its encryption ideas are widely used in terms of network security, data encryption. The Playfair cipher is an encryption algorithm that uses two-letter syllables in plaintext as a unit and converts them into ciphertext. The original algorithm can use 26×26 letter pairs, although it has a slightly flatter frequency distribution curve than plaintext.

The ciphertext still reveals a large amount of information to the cryptanalyst [1]. What makes chaos-based cryptography such a promising field is that chaotic systems are deterministic, vulnerable to change, and without large computational costs. As such chaotic systems set up an exceptional base for implementing various encryption schemes. Therefore, a key characteristic in this field is the introduction of new chaotic maps, such as discrete maps of low dimensions that showcase regions of constant chaotic behavior [2]. Chaotic maps are primarily used as a source of entropy .The popularity of chaos-based cryptography in recent years stems from the fact that chaos can fulfill cryptographic requirements such as topological mixing, periodicity, pseudo-randomness, low correlations, and high sensitivity to initial conditions and control parameters. The use of chaotic maps for cryptography is advantageous due to their desirable characteristics, including complexity, unpredictability, sensitivity to initial values and control parameters, and ergodicity.

However, most chaos-based systems have limitations that make them impractical, such as low efficiency, insufficient security, and small keyspace [3]. The Logistic Map is one of the most famous chaos-based encryption elements, which is a mathematical model for population growth. The random sequences generated by this map have applications in cryptography and are well-suited for key generation. Even a minor variation in input values results in vastly different outputs, making it nearly impossible to predict the encryption keys. This property makes the Logistic Map an effective method for secure key generation in modern encryption systems [4]. The Hénon Map is another example of a chaos-based encryption model.

Operating in two dimensions, it is significantly more complex than the Logistic Map. Due to its high sensitivity to initial conditions, it has been used in secure communication systems and image encryption, ensuring that unauthorized users cannot reconstruct the original data without precise knowledge of the initial parameters [5]. The Arnold Cat Map offers a powerful scrambling technique for visual images. This transformation is particularly useful in biometric security, medical imaging, and digital watermarking, where protecting visual data is crucial. By rearranging pixel positions, the Arnold Cat Map creates a seemingly random distribution, making it nearly impossible to decipher the original image without the proper decryption key [6].

Despite all its advantages, chaos-based encryption faces challenges related to implementation and stability. One of the most critical aspects of ensuring that chaotic encryption systems are secure and do not show any regularities is to use conditions defined to an infinite number of decimal places. Furthermore, some key synchronization between sender and receiver continues to remain a research aspect, as the failure to align encryption keys can lead to decryption failure. Despite these challenges, the integration of chaotic maps into cryptographic systems represents a significant leap forward in data security [7]. In parallel to advancements in classical encryption algorithms using chaos theory, modern cryptographic systems have increasingly emphasized layered security and formal validation.

Recent secure payment protocols demonstrate how the integration of zero-knowledge proofs and structured cryptographic primitives contributes to building trust and preventing unauthorized access in practical systems [8]. Such frameworks, while differing in implementation, reinforce the broader need for hybrid cryptographic models that combine multiple techniques—like the use of chaotic maps in Playfair cipher enhancement. Another important factor that supports the security and reliability aspects of the proposed system is the voting storage mechanism. Without a proper and secure storage mechanism, there is a high possibility of threats occurring in the system.

A sufficient voting storage mechanism should have features such as being simple, reliable, durable, tamper-evident, subliminal-free, and cost-effective. In the following sections of the paper, cryptographic approaches are discussed in more detail, examining their advantages, challenges, and real-world implementation scenarios. Hybrid security models that combine both classical and chaos-based encryption approaches are examined, providing stronger and more viable cryptographic frameworks. The goal of this discussion is to identify how the new encryption mechanism adapts and protects against emerging cyberattacks.

II. THEORETICAL REFERENCE

II.1 LITERATURE REVIEW

The Playfair Cipher is a traditional digraph substitution cipher that has been thoroughly examined and altered to increase its security. Chaotic maps have proved to be an effective tool to increase its security and unpredictability. Chaotic transformations have led to the utility of the Playfair cipher being extended beyond text encryption. Differential cryptanalysis can be defeated by pixel-level disruptions introduced by image encryption done using chaotic theory in the diffusion and confusion processes [9]. Using hyper-chaotic Chen system based triple permutation, XORing, and multi-dimensional Playfair key generation further improves security [10].

By guaranteeing a high level of unpredictability in key evolution, the implementation of logistic-tent maps within encryption networks improves security [11]. In a 2023 study, Mandangan et al. applied Arnold's Cat Map and Hénon Map for color image encryption, demonstrating resilience against statistical and brute-force attacks [12]. In order to improve diffusion properties and make unauthorized decryption more difficult, one study incorporates chaotic maps, specifically the Hénon and Arnold Cat Maps, which introduce nonlinearity and unpredictability into encryption [13]. The frequency analysis flaws in traditional Playfair ciphers are fixed by this integration. Chaotic maps and genetic algorithms also dynamically change the encryption process, making decryption efforts even more challenging [14].

Another invention uses a nonlinear rotational Playfair matrix to provide multi-layered security by fusing chaotic principles with DNA-based encryption. Because chaotic transformations are extremely sensitive, this method guarantees that brute-force and differential attacks are rendered impracticable [15]. By increasing key complexity and unpredictability, the multi-dimensional key matrix used to create a Playfair cipher expands the encryption state space and improves security. This strategy reinforces encryption methods by strengthening defences against statistical analysis and greatly increasing the difficulty of brute-force attacks [16].

In conclusion, this study expands on previous research [9-16] by presenting a new methodology that combines multi-key approaches and chaotic systems. This method combines several chaotic maps to improve security, flexibility, and resistance to cryptanalysis, in contrast to earlier works that concentrated on discrete enhancements. The performance of current Playfair cipher modifications is highlighted by the comparative analysis of previous approaches, which is shown in Table 1. This study not only improves cryptographic resilience but also establishes the groundwork for addressing new security threats in the field by addressing important security parameters like Shannon entropy and Lyapunov exponent.

Table 1: Performance Comparison of Playfair-Based Cryptosystems.

Ref	Approach	Algorithm Used	Encryption Time (ms)	Decryption Time (ms)	Security Strength	Computational Complexity
[9]	Block Image Encryption	Block Image Encryption	Medium (~150 ms)	Medium (~140 ms)	High (Better against cryptanalysis)	$O(n^2)$ (Block based transformation)
[10]	Multidimensional Playfair	Playfair + Chaos Mapping	High (~250-350ms)	High (~250ms)	Very High (Resistant to known attacks)	$O(n^3)$ (Key expansion in multi-dimension)
[11]	PLT-Net SP-Network	Logistic- Tent Map + Playfair	Very High (~500ms)	Very High (~480ms)	Extremely High (Strong Confusion diffusion)	$O(n^3)$ (Neural Network based encryption)
[12]	Color Image Encryption	Arnold's Cat Map + Hénon Map	Medium (~180ms)	Medium (~170ms)	High (Improves Diffusion and Breaks predictability)	$O(n^2)$ (Nonlinear Pixel transformations)
[13]	Selective Image Encryption	Genetic Operations + Chaotic Maps	High (~300ms)	High (~290ms)	Very High (Dynamic and adaptive encryption)	$O(n^3)$ (Multiple transformation layers)
[14]	Time-Signature Based Image Encryption	Latin Squares + Playfair + S-boxes	Medium (~220ms)	Medium (~210ms)	High (Time dependency adds unpredictability)	$O(n^2)$ (Time based S-box variation)
[15]	DNA Playfair Matrix	16×16 DNA Playfair	Very High (~600ms)	Very High (~590ms)	Extremely High (DNA Computing adds complexity)	$O(n^4)$ (Complex DNA encoding)
[16]	Multi-Dimensional Key Matrix	Multi-Key Playfair	Medium (~200ms)	Medium (~190ms)	High (Key variability improves security)	$O(n^3)$ (Key expansion overhead)

Source: Authors, (2026).

II.2 RESEARCH GAPS

Despite the significant enhancement of Playfair cipher security using chaotic maps, most of the existing approaches are centered on either one chaotic map or two, without a comparative study over multiple maps. Few studies have analyzed the security parameters of the Playfair cipher like Shannon entropy and Lyapunov exponent, both of which are essential in assessing randomness and initial condition sensitivity. Current studies mainly utilize these encrypting methods in images, but there is limited research regarding their usability for text-based cryptographic systems [8-14], [17].The research aims to bridge the gap among current Playfair cipher improvements with a new scheme of hybrid cryptography that combines Logistic, Hénon, and Arnold Cat chaotic maps.

II.3 SCOPE AND OBJECTIVES OF THE STUDY

The scope involves thorough performance analysis with Shannon entropy to measure randomness and Lyapunov exponent to determine sensitivity to initial conditions. This research aims to design a hybrid Playfair cipher encryption system based on Logistic, Hénon and Arnold Cat map to improve cipher security. Evaluate the performance, sensitivity and randomness of the system through key metrics such as Shannon entropy and Lyapunov exponent. Carry out a comprehensive comparative analysis to determine which chaotic map is better at generating randomness.

III. METHODOLOGY

The proposed solution consists of two parts. First, the integration of the Playfair cipher with different chaotic maps like the logistic, Hénon, and Arnold cat maps. Then comparative analysis of these hybrid ciphers based on the Lyapunov Exponent and Shannon Entropy.
A. Integration of Playfair Cipher with Chaos Maps:

1. Logistic Map for Generating Keyword:

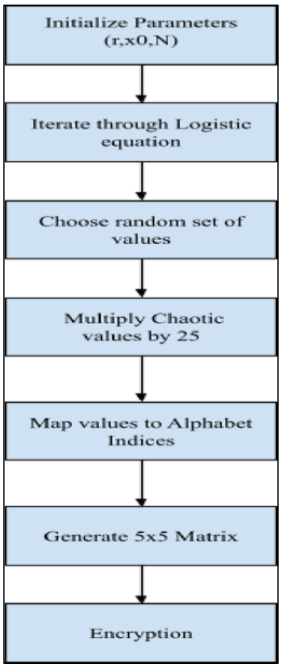

Figure 1: Process of key generation for Logistic Map.
Source: Authors, (2026).

Logistic Map is a 1D chaotic equation expressed as:

$$x_{n+1} = (1 - x_n) \quad (1)$$

Where, r is the control parameter and x_0 is the seed from the origin. Figure 1 represents the process of generating a keyword using a logistic equation. The chaotic Playfair cipher keyword generation begins with initializing the parameters. Then the logistic equation is used to generate chaotic values. From these generated chaotic values, choose a subset of them depending on the length of the keyword needed. If the length of the keyword is to be 7, then randomly 7 chaotic values are selected from this pool. This is done via a cryptographically secure pseudo-random number generator (CSPRNG) so that it's indeterminate. Once the disordered values are selected, they are converted to alphabet indices. This is accomplished by multiplying all the selected disordered values by 25 and taking the integer part of the value, getting indices ranging from 0 to 25.

These indices map to the alphabet letters; I and J are considered a single letter. The generated letters are the keyword that is filled into the 5×5 Playfair cipher key matrix one by one. After inserting the keyword letters, the remaining empty spaces in the matrix are filled with the remaining letters of the alphabet in alphabetical order such that each letter appears once. After filling the matrix, normal Playfair encryption takes place, using the key matrix to encrypt plaintext digraphs in a methodical way. The decryption method remains the same as the traditional Playfair cipher method. Algorithm 1 represents the process of generating the chaotic sequence using the Logistic Map.

Algorithm 1: Generate Chaotic Sequence using Logistic Map.

FUNCTION generate_playfair_matrix(effective_keyword_length = 5):
1. Generate a sequence of chaotic values using the Logistic Map:
chaotic_values ← logistic_map()
2. Securely select 'effective_keyword_length' random values from chaotic_values:selected_values ← securely sample 'effective_keyword_length' values from chaotic_values
3. Convert selected values to integer indices in range [0, 24]:
*letter_indices ← set of floor(value * 25) for each value in selected_values 4. Map indices to characters in the Playfair alphabet (A-Z, with I/J combined): alphabet ← ['A', 'B', 'C', ..., 'Z'] excluding 'J' selected_letters ← characters from alphabet at positions in letter_indices*
5. Remove duplicates and maintain the selected order:
used_letters ← selected_letters (as a set) remaining_letters ← all letters in alphabet not in used_letters
6. Combine selected and remaining letters:
key_matrix_flat ← selected_letters + remaining_letters
7. Reshape into 5x5 matrix: matrix_5x5 ← reshape key_matrix_flat into 5 rows of 5 columns
RETURN matrix 5x5

Source: Authors, (2026).

2. Hénon Map for Generating Keyword:

The Hénon Map is a two-dimensional chaotic system represented by:

$$x_{n+1} = 1 - p_1 x_{n2} + y_n$$
$$y_{n+1} = p_2 x_n \quad (2)$$

Where:

p_1, p_2 are the standard chaotic parameters that determine the system's behavior, x_0 and y_0 are the initial conditions, The values of x_n and y_n evolve iteratively, producing a chaotic sequence. Figure 2 represents the keyword generation process using the Hénon Map. It starts with initializing the parameters (p_1, p_2, x_0, y_0, N). Then using Hénon equations, chaotic values are generated. The remaining process remains the same as the logistic map keyword generation. After the keyword is generated, the remaining steps are the same as a traditional Playfair cipher.Algorithm 2 represents the process of generating the chaotic sequence using the Hénon Map.

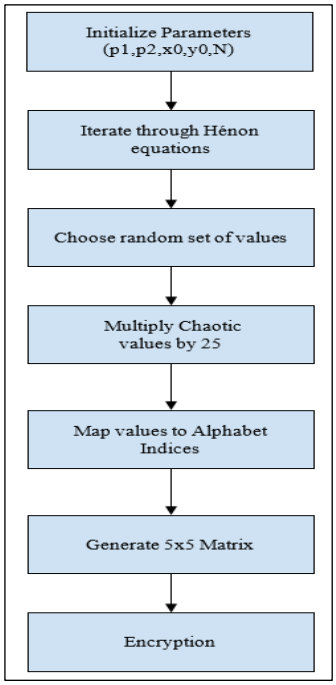

Figure 2: Process of key generation for Hénon Map.
Source: Authors, (2026).

Algorithm 2: Generate Chaotic Sequence using Hénon Map.

FUNCTION generate_playfair_matrix(effective_keyword_length = 5):

1. Generate chaotic values using the Hénon map:

a. Initialize x ← x0, y ← y0

b. FOR each iteration in range(num_values):

*i. x_new ← 1 - p1 * x^2 + y ii. y_new ← p2 * x iii. x ← x_new iv. y ← y_new*

v. Append (abs(x) mod 1) to chaotic_values

2. Securely select 'effective_keyword_length' values from chaotic_values:

selected_values ← secure random sample of chaotic_values

*3. Convert each selected value to an integer in range [0, 24]: letter_indices ← set of floor(value * 25) for each value in selected_values*

4. Map indices to characters in the Playfair alphabet (A-Z excluding 'J'):

alphabet ← ['A', 'B', 'C', ..., 'Z'] excluding 'J'

selected_letters ← characters from alphabet at positions in letter_indices

5. Remove duplicates and maintain original order:

used_letters ← set(selected_letters)

remaining_letters ← all letters in alphabet not in used_letters

6. Combine both lists to get full 25-letter Playfair matrix:

key_matrix_flat ← selected_letters + remaining_letters

7. Reshape the key_matrix_flat into a 5x5 matrix:

matrix_5x5 ← reshape key_matrix_flat into 5 rows and 5 columns

RETURN matrix_5x5

Source: Authors, (2026).

3. Arnold Cat Map used in Encryption process:

The Arnold Cat Map is a two-dimensional chaotic map commonly represented by the transformation:-

$$x_{n+1} = (x_n + y_n) \bmod 1$$
$$y_{n+1} = (x_n + 2y_n) \bmod 1 \quad (3)$$

Where:
x_n and y_n are the coordinates (or values) at the n-th iteration.
x_0 and y_0 are the initial conditions, often chosen from a 2D plane or a numerical sequence.
The mod 1 operation ensures the values remain the range [0, 1].

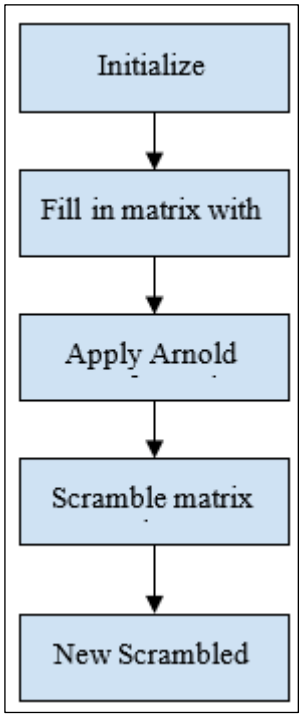

Figure 3: Arnold Cat Map use in encryption process.
Source: Authors, (2026).

In Figure 3, the Arnold Cat Map is used as an extra encryption step to provide security. After obtaining the initial ciphertext by using the Playfair Cipher, it is converted into a square matrix with each character occupying a cell. The Arnold Cat Map is then used on the matrix by iteratively permuting the characters using a chaotic permutation technique. As shown in Algorithm 3, the encryption incorporates diffusion and randomness into the ciphertext by iteratively applying the mapping formula a fixed number of times. The resulting jumbled matrix is then unraveled back into a 1D string, which becomes the cipher text. By combining the random scrambling of the Arnold Cat Map with the formal security of the Playfair Cipher, this two-stage encryption technique makes it very impossible to decipher the encrypted data without knowing the precise Playfair key and Arnold Cat Map settings. Before applying the standard Playfair decryption method, the Arnold Cat Map transform must be reversed in order to precisely recreate the original plaintext.

Algorithm 3: Encryption process using Arnold Cat Map.

```
Function ArnoldCatMap(grid, iterations, n):
    # grid: n x n 2D list of characters
    # iterations: number of transformations to perform
    # n: dimension of the grid

    Define transform(x, y, n):
        x_new = (x + y) mod n
        y_new = (x + 2 * y) mod n
        Return (x_new, y_new)

    Convert grid to a 2D array 'arr'
    Create list of all coordinate pairs (x, y) in grid of size n x n
    Flatten 'arr' to get a 1D list 'flat_values'

    For i from 1 to iterations:
        Create an empty list 'scrambled' of length n*n

        For each (x, y) in coordinates:
            Compute (x_new, y_new) = transform(x, y, n)
            scrambled[x_new * n + y_new] = arr[x][y]

        Reshape 'scrambled' into an n x n array and assign to 'arr'
    Return flattened version of 'arr'
```

Source: Authors, (2026).

B. Evaluation Metrics: Shannon Entropy and Lyapunov Exponent

For measuring the performance of chaotic maps' key generation, two popular measures are used: the Shannon entropy and Lyapunov exponent. Both measure the level of randomness and sensitivity to initial conditions, which are the two inherent requirements for producing secure and unpredictable keys.

Shannon Entropy:

It measures the amount of uncertainty or randomness in a data source, which is crucial for evaluating the security of cryptographic systems.

$$H(x) = -\Sigma p_i log_2 p_i \quad (4)$$

H(x) is defined as the entropy of X random variable.

p_i represents the probability of occurrence of each value in the chaotic sequence.

The logarithm is typically base 2, giving the entropy in bits. This formula is used to assess the randomness of data, such as the output of a random number generator or the distribution of bits in cipher text. Higher value of entropy (about 4.3) indicates that the sequence is well scattered and the Playfair key matrix becomes unpredictable. Low entropy indicates a structured sequence, which would breach security by rendering it simpler for an attacking side to infer the generated key. The bit value depends on chaotic Map used.

Lyapunov Exponent:

The Lyapunov exponent measures a chaotic system's sensitivity to the initial conditions.It is defined as:

$$\lambda(x_0) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)| \quad (5)$$

$f'(x_i)$: The derivative of the chaotic function at each iteration i.

λ(x0): Lyapunov exponent for initial condition.

If:

$\lambda > 0$: Chaotic behavior with small perturbations of the initial conditions inducing exponentially growing divergences of the trajectories.

$\lambda < 0$: Stable system with trajectories that approach.

$\lambda = 0$: Indicates the edge of chaos or a neutral system.

Having a positive Lyapunov exponent is a guarantee that the system is actually chaotic, meaning that with small perturbations of the initial values there will be exponentially divergent sequences in the limit. It is the derivative of the chaotic function at each iteration, describing the way the system is evolving. The greater the Lyapunov exponent, the greater the chaotic behavior, meaning that small perturbations of the input (the initial conditions) lead to very different outputs. It is a desirable feature of cryptographic usage since it means that any matrix of the Playfair key will change by a considerable amount if the input parameters are slightly perturbed.

IV. EXPERIMENTATION

Playfair Cipher with Chaotic Maps to Generate Keys:

Playfair cipher is a classic digraph substitution cipher, i.e., it encrypts text in pairs of letters. Chaotic maps in this code dynamically change the generation of the key matrix to ensure greater security. Chaotic maps employed for key generation possess unique initial conditions and control parameters. The values employed guarantee good chaotic behavior with maximum security.

1. Logistic Map

As discussed earlier in methodology ,the Logistic Map is a one-dimensional chaotic system and is given by:

$$x_{n+1} = (1 - x_n)$$

Control Parameter (r): 3.99 (regulates chaos in the Logistic Map)
Initial Seed Value (x_0): 0.5
Effect of Various Values of r:
0 < r < 1: Converges to zero (not chaotic).
1 < r < 3: Converges to a fixed point.
3 < r < 3.57: Periodic oscillations (bifurcation).
3.57 < r < 4: Chaotic behavior starts.
r = 3.99: Highly chaotic (most frequently used).

2. Hénon Map

As discussed earlier in methodology ,the Hénon Map is a two-dimensional chaotic system represented by:

$$x_{n+1} = 1 - p_1 x_n^2 + y_n$$
$$y_{n+1} = p_2 x_n$$

Control Parameters:

p_1 = 1.4 (Controls nonlinearity in the system)

p_2 = 0.3 (Controls contraction and stability)
Initial Seed Values: x_0 = 0.1, y_0 = 0.1
Effect of different Values:
Standard Chaotic Case: (most widely used parameters).
p_1=1.4,p_2=0.3
Reduced Chaos:
Decreasing value of p_1 (for instance,p_1=1.2) or increasing value of p_2 (for instance, p_2=0.5) stabilizes the system.
Extreme Chaos:
Increasing value of p_1 above 1.4 for more random behavior.(p_1>1.4)

3.Arnold Cat Map:

The Arnold's Cat Map is defined by the transformation:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod\ N \tag{6}$$

Effect of Different Parameter Values:
Iteration count (k):Determines number of transformation is applied. It affects the level of scrambling.
Initial seed (x_0, y_0):Initial value
Grid Size (N): Defines how the text is structured.
Key Characteristics:
Text Scrambling & Rearrangement: Random character disorder with the structure of the text preserved.
Deterministic Chaos: Despite appearing random, the transformation is a strict mathematical rule that can be used for decryption.
Reversibility: Repeatedly applying the transformation will eventually yield the original text, so it is useful for safe encryption.

V. RESULT AND ANALYSIS

This section presents the combination of playfair cipher with three different maps: Logistic, Hénon ,Arnold Cat map on sample text. Same sample plaintext is used to analyze the effectiveness of each chaotic map in enhancing security based on two parameters: Shannon Entropy and Lyapunov Exponent.

```
Enter the text to encrypt: meet me in the park

Generated Playfair Cipher Key Matrix:
A O Q X B
C D E F G
H I K L M
N P R S T
U V W Y Z

Original Text: meet me in the park
Encrypted Text: KGGRKGHPNMDRQNLQ
Decrypted Text: MEETMEINTHEPARKX
Shannon Entropy of Chaotic Sequence: 3.9769520072849187
Lyapunov Exponent: 0.6366281049592013
```

Figure 4: Output for Logistic Map.
Source: Authors, (2026).

```
Enter the text to encrypt: meet me in the park

Generated Playfair Cipher Key Matrix:
C H I T A
B D E F G
K L M N O
P Q R S U
V W X Y Z

Original Text: meet me in the park
Encrypted Text: RMFIRMTMAIBRIUMV
Decrypted Text: MEETMEINTHEPARKX
Shannon Entropy of Chaotic Sequence: 4.111543910155225
Lyapunov Exponent: 0.3951320625800923
```

Figure 5: Output for Hénon Map.
Source: Authors, (2026).

```
Enter plaintext: meet me in the park
Enter key: keyword
Ciphertext: nkkunkgqvfynbdwt
Scrambled Matrix:
n d y q
n n k w
k t v k
f g u b
Transformed Text: ndyqnnkwktvkfgub
Shannon Entropy: 3.4056390622295662
Lyapunov Exponent: 0.8981271110560293
```

Figure 6: Output for Arnold Cat Map.
Source: Authors, (2026).

Figure 7 represents the values of Shannon entropy and Lyapunov exponent for different chaotic maps. From Figure 4, Figure 5, Fig 6 in case of Shannon entropy, it is observed that the Hénon Map is more chaotic than the Logistic Map and Arnold's Cat Map.Because the Hénon Map is in a two-dimensional phase space, it is more random than the Logistic Map. Although the Arnold's Cat Map is also 2D, the dissipative characteristic of the Hénon Map makes it even more random. The process includes nonlinear dynamics that produce more varied outputs, decreasing patterns in the ciphertext.The Hénon Map attains the maximum entropy, i.e., its ciphertext is most random and is more immune to frequency-based attacks. The Logistic Map is next, exhibiting good randomness, but slightly less than the Hénon Map. The Arnold's Cat Map has the least entropy, which can be an indication of redundancy in the encrypted data, thus making it more susceptible to attacks based on redundancy.

From Figure 4, Figure 5, Figure 6 in the case of the Lyapunov exponent, it is observed that Arnold's Cat Map has the largest Lyapunov exponent, thus the most chaotic behavior, which is very sensitive to important variations. The Arnold's Cat Map has the highest Lyapunov exponent as observed in table 2 implying that it possesses the strongest chaotic behavior and thus is very sensitive to significant changes. This makes encryption more secure against brute-force and differential attacks. The Logistic Map has a moderate Lyapunov exponent, suggesting a decent amount of unpredictability but lower than Arnold's Cat. The Hénon Map has the lowest Lyapunov exponent, so its chaotic behavior is weaker than the other two.

Table 2: Values for Shannon entropy and Lyapunov Exponent for different chaotic maps.

Chaotic Map	Shannon Entropy	Lyapunov Exponent
Logistic	3.97695	0.63663
Hénon	4.11257	0.39513
Arnold Cat	3.40564	0.89813

Source: Authors, (2026).

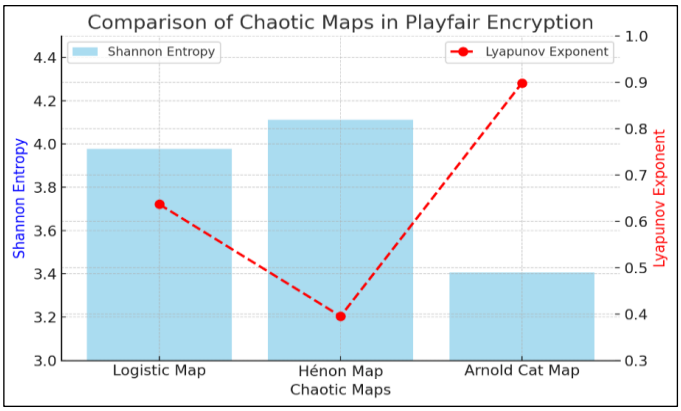

Figure 7: Visual representation of Comparative Analysis.
Source: Authors, (2026).

In addition to their chaotic strengths, the proposed maps maintain manageable computational complexities, all within polynomial time as mentioned in Table 3. These suggested methods offer a more balanced trade-off between security and efficiency, making them appropriate for practical cryptography application, in contrast to the literature presented in Table 3, where numerous solutions suffer from higher computing cost due to complex algorithmic structures.

Table 3: Computational Complexity Analysis of Proposed Models.

Version	Key Generation Time	Encryption Time	Total Complexity
Logistic	O(m)	O(n)	O(m + n)
Hénon	O(m)	O(n)	O(m + n)
Arnold Cat	O(n)	O(k × n)	O(k × n)

Source: Authors, (2026).

VI. CONCLUSION

A proper implementation of the Playfair cipher has many disadvantages, such as susceptibility to frequency analysis and weak resistance against modern attacks. The study proposed an improved version of the Playfair cipher by integrating chaotic maps (Logistic, Hénon, and Arnold Cat) to enhance the randomness of the key matrix, making encryption more secure. The comparative analysis shows that the Hénon Map provides the highest level of randomness, ensuring better diffusion in encryption. Due to its superior scattering effects, the Arnold Cat Map makes the ciphertext highly unpredictable. The Logistic Map, on the other hand, exhibits extreme sensitivity to given parameters, ensuring that even a minor change in input leads to unique outputs after encryption. Evaluations of data security metrics, including Shannon entropy and the Lyapunov exponent, confirm the improved security of this system.

The highest Shannon entropy value (4.11257) among the analyzed maps highlights the superior random behavior of the Hénon Map. In terms of the Lyapunov exponent, the Arnold Cat Map shows the highest potential value (0.89813), making it the most sensitive to key variations. Meanwhile, the Logistic Map maintains a balance between these two critical cryptographic properties while managing computational cost effectively. It is evident that this hybrid encryption approach offers significantly stronger security compared to standard Playfair ciphers. Future work may explore adaptive selection of chaotic maps based on the characteristics of the input to optimize performance. Additionally, further research could investigate the feasibility of implementing this approach in real-time cryptographic environments.

VII. AUTHOR'S CONTRIBUTION

Conceptualization: Radhika Patel, Isha Patel, Mahek Vira and Stevina Dias.
Methodology: Isha Patel, Mahek Vira and Stevina Dias.
Investigation: Isha Patel, Mahek Vira and Stevina Dias.
Discussion of results: Radhika Patel, Isha Patel, Mahek Vira and Stevina Dias.
Writing – Original Draft: Isha Patel, Mahek Vira and Stevina Dias.
Writing – Review: Radhika Patel.
Supervision: Radhika Patel.
Approval of the final text: Radhika Patel, Isha Patel, Mahek Vira and Stevina Dias.

VIII. REFERENCES

[1] Y. Wang, "A Classical Cipher-Playfair Cipher and Its Improved Versions," *2021 International Conference on Electronic Information Engineering and Computer Science (EIECS)*, Changchun, China, 2021, pp. 123-126, doi: 10.1109/EIECS53707.2021.9587989.

[2] N. Charalampidis, C. Volos, L. Moysis, A. V. Tutueva, D. Butusov and I. Stouboulos, "Text Encryption Based on a Novel One Dimensional Piecewise Chaotic Map," *2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*, Saint Petersburg, Russian Federation, 2022, pp. 263-268, doi: 10.1109/ElConRus54750.2022.9755622.

[3] Moatsum Alawida,Enhancing logistic chaotic map for improved cryptographic security in random number generation,Journal of Information Security and Applications,Volume 80,2024,103685,ISSN 2214-2126,https://doi.org/10.1016/j.jisa.2023.103685.

[4] Kumar, Sunil & Shailani, Manish & Budhiraja, Rajat & Das, Mrinal & Singh, Sanjeev. (2018). A secured cryptographic model using intertwining logistic map. Procedia Computer Science. 143. 804-811. 10.1016/j.procs.2018.10.386.

[5] Ibrahim, S., & Alharbi, A. (2020). Efficient image encryption scheme using Hénon map, dynamic S-boxes and elliptic curve cryptography. Journal of King Saud University – Computer and Information Sciences, 34(3), 502–510.

[6] Turan, Mehmet & Gökçay, Erhan & Tora, Hakan. (2024). An unrestricted Arnold's cat map transformation. Multimedia Tools and Applications. 83. 1-15. 10.1007/s11042-024-18411-9.

[7] Kocarev, L., & Parlitz, U. (2015). General approach for chaotic synchronization with applications to communication. Physical Review Letters, 74(25), 5028–5031.

[8] Rura, L., Issac, B., & Haldar, M. K. (2016). Implementation and evaluation of steganography-based online voting system. International Journal of Electronic Government Research, 12(3), 71–93.

[9] E. A. Albahrani, A. A. Maryoosh, and S. H. Lafta, "Block image encryption based on a modified Playfair and chaotic system," Journal of Information Security and Applications, vol. 51, p. 102445, 2020. doi: 10.1016/j.jisa.2019.102445

[10] K. Bhat and D. Mahto, "Securing images using chaos and multidimensional Playfair cipher," in 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), IEEE, pp. 1009–1015, 2020. doi: 10.1109/ICECA49313.2020.9297380

[11] A. Maitra, A. Pal, and R. Karmakar, "PLT-Net: A 2-layer SP-network using a modified Playfair cipher and the Logistic-Tent map," in 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, pp. 1–7, 2022. doi: 10.1109/ICCCNT56485.2022.10051792

[12] A. Mandangan and S. N. H. Mohammad, "Colour image encryption and decryption using Arnold's Cat Map and Henon Map," International Journal of Computational Thinking and Data Science, vol. 1, no. 1, pp. 41–52, 2024. doi: 10.37934/CTDS.1.1.41-52 .

[13] P. Murali, G. Niranjana, A. J. Paul, et al., "Domain-flexible selective image encryption based on genetic operations and chaotic maps," The Visual Computer, vol. 39, pp. 1057–1079, 2023. doi: 10.1007/s00371-021-02384-z

[14] S. T. Dougherty, S. Sahinkaya, and D. Ustun, "A novel method for image encryption using time signature-dependent S-boxes based on Latin squares and the Playfair system of cryptography," Multimedia Tools and Applications, vol. 83, pp. 4167–4194, 2024. doi: 10.1007/s11042-023-15240-0

[15] D. Ibrahim, K. Ahmed, M. Abdallah, and A. A. Abd-Elmgeid, "A new chaotic-based RGB image encryption technique using a nonlinear rotational 16×16 DNA Playfair matrix," Cryptography, vol. 6, no. 2, p. 28, 2022. doi: 10.3390/cryptography6020028

[16] M. D. Al-Hassani and M. T. Gaata, "Development of a Playfair cryptosystem based on generating a multi-dimensional key matrix," Bulletin of Electrical Engineering and Informatics, vol. 12, no. 3, pp. 1849–1856, 2023. doi: 10.11591/eei.v12i3.4418

[17] A. Z. Ghavidel and B. Isaac, "Secure transport protocols for DDoS attack-resistant communication," 5th Student Conference on Research and Development, IEEE, pp. 1–5, 2007. doi: 10.1109/SCORED.2007.4451370