Qualitative and Quantitative Analysis of Modifications in Playfair Cipher

Anubhab Ray(✉), Kartikeya Singh, Aditya Harsh, Shubham Thorat, and Nirmalya Kar

Department of Computer Science and Engineering, NIT Agartala, Agartala, India
rayanubhab@gmail.com, nirmalya@ieee.org

Abstract. Security in digital world has become a paramount issue, even more so in the post pandemic world when the digital footprint of the world has increased. Multiple encryption techniques are used to ensure the same. Certain famous classical ciphers which were in prevalent use during ancient times are now not robust enough to keep up with security requirements of modern world. This paper analyses the different modifications proposed to one such cipher i.e., Playfair Cipher and how these modifications enhance it's performance thus making it usable in modern world.

Keywords: encryption · decryption · playfair cipher · cryptography

1 Introduction

In the post pandemic era, the digital footprint of the world has increased as a result of professional settings like institutions and industries adopting remote work. With this increase in internet traffic data security is needed more than ever. Data Encryption refers to the transformation of a given message into a structure that makes it indecipherable to anyone without a secret key. This technique ensures the message is read by only the intended recipient thus ensuring privacy and safety of both parties.

In the current world when the transfer of data has become a big part of everyday life, encryption is more important than ever to ensure the protection of private information, sensitive data, and enhancing the security of both sender and receiver. Cryptography [1] is one such technique. Cryptography is essentially a process of conversion of plain text into indiscernible text and vice-versa. By doing so, it is ensured that the message can only be read by intended recipient and sender. Cryptography has various applications ranging from preventing data theft and ensuring user security to user authentication. Cryptography is divided into two categories: symmetric and asymmetric. The classical cipher [2] techniques like Hill Cipher [3], Playfair Cipher, etc. while used in ancient times are now obsolete can't be employed because of complexity of today's protocols.

However, modified version of some of these classical ciphers [4] can be used in modern world as they are stronger and can sustain certain attacks. They can

K. Dasgupta et al. (Eds.): CICBA 2023, CCIS 1956, pp. 186–195, 2024.
https://doi.org/10.1007/978-3-031-48879-5_15

be employed in a resource constrained environment where computation speed and size requirements play a vital role. In this paper we will discussing the modifications proposed to one of the most widely known encryption algorithms i.e., the Playfair cipher and how these modifications affect it's performance. We tried to do a qualitative and quantitative analysis of modifications in playfair cipher and how these changes affect it's performance and analyse the attacks possible.

2 Motivation and Objective

The enduring popularity of the classic Playfair cipher has prompted researchers and practitioners to subject it to both qualitative and quantitative analyses. Such multifaceted investigations offer valuable opportunities to thoroughly examine the cipher's advantages and disadvantages, as well as identify ways to enhance its security and performance. By exploring the cipher from a variety of angles, researchers can gain a deeper understanding of its underlying principles and assumptions, uncover vulnerabilities that can be exploited by attackers, and develop novel modifications to bolster its security. Moreover, quantitative analysis empowers researchers to rigorously test the cipher's effectiveness against a range of attacks, providing insights into its practicality, efficiency, and resilience. In combination, qualitative and quantitative analyses are essential tools for ensuring that the classic Playfair cipher continues to serve as a valuable cryptographic system in an ever-changing digital landscape [5].

Our goal is to research the different variations of the well-known Playfair cipher, a classical cryptography technique. We want to examine the adjustments made by earlier researchers to increase the complexity and security of the algorithm. We want to obtain a greater grasp of the approaches used to accomplish the desired result by understanding these techniques. We intend to build our own algorithm in the future using this information.

3 Literature Survey

3.1 Traditional Playfair Cipher

Playfair cipher [6] algorithm is one of the most renowned symmetric encryption algorithms. It is dependent on the 5×5 matrix which is created by inputting the given key into the matrix row-wise, left to right first and then using all the other alphabets to fill the rest of the matrix in chronological order. The encryption is carried out in following steps:

1. Termination of white space in the given plaintext and then grouping the letters into groups of two. The two grouped letters must be distinct, if two letters in a group happen to be same, an additional "X" is inserted between them to maintain aforementioned condition. In the case of length of plaintext being odd, a "X" is concatenated at the end of the plaintext.

2. The resulting groups of two characters, are then taken one by one and encrypted with respect to their position in the matrix.
   - The characters immediately to their right take the place of the two characters if they happen to lie in the same row of the matrix. If a character is last in the row it is replaced by first.
   - In a similar manner, in case the two characters are located in the same column of the matrix, they are substituted with the characters located just below them. When the character is positioned at the last slot of the column, it is substituted with the first character
   - If the two plaintext characters are neither in same row nor same column, they are replaced by character in their own row and in the column of the other character in the pair of two.

Playfair cipher, however has some major disadvantages:

- The plaintext can only contain 25 upper case alphabets (with I and J considered one character), lower case characters are not handled.
- Encrypted text when decrypted contains extra characters, like X which is added when the given pair has the same characters or the plaintext's length is odd. Thus adding to the confusion.
- Since the matrix purely constitutes upper case letters, plaintext with numbers, special characters and lower case letters are not handled.
- Whitespace in the plaintext is ignored and hence cannot be handled.

3.2 Discussion on the Modifications of Playfair Cipher

It is evident from the discussion that the traditional playfair cipher cannot be employed in most cases of real world application. Hence many modifications have been proposed to the traditional playfair cipher over the years along with it being used with other encryption techniques to improve on its core functionality. Some of the commonly used modifications which can be used to overcome the limitations of Playfair Cipher are given in Fig. 1.

The methodology proposed by Marzan et al. [7] aims to tackle the security problem of the playfair cipher by encrypting and decrypting the key. Using a 16×16 matrix along with the aforementioned method, the intent is to overcome the shortcomings of both symmetric and asymmetric keys with the use of XOR operations, two's complement followed by bit swapping. First sender enters both plaintext and the key, the key is used to convert plaintext into ciphertext. The key's security is then ensured by encrypting key by converting ASCII characters into decimal, converting decimal into binary, applying 2's compliment, XOR and bit swapping. The result ciphertext and the original ciphertext are both sent to receiver and decrypted to get the intended message.

Albahrani et al. [8] presented a method for encrypting images using a combination of diffusion and modified Playfair cipher. Their approach employs two cross-chaotic maps to generate a 16×16 Playfair matrix as the encryption key. To encrypt an input bitmap image, it is first divided into red, blue, and green

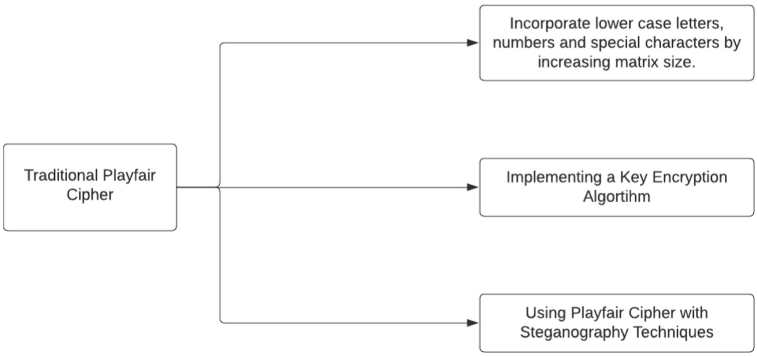

Fig. 1. Playfair Cipher Possible Modification

color matrices. The two cross-chaotic maps are then iterated to generate random numbers in the range of [0 to Number of Rows] and [0 to Number of columns], which are used to encrypt each of the color matrices using the Playfair matrix. The resulting image is further divided into 16×16 blocks and each block is encrypted as a separate Playfair matrix. The proposed method is capable of encrypting all types of inputs, including alphanumeric and special characters. Additionally, the encrypted image exhibits a low correlation coefficient, indicating that statistical attacks are unlikely to reveal any useful information to an attacker. Furthermore, the algorithm demonstrates remarkable resilience against differential attacks as even a minor change to the original image results in significant modifications in the encrypted counterpart.

In [9] the authors seek to combine the advantages of 3D Playfair Cipher and PVD method. 3D Playfair Cipher is easy to implement and has reliable encoding and lossless fat compression while PVD helps algorithm hide more info without causing distinguishable distortions between original and stego image. Maximum hiding of bits and falling of problem are addressed by treating each RGB pixel pair on RGB cover image as three distinct pixel pair. It is observed that the Peak signal to noise ratio (PSNR) and data hiding capacity are better in the proposed method than just using original PVD method, 1.023 times and 1.333 times respectively.

Siswanto et al. [10] suggest using cryptography and LSB (Least Significant Bit) steganography in combination to ensure safety of a message. The text message is first encrypted with playfair cipher method and the resultant ciphertext will be embedded om 8-bit grayscale digital image using steganography. Using both Cryptography and Steganography in combination helps user maintain confidentiality of a message. The Mean Square Error (MSE) and Peak Signal to Noise Ratio showed normal results. MSE is valued between the original image and the manipulated image. Based on the result of the study, there's no notable difference in the stego image containing secret message from the plain image.

The methodology proposed by Patil et al. [11] aims to address modern day attacks by proposing security improvements in existing models. RSA, steganog-

raphy and RMPS keyless transposition is used in tandem with playfair cipher for encryption and decryption. The traditional 5×5 playfair matrix is replaced by 19×4 matrix to accommodate more characters. Sender encrypts the Playfair cipher using recipient's public key which employs RSA algorithm. Then RMPS keyless transposition and LSBS is used to encrypt the message and insert it into image and send it to receiver. Then the exact reverse process of encryption is applied in decryption. The resulting method can withstand Brute-Force, Frequency analysis, Replay attack and Man in the middle attack due to it's various properties.

4 Result and Analysis

The following aspects have been considered for the evaluation of the cryptographic algorithms:

4.1 Brute Force Attack

In a cryptographic assault known as a "brute force", the attacker tries every key combination and password combination until they find the one that works. In other words, until they discover the one that unlocks the ciphertext or allows them access to the system, the attacker thoroughly tests every potential answer.

When there is no other way for the attacker to decrypt the data, such as when the encryption key is unknown or the password is challenging to figure out, brute force attacks are frequently utilised. Despite their potential effectiveness, brute force attacks can be time-consuming and computationally demanding, especially for longer keys or passwords. Generally, if the size of key space is less than 2^{128} it is considered vulnerable [5].

The calculation of the projected duration for a brute force attack is as follows:

$$\frac{\text{Number of character set}^{\text{length of key}}}{\text{Encryption/Second(EPS)}}$$

4.2 Frequency Analysis Attack

A frequency analysis attack exploits predictable patterns in certain encryption schemes that substitute one letter or symbol for another based on a fixed pattern. By analyzing the frequency of letters or symbols in a ciphertext, an attacker can infer the substitution pattern used and eventually decipher the message. To protect against frequency analysis attacks, encryption schemes can be designed to avoid predictable patterns, use more complex substitution rules, or use polyalphabetic ciphers with multiple substitution rules [11].

4.3 Avalanche Effect

The avalanche effect serves as a means to test the randomness of a cryptographic system. A desirable characteristic of an encryption algorithm is that even a minor modification to either the plaintext or the key should bring about a considerable change in the resulting ciphertext. If an algorithm fails to demonstrate a strong avalanche effect, it could be vulnerable to attacks such as known plaintext or chosen-plaintext, where an attacker can potentially predict the input from the given output.

The avalanche effect is calculated as:

$$\text{AE}(\%) = \frac{\text{No. of Changed Bits in Cipher text}}{\text{Total no. of Bits in Cipher text}} \times 100$$

Generally, if the avalanche effect is greater than 50% the cryptosystem is considered to be secure [12]. The following metrics are used to measure avalanche effect in a cryptosystem:

4.3.1 Mean Squared Error (MSE)

Mean Square Error (MSE) is a commonly used measure of the difference between an estimator or predictor and the true value of what is being estimated or predicted. It is often used in statistical analyses and machine learning to evaluate the performance of a model or algorithm. The MSE is calculated by taking the average of the squared differences between the predicted and actual values. The formula for MSE is:

$$\text{MSE} = \frac{1}{\text{H} \times \text{W}} \sum_{i=0}^{H-1} \sum_{j=0}^{W-1} | \text{C(i,j)} - \text{P(i,j)} |^2$$

where C(i,j) and P(i,j) denotes the pixels at the i^{th} row and j^{th} column of H X W cipher and plain image respectively. Normally, If $MSE > 30dB$ then it is considered to be secure enough and no relationship can be established easily between the two images [13].

4.3.2 Number of Pixel Change Rate (NPCR)

The NPCR value is determined by the number of pixels in the original and processed images that have the same location. A higher NPCR score signifies that there has been an abrupt alteration of the position of pixels in the image. The NPCR score should ideally be 99.6094% [13]. NPCR is calculated as:

$$\text{NPCR}(\ \%\ ) = \frac{\sum_{i=1}^{H} \sum_{j=1}^{W} \text{D(i,j)}}{\text{H} \times \text{W}} \times 100$$

where, H and W are the height and width of the image respectively and D(i, j) is defined such that D(i, j) = 0, if C1(i, j) = C2(i, j); else D(i, j) = 1.

4.3.3 Unified Averaged Changed Intensity (UACI)

The UACI score is a measure of the average difference in intensity between two cipher images c1 and c2. The value of UACI should ideally be: 33.46% [8]. The formula for calculating UACI is:

$$\text{UACI}(\ \%) = \frac{1}{\text{H} \times \text{W}} \sum_{i,j} \frac{|\ \text{C1(i,j)} - \text{C2(i,j)}\ |}{255} \times 100$$

A high UACI/NPCR value is typically interpreted as a strong resistance to differential attacks (Tables 1 and 2).

The tables presented above offer a comprehensive comparison and analysis of different variations of the Playfair cipher that have been proposed by several authors. These variations suggest diverse strategies for enhancing the cipher's security and effectiveness, which has undergone several modifications over time. By studying these improvements, we can gain insights into the strengths and weaknesses of the Playfair cipher and explore ways to enhance it further. This analysis can be valuable in reinforcing current cryptographic systems and ensuring the confidentiality of sensitive information.

Table 1. Comparative analysis

Ref	Encryption technique	Complexity	Avalanche effect	Drawbacks
[11]	4×19 playfair matrix and RSA for encryption, RMPS keyless transposition followed by LSB steganography	Medium (Matrix size is 4×19, so a little slower as compared to traditional 5×5. The usage of RSA, steganography and RMPS keyless transposition adds to the complexity)	Weak (< 50%)	Can be broken by Man-in-the-middle attack as standard RSA is used risking the security of the public Key
[10]	Encryption using 5×5 playfair cipher method followed by LSB steganography	Medium (In Comparision to 16×16 matrix it will be fast but all characters won't be included)	Weak (MSE < 30 dB)	i) Large overhead to hide a very tiny amount of information using LSB. ii) When embedding the message in more than one LSB, the image quality may decrease depending on how many pixels are changed. So it is not robust.
[9]	3D $4 \times 4 \times 4$ matrix is used for encryption, size is reduced by altering 8 digit ASCII code's binary form to it's corresponding 6 digit form followed by PVD steganography to conceal the message.	High (Lengthy algorithm that involves encoding using 3D $4 \times 4 \times 4$ matrix, compression followed by hiding)	Weak (MSE < 30 dB)	i) Might be computationally complex ii) PVD displays a greater disparity between the original pixel values of the image allowing for more alteration.
[8]	Using two cross-chaotic maps a 16×16 Playfair matrix is produced. Image is divided into numerous blocks of size 16×16 bytes each which is encrypted using different playfair matrices.	High (Chaotic system is used for generating 16×16 byte playfair matrix corresponding to each image block)	Strong (The values of NPCR & UACI are in proximity to the optimal values.)	i) Original message cannot be retrieved from the enciphered text in many cases ii) Third party can access the information in the arrays, in case they get the algorithm. iii)Unless cipher text and plain text are in the same row or column they have a reciprocal relationship.
[7]	Use of 16×16 cipher matrix, XOR operations, two's complement followed by bit swapping	Medium (Improved performance significantly and processing time of the algorithm is linearly proportional)	Strong (around 53.7% on an average)	The proposed playfair cipher algorithm might not be highly optimised for implementation in software applications

Table 2. Analysis of different types of attacks on the modified playfair algorithm

Ref.	Brute force attack	Frequency analysis attack
[11]	Very difficult to carry out(Key domain size is 73! which is a very large number)	Although difficult but can be broken (Chance of occurrence is 0.013 as compared to 0.0385 in traditional cipher which is a significant improvement)
[10]	Can be broken(Key domain size is 25! Which is less than 2ˆ128)	Weak resistance. Can be deciphered using modern techniques
[9]	Difficult as the attacker must find in 4096($64 \times 16 \times 4$) trigraphs	A character's likelihood of appearing in 3D Playfair matrix is $1/16 \times 1/4 = 1/64(0.0156)$. Thus frequency analysis attack is difficult to carry out but chance of attack still persists
[8]	Might be regarded to be safe from brute force attack because of the large size of search space: $256 \times 256 = 65{,}536$	The likelihood of occurence is 0.0039(1/256) which is comparatively less when compared to traditional cipher making frequency analysis a more durable employment.
[7]	Good resistance (estimated 43.2 billion years required to crack a key containing 10 characters)	Randomness analysis of the algorithm indicated that the binary sequence is arbitrary. Thus difficult to decipher by analyzing the frequency of zeroes and ones [14]

5 Conclusion

After analysing different kinds of modification to Playfair Cipher, we came to conclusion that their security is not too high but can be employed in specific circumstances due to easy and low cost implementation. Playfair Cipher was in wide use during ancient period but due to increasing security requirements it became easily breach-able and thus unfit to use. We analysed few of the modifications to the Playfair cipher proposed in the last few years to strengthen it. The modified versions can be used in certain implementations due to their increased performance and low cost implementation thus, making it employable in modern day scenario.

References

1. Pandey, M., Dubey, M.: Survey paper: cryptography the art of hiding information. Int. J. Comput. Eng. Technol. **2**, 3168–3171 (2013)
2. Chhabra, P.: A survey on classic cipher in cryptography. Int. J. Innov. Res. Sci. Eng. Technol. **6** (2017). https://doi.org/10.15680/IJIRSET.2017.0605020
3. Rahman, M.N.A., Abidin, A., Yusof, M.K., Usop, N.: Cryptography: a new approach of classical hill cipher. Int. J. Secur. Appl. **7**(2), 179–190 (2013)
4. Majumder, R., Datta, S., Roy, M.: An enhanced cryptosystem based on modified classical ciphers. In: 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), vol. 1, pp. 692–696 (2022). https://doi.org/10.1109/ICACCS54159.2022.9785033
5. Ahmad, J., Ahmed, F.: Efficiency analysis and security evaluation of image encryption schemes. IJENS **12**, 18–31 (2012)

6. Deepthi, R.: A survey paper on playfair cipher and its variants. Int. Res. J. Eng. Technol. **4**, 2607–2610 (2017)
7. Marzan, R.M., Sison, A.M.: An enhanced key security of playfair cipher algorithm. In: ICSCA 2019: Proceedings of the 2019 8th International Conference on Software and Computer Applications, pp. 457–461 (2019). https://doi.org/10.1145/3316615.3316689
8. Albahrani, E.A., Maryoosh, A.A., Lafta, S.H.: Block image encryption based on modified playfair and chaotic system. J. Inf. Secur. Appl. **51**, 102445 (2020). https://doi.org/10.1016/j.jisa.2019.102445
9. Kaur, G., Verma, H., Singh, R.: Dual steganography approach using 3D playfair cipher and pixel value differencing method. SSRN Electron. J. (2020). https://doi.org/10.2139/ssrn.3526694
10. Siswanto, A., Wahyuni, S., Arta, Y.: Combination playfair cipher algorithm and LSB steganography for data text protection, pp. 125–129 (2019). https://doi.org/10.5220/0009144501250129
11. Patil, R., Chaudhari, P.R., Dindorkar, M.R., Bang, S.V., Bangar, R.B.: Improved cryptography by applying transposition on modified playfair algorithm followed by steganography (2021)
12. Kshiteesh, R.B., Koundinya, U.R., Varun, R., Ajina, A., Prathima, G.: A review on challenges and latest trends on cyber security using text cryptography. In: Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication and Security (ICIIC 2021), pp. 194–201 (2021). https://doi.org/10.2991/ahis.k.210913.024
13. Ahmed, N., Asif, H., Saleem, G.: A benchmark for performance evaluation and security assessment of image encryption schemes. Int. J. Comput. Netw. Inf. Secur. **8**, 18–29 (2016). https://doi.org/10.5815/ijcnis.2016.12.03
14. Marzan, R.M., Sison, A.M., Medina, R.P.: Randomness analysis on enhanced key security of playfair cipher algorithm. Int. J. Adv. Trends Comput. Sci. Eng. 1248–1253 (2019). https://doi.org/10.30534/ijatcse/2019/34842019
15. Modupe, A., Adedoyin, A., Titilayo, A.: A comparative analysis of LSB, MSB and PVD based image steganography. Int. J. Res. Rev. **8**, 373–377 (2021). https://doi.org/10.52403/ijrr.20210948
16. Wang, Y.: A classical cipher-playfair cipher and its improved versions. In: 2021 International Conference on Electronic Information Engineering and Computer Science (EIECS), pp. 123–126 (2021). https://doi.org/10.1109/EIECS53707.2021.9587989
17. Rajeswari, S., Ramya, N., Saranya, K.: Avalanche effect based variants of playfair cipher for data security. Int. J. P2P Netw. Trends Technol. (2017)
18. Tunga, H., Mukherjee, S.: A new modified playfair algorithm based on frequency analysis. Int. J. Emerg. Technol. Adv. Eng. **2** (2012)
19. Yadav, M., Dhankhar, A.: A review on image steganography. Int. J. Innov. Res. Sci. Technol. **2**, 243–248 (2015)
20. Oladipupo, E.T., Abikoye, O.C.: Modified playfair cryptosystem for improved data security. Comput. Sci. Inf. Technol. **3**, 51–64 (2022). https://doi.org/10.11591/csit.v3i1.p51-64
21. Hamad, S., Khalifa, A., Elhadad, A., Rida, S.: A modified playfair cipher for encrypting digital images. J. Commun. Comput. Eng. **3**, 1 (2014). https://doi.org/10.20454/jcce.2013.731
22. Shakil, T., Islam, M.: An efficient modification to playfair cipher. ULAB J. Sci. Eng. **5**, 26 (2014)

23. Sankpal, P.R., Vijaya, P.A.: Image encryption using chaotic maps: a survey. In: 2014 Fifth International Conference on Signal and Image Processing, pp. 102–107 (2014). https://doi.org/10.1109/ICSIP.2014.80
24. Salunkhe, J., Sirsikar, S.: Pixel value differencing a steganographic method: a survey. Int. J. Comput. Appl. **975**, 8887 (2013)
25. Mathur, S.K., Srivastava, S.: Extended 16x16 play-fair algorithm for secure key exchange using RSA algorithm. Int. J. Future Revolution Comput. Sci. Commun. Eng. **4** (2018)
26. Anshari, M., Mujahidah, A.: Expending technique cryptography for plaintext messages by modifying playfair cipher algorithm with matrix 5 x 19. In: 2019 International Conference on Electrical Engineering and Computer Science (ICECOS), pp. 10–13 (2019). https://doi.org/10.1109/ICECOS47637.2019.8984560
27. Ahmed, A.M., Ahmed, S.H., Ahmed, O.H.: Enhancing 3D-playfair algorithm to support all the existing characters and increase the resistanceto brute force and frequency analysis attacks. In: 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT), pp. 81–85 (2017). https://doi.org/10.1109/CRCSIT.2017.7965538
28. Liu, L., Wang, J.: A cluster of 1D quadratic chaotic map and its applications in image encryption. Math. Comput. Simul. **204**, 89–114 (2023). https://doi.org/10.1016/j.matcom.2022.07.030
29. Sai D, J., Krishnaraj P, M.: Cryptographic interweaving of messages. Int. J. Data Inform. Intell. Comput. **2**(1), 42–50 (2023). https://doi.org/10.5281/zenodo.7766607