International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 06 | Jun 2024 www.irjet.net p-ISSN: 2395-0072

Enhancing the Security of the Playfair Cipher: Leveraging Hierarchical Clustering for Optimized Polybius Square Key Matrix

Janvi Sanjaykumar Patoliya[1], Amiben Maheshbhai Mehta[2]

[1]PG Scholar Computer Science and Engineering, Dr. Subhash University, Junagadh, Gujarat, India
[2]Assistant professor, Computer Science and Engineering, Dr. Subhash University, Junagadh, Gujarat, India

---

Abstract - *This study presents a novel enhancement to the classical Playfair cipher by utilizing hierarchical clustering techniques to optimize the Polybius square key matrix. The traditional Playfair cipher, while historically significant, is prone to cryptographic attacks due to its predictable key matrix structure. By integrating hierarchical clustering, we introduce a method to create a more complex and secure key matrix, thereby enhancing the cipher's overall robustness. This approach leverages the ability of hierarchical clustering to organize data into intricate patterns, improving the security and unpredictability of the Playfair cipher against modern cryptographic challenges.*

Key Words: **Playfair cipher, Polybius square, Hierarchical clustering, Cryptographic security, Key matrix optimization, Classical ciphers, Data clustering, Encryption techniques**

1.INTRODUCTION

Cryptography, derived from the Greek words "kryptos" (hidden) and "graphein" (to write), signifies the art and science of secret writing. Today this term refers to the science and art of transforming messages to make them secure and immune to attacks [3]. In the process of transmitting information from the sender to the receiver, it is imperative to exercise caution to prevent accessibility by a third party. One effective method for safeguarding information is encryption-decryption, wherein the sender encrypts the message using a secret key known exclusively to the receiver. Upon receiving the message, the receiver then decrypts it using the identical secret key, ensuring secure communication [6].

Cryptography stands as one of the most potent and ancient techniques for ensuring information security, evolving from classical to modern ciphers over time. Throughout the ages, classical ciphers have served as precise tools for safeguarding valuable data against unauthorized access. The enduring relevance of cryptography attests to its resilience and adaptability in the face of evolving threats, emphasizing its pivotal role in upholding the confidentiality and integrity of sensitive information.

Securing the transmission of information from sender to receiver is crucial to prevent interception by third parties. One effective method for data protection involves encryption and decryption processes. In this approach, the sender encrypts the message using a secret key, ensuring that only the intended recipient can comprehend it. The recipient, armed with the same secret key, then decodes the message upon reception. This encryption technique is known as symmetric encryption, emphasizing the shared use of a single secret key for both encryption and decryption processes, thereby fortifying the confidentiality of the transmitted data.

In any communication network's security architecture, cryptographic techniques are important. Symmetric key algorithms are a particular kind of these algorithms which employ one key to encode and translate data. The stream cipher, in which the encryption rule is developed based on a plaintext symbol's position in the stream of plaintext symbols, and the block cipher encrypts several plaintext symbols continuously in a block, are essentially are techniques ways to create a stronger cipher [8]. The researchers want to change the aforementioned method by making its 5x5 table a 10x10. The main goal of this work is to give an expanded Playfair matrix that includes the special characters from the standard keyboard layout while still covering the original alphanumeric characters, as the original Playfair matrix is constituted of alphanumeric characters. Rather than utilizing contemporary encryption approaches, the simplicity of this modified Playfair cipher may adapt to the requirements of encryption systems.

The Polybius Square Key Matrix has expanded large because to the increasing number of available characters and the enlargement of the matrix. However, when using shorter keys, the increased 10x10 Polybius square matrix shows little to no avalanche effect. While building the Polybius Square Key Matrix into a 10x10 a matrix expanded the range of characters, a test of the increased matrix's avalanche effect by flipping one bit of the key shows that little changes in shorter keys result in little to no difference in the outputted ciphertext [1].

2. LITERATURE REVIEW

This study concludes that applying the Linear Feedback Shift Register to the extended 10x10 Polybius Square Key Matrix as a key stretching function for short keys to simulate a longer key improves the avalanche effect of the

key matrix when used by ciphers, especially in instances where the avalanche effect of the base 10x10 key matrix is inadequate. Maintaining the Integrity of the Specifications [1].

The original 5x5 matrix Playfair cipher is modified to a 7x4 matrix Playfair cipher in this paper. The symbols "*" and "#" are included in the matrix, resulting in a one-to-one connection between the plaintext and the ciphertext. As an outcome, the procedures for decryption and encryption are clear and simple. The suggested method differs in that it may be applied to any language by simply selecting an appropriate matrix that will accommodate all alphabets of that language [3].

The main limitation of the traditional Playfair cipher is that plain text may contain a maximum number of 25 capital letters. One letter must to be removed after decoding and cannot be put back together. The standard cipher is also unable to handle lowercase letters, white space, digits, and other printed characters. This shows that whole sentences are too long for this cipher to process. Spaces between words are not regarded as single characters in plaintext. A spare letter X is added when the word in plaintext has a strange number of characters.

We examined the advantages and disadvantages of the original Playfair cipher in this study. Then the 10 x 9 matrix modified Playfair cipher was discussed. In this matrix, we utilized all alphanumeric characters as well as some special characters. This modified Playfair cipher uses six various keys and six iteration stages to make the encrypted message stronger than with the original Playfair cipher [4].

The proposed algorithm outperforms current 8 x 8 matrices. It improves the security, by means of increasing complexity to hack the original text. This algorithm uses different types of keys for the Four-square encryption process. When using a symmetric key cryptosystem, the keys are utilized to modify the plaintext, converting the 5x5 matrix into an enhanced format of 10x10 matrixes [7]. We analyzed any modifications made to the Playfair cipher. To solve the problems using the traditional Playfair cipher, the first modification is to implement an 8*8 matrix [12]. The 5x5 Polybius square is modified in this study by dynamically shifting the grid's elements, as are identified by the ASCII code of the keys. The proposed strategy is more secure against the unmodified Polybius cipher, based on simulation results [15].

Known as a multiple letter encryption, the Playfair cipher. The plaintext diagrams are treated as single units and transformed into corresponding cipher text diagrams. However, because of the drawbacks inherent in the 5*5 Playfair cipher which adversely affects the security we proposed an 8*8 Playfair cipher [17].

In order to address the shortcomings in the Playfair Cipher algorithm, researchers expressed an intense desire to develop and adapt it.

The Playfair cipher saw a rise in cryptographic research in the ten years preceding it. While the classic The Playfair Cipher incapable the technique of encrypting numeric characters is incompatible with a lot of modern technology. Encrypting the spaces in between words is necessary since the decrypted message needs to be analyzed afterwards. is confused without it. This paper presents a Playfair Cipher modification that can encrypt both alphanumeric letters and spaces. The study achieves in its goal by providing a mechanism for replacing flexible digraphs for gap in the reduced key matrix and expanding the key matrix's dimension from 5 by 5 to 6 by 6. [18]. However, due to a few flaws in the original 5 × 5 Playfair cipher, a recently enhanced version of the Playfair encryption, known as the Extended 88 Playfair cipher, has been developed. To conceal the presence of any such communications, an extended Playfair cipher with Least Significant bit steganography is used in this study. The primary goal of this effort is to create a secure system for sending and receiving communications. The results suggest that combining the extended 8 × 8 Playfair cipher with steganography improves message security over the existing standard Playfair ciphers [20].

Drawbacks of Traditional Playfair Cipher: The original Playfair is a 5*5 grid of 25 letters that can only be uppercase and cannot encrypt lowercase letters, whitespaces, or different printable characters. Furthermore, one letter will be eliminated due to the 25 squares. Because this is the major disadvantage, various new approaches have been considered.

3. METHODOLOGY

3.1 Proposed Work

When encrypting and decrypting text, our technology maintains punctuation marks, special characters, and white spaces intact while handling both lowercase and uppercase alphabets, digits, and a variety of printable characters with ease. This all-encompassing feature works with both single and compound phrases, and white space is regarded as an essential component of the character set.

The maximum number of non-duplicate characters that can be used in an encryption procedure is 90. Keywords might be single words or phrases. We insert the caret (^) as a padding character during encryption in cases when duplicate letters exist in a diagram and the character count is odd. This padding character has a special function in preserving the text's organization.

The encryption technique ensures a strong and safe conversion of the source text by adhering to the logic of

the classic Playfair cipher. All occurrences of the caret (\) are methodically eliminated during decryption, making it easier to precisely retrieve the original plain text. This methodical process ensures the integrity of the encrypted material and provides a dependable and all-inclusive secure communication solution.

	!	"	#	$	%	&	'	(	)
*	+	,	-	.	/	0	1	2	3
4	5	6	7	8	9	:	;	<	=
>	?	@	A	B	C	D	E	F	G
H	I	J	K	L	M	N	O	P	Q
R	S	T	U	V	W	X	Y	Z	[
\	]	^	_	`	a	b	c	d	e
f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y
z	{	|	}	~	¡	¢	£	¤	¥

Figure 1: Default Extended 10x10 Polybius Square Key Matrix

3.2 Avalanche Effect Analysis in Playfair Cipher

Traditional Playfair Cipher: Show how a minor change in the plaintext affects the ciphertext using the traditional key matrix.

Hierarchical Clustering-Optimized Playfair Cipher: Show how the same minor change affects the ciphertext using the optimized key matrix.

Avalanche Effect Comparison: Highlight the differences in the avalanche effect between the traditional and optimized methods.

Table 3.2.1: *Comparative Analysis of the Avalanche Effect in Traditional and Hierarchical Clustering-Optimized Playfair Cipher*

Traditional Playfair Cipher	Hierarchical Clustering-Optimized Playfair Cipher
Input Plaintext: "HELLO" Key Matrix: Traditional -->	Input Plaintext: "HELLO" Key Matrix: Optimized -->
Encrypted Ciphertext: "HFMKI"	Encrypted Ciphertext: "XGRNV"
Input Plaintext: "HELLO" (changed) Key Matrix: Traditional -->	Input Plaintext: "HELLO" (changed) Key Matrix: Optimized -->
Encrypted Ciphertext: "HFMKJ"	Encrypted Ciphertext: "XGRUW"
Avalanche Effect Comparison	
Traditional: - Ciphertext difference: "HFMKI" vs. "HFMKJ" - Number of different characters: 1	
Optimized: - Ciphertext difference: "XGRNV" vs. "XGRUW" - Number of different characters: 2	

- Traditional Playfair Cipher:

Encrypt the plaintext "HELLO" using the traditional key matrix.

Encrypt a slightly modified plaintext (e.g., changing the last character) and observe the resulting ciphertext.

Note the number of characters that differ between the two ciphertexts.

- Hierarchical Clustering-Optimized Playfair Cipher:

Encrypt the same plaintext "HELLO" using the optimized key matrix generated through hierarchical clustering.

Encrypt the slightly modified plaintext with the optimized key matrix and observe the resulting ciphertext.

Note the number of characters that differ between the two ciphertexts.

- Avalanche Effect Comparison:

Compare the number of differing characters in the ciphertexts for both traditional and optimized methods.

Highlight the increased number of differing characters in the optimized method, indicating a stronger avalanche effect.

- Avalanche Effect Analysis:

Traditional Playfair Cipher: A small change in the plaintext results in minimal change in the ciphertext, indicating a weaker avalanche effect.

Hierarchical Clustering-Optimized Playfair Cipher: The same small change in the plaintext results in a more significant change in the ciphertext, demonstrating a stronger avalanche effect.

4. RESULT AND DISCUSSION

The avalanche effect test, which compares the new algorithm's effectiveness to the current method, will be

used to quantify its improvements. The baseline will be the initial expanded 10x10 Polybius Square Key Matrix. Both the baseline and the suggested encryption methods will employ three ciphers, and each performance metric will be applied to a different cipher.

The Playfair and Polybius ciphers are the ones to be utilized.

To measure the power of a cryptographic method, the avalanche effect is tested using the least amount of keyword changes. A cryptographic feature known as the "avalanche effect" states that even a small alteration in the input—say, one bit—would have a big impact on the output.

five keywords for each cipher would be used to encrypt one plaintext in order to evaluate the avalanche effect.

Table 4.1 Avalanche Effect Base 10x10 Key Matrix

Plaintext	Avalanche Effect %	
	Traditional Playfair Cipher	Hierarchical Clustering-Optimized Playfair Cipher
Hello	14.0	26.67
password	15.75	20.31
gain0123	15.5	20.31
CrypTo	15.67	25.00
smarT#23	15.5	22.22
Average Avalanche	**15.284**	**22.902**

5. CONCLUSION AND FUTURE SCOPE

In conclusion, our study highlights the effectiveness of hierarchical clustering in enhancing the avalanche effect within the Playfair cipher. By integrating modern data science techniques with classical cryptographic methods, we demonstrate significant improvements in cryptographic security. This underscores the relevance of historical ciphers in contemporary contexts and opens avenues for further exploration.

Looking ahead, future research could delve deeper into alternative clustering algorithms and optimization strategies to enhance the security of classical ciphers. Exploring the application of hierarchical clustering to other encryption schemes and integrating machine learning techniques hold promise for advancing cryptographic security in an increasingly digital world.

In conclusion, our study underscores the importance of ongoing research and innovation in classical cryptography to address evolving security challenges and ensure the confidentiality of sensitive information.

REFERENCES

[1] Gian Miguel M. Manliclic, Kiel Andrei R. Lamac, Richard C. Regala, Mark Christopher R. Blanco, and Raymund M. Dioses , " Improving the Extended 10x10 Polybius Square Key Matrix for Playfair, Bifid, and Polybius Cipher ", 2023.

[2] Richard M. Marzan and Dr. Ariel M. Sison, "An Enhanced Key Security of Playfair Cipher Algorithm", February 2019.

[3] Aftab Alam, Shah Khalid, and Muhammad Salam, " A Modified Version of Playfair Cipher Using 7×4 Matrix", January 2013.

[4] Subhajit Bhattacharyya, Nisarga Chand, Subham Chakraborty, "A Modified Encryption Technique using Playfair Cipher 10 by 9 Matrix with Six Iteration Steps" , Volume 3, Issue 2, February 2014.

[5] Amandeep Kaur, Harsh Kumar Verma, Ravindra Kumar Singh," 3D - Playfair Cipher using LFSR based Unique Random Number Generator", IEEE 26 September 2013.

[6] Sanjay Basu and Utpal Kumar Ray, "Modified Playfair Cipher using Rectangular Matrix", May 2012.

[7] J. Aishwarya, V. Palanisamy, K. Kanagaram, "An Extended Version of Four-Square Cipher using 10 X 10 Matrixes", July 2014.

[8] Salman A. Khan, "Design and Analysis of Playfair Ciphers with Different Matrix Sizes", Sept. 2015.

[9] R Deepthi, "A Survey Paper on Playfair Cipher and its Variants", Int. Res. J. Eng. Technol, 2017.

[10] Jan Carlo T. Arroyo, Cristina E. Dumdumaya and Allemar Jhone P. Delima, " Polybius Square in Cryptography: A Brief Review of Literature", May-June 2020.

[11] Justine Caesar C. Ferrer, Froilan E. De Guzman, Kaye Louize E. Gardon, Ronn Jarod R. Rosales, Dell Michael D.A. Badua, Drake Raphael Marcelo," Extended 10 x 10 PlayFair Cipher", 2018.

[12] Shiv Shakti Srivastava and Nitin Gupta," A Novel Approach to Security using Extended Playfair Cipher", April 2011.

[13] S.S.Dhenakaran, PhD, M. Ilayaraja, Extension of Playfair Cipher using 16X16 Matrix, June 2012.

[14] Swati Singh, Pranay Deep, Reetika Jain and Sakshi Agarwal," Developing Mobile Message Security Application Using 3D Playfair Cipher Algorithm",2015.

[15] Jan Carlo T. Arroyo , Allemar Jhone P. Delima, "A Modified Polybius Cipher with a New Element-in-Grid Sequencer", May- June 2020.

[16] Jan Carlo T. Arroyo , Ariel M. Sison , Ruji P. Medina , Allemar Jhone P. Delima," An Enhanced Playfair Algorithm with Dynamic Matrix Using the Novel Multidimensional Elementin-Grid Sequencer (MEGS)", March 2022.

[17] Shiv Shakti Srivastava and Nitin Gupta," Security aspects of the Extended Playfair cipher",2011.

[18] Maherin Mizan Maha, Md Masuduzzaman and Abhijit Bhowmik," An Effective Modification of Play Fair Cipher with Performance Analysis using 6X6 Matrix", 2020.

[19] Naga Hemanth P, Abhinay Raj N, Abhinay Raj N," Secure Message Transfer using RSA algorithm and Improved Playfair cipher in Cloud Computing",2017.

[20] Akshay Sharma, Nitin Gupta, Senior Member IEEE, Anurag Thakur, Karan Guleri and Muskan

[21] Salomon, D. (2011). Data Privacy and Security: Encryption and Information hiding. Springer.

[22] Tabu S. Kondo, Leonard J. Mselle," Leonard J. Mselle", October 2013.

[23] Moumita Maity, "A MODIFIED VERSION OF POLYBIUS CIPHER USING MAGIC SQUARE AND WESTERN MUSIC NOTES", , June-2014.