Enhancing Communication Using 8 × 8 Extended Playfair Cipher and Steganography

Akshay Sharma [1], Nitin Gupta [1], Anurag Thakur [1], Karan Guleri [1], and Muskan Dhiman [1]

[1]Affiliation not available

October 30, 2023

Abstract

In this world of communication, the security of the

messages to be transferred plays a very important role. Strategies like Encryption/Decryption, Digital Signatures, Steganography etc., have been developed to ensure the security, privacy and integrity of these messages. Playfair cipher is one of the well known polyalphabetic ciphers used for the encryption and decryption. However in account of few drawbacks inherent in existing 5*5 playfair cipher, recently improved version of Playfair cipher i.e., Extended 8*8 Playfair cipher has been developed. In this work, extended playfair cipher with Least Significant bit steganography are applied to hide the presence of any such messages. The main objective of this work is to build a secure mechanism of sending and receiving messages. The results show that combination of both extended 8 * 8 playfair cipher and stegnography increases the security of messages in contrast to the existing traditional Playfair ciphers.

Enhancing Communication Using 8×8 Extended Playfair Cipher and Steganography

Akshay Sharma, Nitin Gupta, *Senior Member IEEE*, Anurag Thakur, Karan Guleri and Muskan Dhiman
Department of Computer Science and Engineering,
National Institute of Technology Hamirpur
Himachal Pradesh, India
Email: {newakshaysharma, nitin3041, ranaanurag67, karanguleri.kd, muskandhiman97}@gmail.com

***Abstract*—In this world of communication, the security of the messages to be transferred plays a very important role. Strategies like Encryption/Decryption, Digital Signatures, Steganography etc., have been developed to ensure the security, privacy and integrity of these messages. Playfair cipher is one of the well known polyalphabetic ciphers used for the encryption and decryption. However in account of few drawbacks inherent in existing 5×5 playfair cipher, recently improved version of Playfair cipher i.e., Extended 8×8 Playfair cipher has been developed. In this work, extended playfair cipher with Least Significant bit steganography are applied to hide the presence of any such messages. The main objective of this work is to build a secure mechanism of sending and receiving messages. The results show that combination of both extended 8×8 playfair cipher and stegnography increases the security of messages in contrast to the existing traditional Playfair ciphers.**

***Index Terms*—Cryptography, Steganography, Ciphers, encryption, decryption, playfair cipher, polyalphabetic.**

I. Introduction

The field of information security has been seen evolving in the past recent years. Data sent from one place to another can be intercepted at any time of transmission. Hence, it becomes open for any kind of malevolent action. To protect this data, techniques like Cryptography- Changing of data to unrecognizable format and retrieving it back and Steganography- Hiding the presence of any data, have been developed [1]. An algorithm used for performing encryption and decryption is known as cipher. Further, 5×5 playfair cipher is one of the polyalphabetic ciphers which uses matrix for encryption and decryption of texts containing alphabets only [2], [3]. This cipher uses five different letters that can be substituted for each letter. However it has its own shortcomings like numeric values and special characters cannot be encrypted and it also does not exploit spacing between the words. Therefore, not only its cryptanalysis becomes a bit easy but also at the time of decryption some assumptions has to be made which have the probability of getting wrong results. To overcome these demerits, 8×8 extended playfair cipher (EPC) is used in this work [4], [5].

EPC is the modified version of a playfair cipher which overcomes drawbacks and loopholes of 5×5 playfair cipher. It was shown that this cipher can handle various kinds of attacks [6], [7]. Detailed EPC is explained in Section III. The EPC uses different blocks for numerals, alphabet and symbols. Rules for encoding and then decoding are similar to the existing playfair cipher. In EPC, two matrices alternatively are used for encoding of the digraph (pairs of two) and this work also uses the Rail-fence cipher [8] in the end to get the final ciphertext.

Steganography is the method to hide a communication by encapsulating information in the other information. In the proposed work, the Least Significant Bit (LSB) Steganography [9] is applied to hide the ciphertext by an image. In this method the LSB of an image is replaced by bits of the desired confidential message. This is done to keep the encrypted message out of sight of the attackers. Basically, the very essence of a message being transferred is made hidden which adds to its security level.

Data security has become of prime importance in today's world. We are constantly communicating data with each other through the internet and the messaging applications. Sent messages if not secured properly can be intercepted or modified by a third party at any time of transmission, which can lead to the loss of privacy. Confidentiality in communication is the need of the hour. In the proposed work, the main objective is to increase the security level of the communication by combination of EPC and LSB steganography. It not only increases the security of transmitted data but also removes weaknesses of current ciphers and security techniques. The results show the validity of the proposed method.

Rest of the paper is organized as follows. In the next section related work is discussed. In section III the EPC is explained. In the section IV and V the proposed method is discussed followed by the results and discussion.

II. Related Work

In the recent times, various ways to secure message delivery have been developed. Putera et al. in [10] implemented a Super Playfair and two square cipher algorithms to secure the messages. The proposed Super Playfair cipher is a modification of the traditional playfair cipher, wherein, after encrypting each digraph of the message, a square change is made to the key. After encrypting with Super Playfair cipher, two Square cipher algorithm is used for transposition of the cipher text. This method of encryption is proposed to be applied for messaging applications on the android platform.

Authors in [11] combined steganography and cryptography on android platform to achieve a high-level security. Authors performed cryptography with a combination of steganogaphy with other cipher to increase the security of encryption. In this paper, various problems and challenges that may arise in the development of the application on android have been discussed and the solutions are also provided. The work discusses the various possibilities of experimenting with the combination and how they can be used in smart phones. Anil Kumar and Rohini Sharma [12] in their work, proposed to use steganography for encrypting the data in such a way that only sender and receiver can decrypt the information. No one else except receiver can access the information. In this work authors defined various techniques for steganography like Hash- LSB with RSA (Rivest–Shamir–Adleman) algorithm. In this technique the data is encrypted firstly and then embedded behind the image. In case if encrypted data is revealed even then only receiver can access the data.

Authors in [13] proposed an image steganography framework known as adaptive stego key LSB (ASK-LSB). The authors proposed to improve the data-hiding algorithm in cover images by maintaining the Peak Signal-to-Noise Ratio of the steganography framework. The work is based on a LSB substitution method, encryption and combination random function method. The secret bits are inserted directly or inversely, enhancing the the process of embedding.

Recently researchers have used the EPC than the traditional playfair cipher as it uses alphabets and numerals along with some frequently used special symbols. Various modifications have done to 8×8 playfair cipher. Gaurav et al. in [14] proposed a modified version of the cipher. In each round during encryption, the positions of the columns are changed. The resultant ciphertext makes identification of digraphs difficult and also makes cryptanalysis difficult. In other work authors [15] proposed a 8x8 cipher that is coupled with LSR (Linear shift register) to make the traditional playfair cipher as strong as DES or AES. The paper also discusses the various security aspects of the proposed technique. It discusses the various attacks that are possible and how they are countered. This paper also showed that this type of approach is useful in areas with low bandwidth or very less memory.

Ouday Nidhal et al. [16] proposed an advancement of playfair cipher in which the 5×5 matrix is replaced by a 11×11 matrix to support all the 26 alphabets in both upper case letters as well as lower case letters. Further it also support all the numeric digits, special characters and the extended special characters. They also suggested setting the cipher text of a playfair cipher as input to the complete procedure of a cascade LFSR to get the final cipher text. However by including the white space the cipher becomes weak as it becomes easier for the cryptanalyst to decipher the cipher text. Moreover, encryption and decryption process takes more time due to LFSR. Swati Hans et al. in [17], proposed an advancement of playfair cipher in which the original 5×5 matrix is coupled with a random pattern generator method. They suggested swapping the order of rows and columns using patterns sequence of ten digits containing decimal numbers 1-5, like 1234525314. However the limitations that were existing in original playfair cipher still persist.

Verma et al. [18] proposed an advancement of the playfair cipher in which the $5\times$ 5 matrix is replaced by a $4 \times 4 \times 4$ three dimensional matrix to accommodate 64 characters that include all the uppercase 26 alphabets, 10 numeric digits and 28 special symbols. However lowercase alphabets cannot be handled and the diagraph formed consists of three characters. S.S.Dhenakaran and M. Ilayaraja in [19] replaced the 5×5 matrix by a 16×16 matrix to accommodate all the possible ASCII characters in ascending order of their values (0-255). However by increasing the size of matrix by huge amount, the time increases to construct the key matrix and substituting characters from it.

Authors in [20] implemented a novel Rail fence Cryptography for securing the information, where plaintext is encrypted by arranging it in a zigzag pattern in an empty matrix whose number of rows acts as a key. Based on this key, encryption and decryption is done but it alone is not efficient enough to protect the data as it can easily be broken by brute-force attack. This disadvantage can be overcome if it is combined with another technique or modify the table by changing the trajectory.

All the above mentioned techniques poses some advantages and disadvantages. In this work cryptography and LSB setganography techniques are combined to get the added benefits and reduce the disadvantages.

III. Introduction to the Extended Playfair Cipher

The traditional playfair cipher does not take numerals, symbols into account. The modified version of the playfair cipher uses 8×8 matrix including all the alphabets $(A-Z)$, numerals $(0-9)$ and 28 special symbols that were selected based on their frequency analysis. Unlike the traditional playfair cipher, all alphabets are considered individually, like E/F are not considered the same. The space between the words is also shown at the time of encryption by the symbol 'l'. For the repeated characters or plaintext with odd length, ˆ is appended at the end of the message. The keyword is entered into the 8×8 matrix first, without repeating any alphabet, number or symbol and then the remaining characters are entered to form 8×8 matrix, which becomes the key. The Table I shows the list of characters used in the EPC.

TABLE I
LIST OF CHARACTERS USED IN EXTENDED PLAYFAIR CIPHER

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	0	1	2	3	4	5
6	7	8	9	!	@	#	$
%	ˆ	&	*	(	)	_	+
=	{	}	[	]	|	\	:
;	”	’	<	>	.	/	?

The encryption for the EPC is same as the traditional playfair cipher. The message is first divided into digraphs and

encrypted one pair at a time. The rules for encryption are:

a) If both the characters of the digraph are in the same column of the key matrix, they are replaced by the letter immediately below them.
b) If both the characters of the digraph are in the same row, they are replaced by the one immediately right to them.
c) If they are in different row and columns, and form a rectangle, the characters on the horizontal opposite of the rectangle replace the characters.

Example of message encryption using the EPC is shown in the Appendix.

IV. Proposed Approach

Although, the EPC removes the limitations of using characters, it still suffers from the same weaknesses as playfair cipher. Brute force for the extended playfair is even harder, as it has 64! possible key combinations. However, as it follows the same rules as playfair, the reverse of a digraph will give the same pattern of characters, which makes cryptanalysis not so difficult. The average frequency of digraphs in the English language can tell about most used digraphs, and using hit and trial one may arrive at a result. Hence to overcome the limitations, this work proposes the Modified EPC.

The modified playfair cipher is a combination of playfair cipher substitution and transposition. When the rows or columns of the key matrix are rotated, it does not affect the result of the cipher. However, if the transpose of the rows is taken, it give an entirely different result. For the modified encryption technique, two key matrices KeyMatrix1 and KeyMatrix2 are considered, where KeyMatrix1 is the original key matrix and KeyMatrix2 is the transpose of the KeyMatrix1. Then the message is divided into digraphs, on the digraphs at odd positions playfair using KeyMatrix1 is performed and on digraphs at even positions playfair cipher using KeyMatrix2 is executed.

After playfair substitution, transposition on the ciphertext is done. To perform this task, the railfence cipher [8] with a key of 3 for jumbling the ciphertext is used. In a transposition cipher, the order of the alphabets is re-arranged to obtain the cipher-text as follows:

a) The plain-text is written downwards and diagonally on the successive rails of an imaginary fence.
b) When the bottom rail is reached, then traverse upwards moving diagonally. After reaching the top rail, the direction is changed again. Thus the alphabets of the message are written in a zig-zag manner.
c) After each alphabet is written, the individual rows are combined to obtain the cipher-text.

The railfence cipher with key 3 adds difficulty in the decryption process. It also adds diffusion in the cipher, which disturbs the statistical properties of the message and makes the statistical analysis difficult. The railfence cipher can be explained with the following example. Given the word 'MONALISA', railfence cipher carries out transposition as follows:

The table II shows the process of railfence cipher implementation. The resultant ciphertext is generated by reading the alphabets row by row, which is MLOAIANS. By using railfence cipher the already encrypted message has become even more meaningless.

TABLE II
RAILFENCE CIPHER

M				L			
	O		A		I		A
		N				S	

Let's assume that the keyword is 'NIT@123'. The keyword is inserted into the 8×8 matrix and the rest of the cells are filled with the remaining characters. The key obtained here is KEY 1. The transpose of this key is KEY 2. The table III and table IV shows KEY 1 and KEY 2 respectively.

TABLE III
KEY 1

N	I	T	@	1	2	3	A
B	C	D	E	F	G	H	J
K	L	M	O	P	Q	R	S
U	V	W	X	Y	Z	0	4
5	6	7	8	9	!	#	$
%	^	&	*	(	)	_	+
=	{	}	[	]	|	\	:
;	"	'	<	>	.	/	?

TABLE IV
KEY 2

N	B	K	U	5	%	=	;
I	C	L	V	6	^	{	"
T	D	M	W	7	&	}	'
@	E	O	X	8	*	[	<
1	F	P	Y	9	(	]	>
2	G	Q	Z	!	)	|	.
3	H	R	0	#	_	\	/
A	J	S	4	$	+	:	?

A. Encryption Process

The flowchart in figure 1 shows the complete encryption process. The encryption process consists of adding '|' character for every blank space and '^' between the repeated characters. Then the message is converted into the digraphs, which are encrypted using the same rules as EPC. Then railfence cipher is performed for transposition of the message.

Let us take an example. Let the message to be encrypted is "WELCOME TO NIT123". This message is first converted to an acceptable format: WELCOME|TO |NIT123. Then, it is divided into digraphs:

WE LC OM E|TO |N IT 12 3^

Now, KEY 1 and KEY 2 are used alternately to encrypt these digraphs. 'WE' is encrypted using KEY 1 and gives the result as 'XD'. Then 'LC' is encrypted using KEY 2, and gives the result as 'VL'. Similarly, the ciphertext will be :

XD VL PO [G @M =2 T@ 23 I-

Now the railfence is applied on the ciphertext just obtained, the result is: XP@TIDLOGM2@3-V[=2

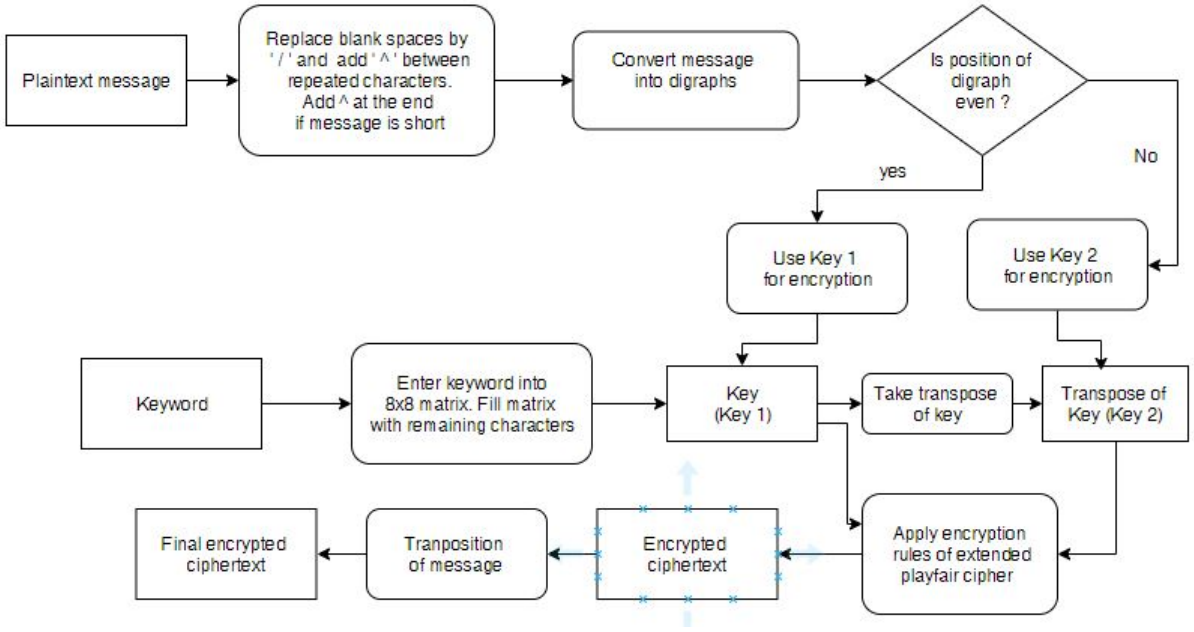

Fig. 1. Flow chart showing encryption of message

It can be observed that the ciphertext before and after transposition has become more jumbled and difficult to find a pattern to decipher.

B. Decryption process

For the decryption process, the reverse of encryption is followed. First, the ciphertext from LSB bits of each pixel is generated. Then, the railfence cipher is applied in reverse. After the ciphertext is obtained, it is divided into the digraphs. The key matrix of 8×8 and its transpose are used for decryption of alternate digraphs. These are fed into the Extended Playfair decryption algorithm to get the original message. The flow chart in figure 2 explains the entire decryption process. Further, in the flow chart in figure 2 the few steps of steganography explained in the next section are also included.

V. Combining Playfair Cipher and Steganography

Cryptography enables us to hide the meaning behind the message by converting it into gibberish. It is one of the effective ways to ensure confidentiality while communication. However, steganography is an even more effective way of communication, since it hides the existence of the message itself without drawing any attention from attackers. A combination of cryptography and steganogaphy can prove to be very effective, since it introduces an added level of difficulty while trying to decrypt the message. Even if the attacker is aware of the presence of steganography, and is successful in acquiring the message, he still needs to decipher that message. Thus, this method can be used for highly secure communications.

A. Steganography algorithm

In this work LSB Steganography is considered, which replaces the LSBs of the pixels in the image with the binary bits of the message. This does not destroy the integrity of the image in any way, since the lowest bits in an image contribute the least in its pixel value. First, the message is converted into binary where each character is converted into its ASCII value. Then this binary form is converted to its 8-bit binary equivalent. The image is read pixel by pixel, and the LSBs of the pixel is replaced by the string of bits.

1) Encoding data: Each pixel has 3-values, (Red, Green and Blue)and is made of 3-Bytes (one-byte per value). Once the data has been encoded into the 8-bit ASCII value, 3 pixels are read at a time. These 3 pixels have a total of 9 values. The bit values in the first 8 values (each of 8-bit) is changed by the encoded data bit. The value of the pixel is made odd, if bit value is 0, otherwise it is made even. The process of changing the pixel into either odd or even is done by adding 1 to the pixel value. This ensures that a situation is never encountered where the pixel value is negative (-1). If after adding the pixel value goes out of bound , the mod is taken of the value with 255. The flowchart in figure 3 shows the entire encryption process.

Let's consider that the message needs to be hidden is 'YES'. When converted to the ASCII values, it will be 896983. After converting them into binary stream, they will give 010110010100010101010011. Let the pixel values for a 4×3 image is as follows:

[(27, 64, 164), (248, 244, 194), (174, 246, 250), (149, 95, 232), (188, 156, 169), (71, 167, 127), (132, 173, 97), (113, 69, 206),(255, 29, 213), (53, 153, 220), (246, 225, 229), (142, 82, 175)]

Each bit of the binary stream will change the bits of the first 8 values of the 3 pixels it reads. If there is more data to be written in the image, the last value is made even, otherwise it

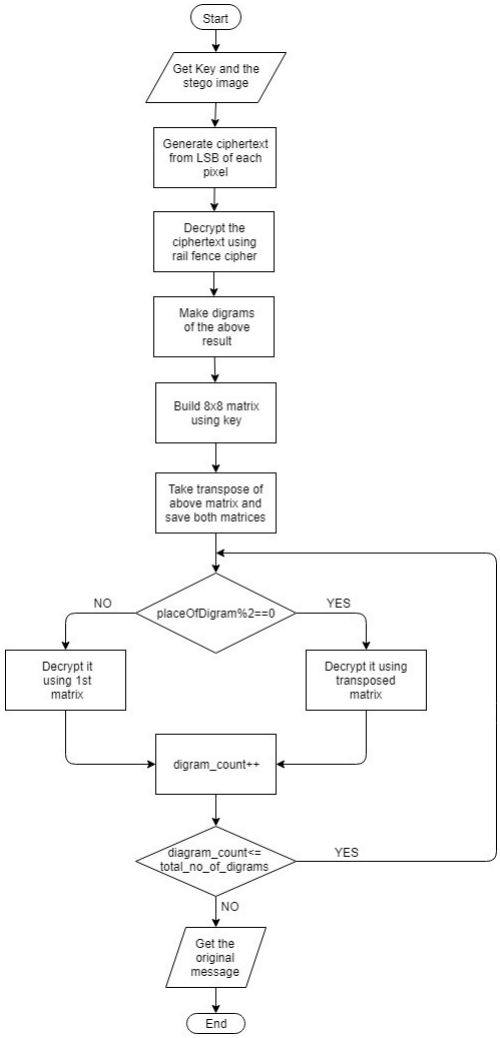

Fig. 2. Flow chart showing decryption of message

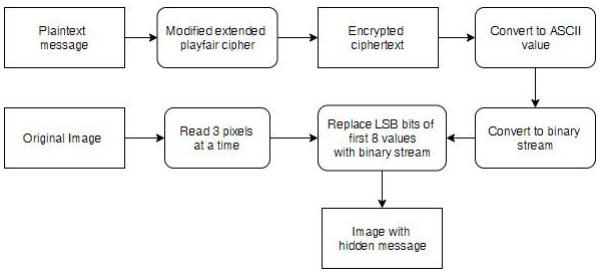

Fig. 3. Flow chart showing encryption of message

is made odd by adding 1. Here, after encryption, the resulting values of the pixels will be:

[(28, 65, 164), (249, 245, 194), (174, 247, 250), (150, 95, 232), (188, 156, 169), (72, 167, 128), (132, 173, 98), (113, 70, 206),(255, 29, 213), (53, 153, 220), (246, 225, 229), (142, 82, 175)]

2) Decoding data: For decoding the image, the pixels of the image are read 3 at a time, till an odd value is encountered in the last value. If the value of the pixel is odd, value of the bit is 0 otherwise it is 1. When the pixel value is even, the value of bit is 0, otherwise it is 1. This binary stream is converted into ASCII values. The ASCII value is converted to characters. Thus, the ciphertext is obtained. This is given to the modified extended playfair decryption. The output is the original plain text.

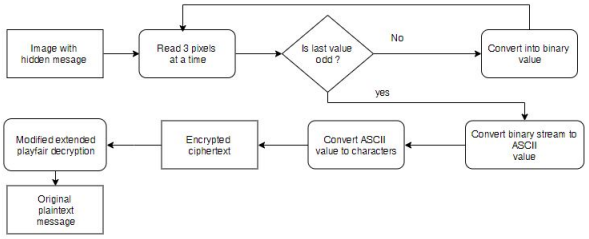

Fig. 4. Flow chart showing decryption of message

The flowchart in figure 4 shows the entire process of decoding data. Further, Encoding is done at the sending end whereas decoding is done at the receiving end.

VI. Cryptanalysis

Firstly, steganography will make it difficult for attackers to realise that a message is being passed. Further, if he is somehow able to detect that a stego image is being passed then it would be difficult for him to recognise the real ciphertext in sense that which bits of pixels are used for encoding the message into the picture.

Even after attacker is able to detect the ciphertext it would be very difficult for him to decrypt it. Due to the diffusion and confusion in the ciphertext caused by rail fence cipher, finding the real ciphertext, upon which playfair cipher is to be applied, becomes very difficult. As there can be many possible combination on the basis of key. This makes difficult to produce digraphs which are very essential for decryption process. Without it decryption cannot start.

Once the digraphs are obtained, firstly a matrix using some key is required which is used for decryption of oddly placed diagrams and its transposed matrix is required for decryption of evenly placed digraphs. In traditional playfair cipher, $26 \times 26 = 676$ different digraphs were possible. However in the extended 8×8 matrix, $64 \times 64 = 4096$ different digraphs are possible. For the same letter, there can be 16 possible substitutes i.e., 8 from each matrix. For each of these possible digraphs, there exists $(64!)$ Matrices i.e., in total $4096 \times (64!) = 10^{93} \approx= 2^{310}$ combinations has to be tried after the intermediate ciphertext. However obtaining this intermediate ciphertext itself is a difficult task and this technique of encryption using two matrices of 8×8 makes decryption even further more difficult. Therefore, it can be concluded that cryptanalytic attack is difficult for the proposed system.

VII. Conclusion

In this paper, the objective is to secure the communication by combining cryptography and steganography. First an extended 8×8 matrix is used and then finally rail fence cipher is used which increases the diffusion and confusion of intermediate ciphertext generated. The final ciphertext is then more dispersed by using steganography by which the very notion of message being transferred is made hidden from the attackers and also it can withstand any kind of cryptanalytic attacks. As a result, high level of security is achieved by this method with securing multiple times that of normal traditional playfair cipher and it would be very effective for areas having low bandwidth or very less memory storage.

Appendix

Let's assume the keyword MONALISA123. The message is "HELLOXYZ". This message will be divided into digraphs as HE Lˆ LO XY Zˆ
The key formed for the keyword is shown in Table V

M	O	N	A	L	I	S	1
2	3	B	C	D	E	F	G
H	J	K	P	Q	R	T	U
V	W	X	Y	Z	0	4	5
6	7	8	9	!	@	#	$
%	ˆ	&	*	(	)	_	+
=	{	}	[	]	—	\	:
;	”	’	<	>	.	/	?

TABLE V
KEY FOR KEYWORD "MONALISA123"

A. Encryption Process

For digraph 'HE', both H and E are in different row and columns. They map to the corners of the rectangle they form. Thus, they encrypt to 'R2'. Similarly, 'Lˆ' encrypts to '0('. For 'XY', since both 'X' and 'Y' lie in the same row, they map to the character to its right, i.e., 'YZ'. The ciphertext will be: R2 O(IN YZ W(

B. Decryption Process

For the decryption purposes, since playfair cipher is a symmetric cipher, the key will be present with both the sender and the receiver. To decrypt the message, the ciphertext is divided into digraphs. The same rules as applied with encryption are applied to the ciphertext using the key matrix. For example, the ciphertext obtained was R2O(INYZW(. This is divided into digraphs : R2 O(IN YZ W(. When EPC is performed on the digraphs, the original message will be back : HELLOXYZ.

References

[1] O. Goldreich, "On the foundations of cryptography," in *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, 2019, pp. 411–496.

[2] S. S. Srivastava, N. Gupta, S. Chturvedi, and S. Ghosh, "A survey on mobile agent based intrusion detection system," in *International Symposium on Devices MEMS, Intelligent Systems & Communication (ISDMISC)*, 2011.

[3] S. S. Srivastava and N. Gupta, "A novel approach to security using extended playfair cipher," *International Journal of Computer Applications*, vol. 20, no. 6, pp. 0975–8887, 2011.

[4] S. Hamad, "Novel implementation of an extended 8x8 playfair cipher using interweaving on dna-encoded data." *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 4, no. 1, 2014.

[5] S. S. Srivastava and N. Gupta, "Optimization and analysis of the extended playfair cipher," in *2011 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*. IEEE, 2011, pp. 267–270.

[6] P. Goyal, G. Sharma, and S. S. Kushwah, "Network security: A survey paper on playfair cipher and its variants," *Int. J. Urban Des. Ubiquitous Comput*, vol. 3, no. 1, p. 9, 2015.

[7] S. S. Srivastava and N. Gupta, "Security aspects of the extended playfair cipher," in *2011 International Conference on Communication Systems and Network Technologies*. IEEE, 2011, pp. 144–147.

[8] A. Banerjee, M. Hasan, and H. Kafle, "Secure cryptosystem using randomized rail fence cipher for mobile devices," in *Intelligent Computing-Proceedings of the Computing Conference*. Springer, 2019, pp. 737–750.

[9] S. Gupta, A. Goyal, and B. Bhushan, "Information hiding using least significant bit steganography and cryptography," *International Journal of Modern Education and Computer Science*, vol. 4, no. 6, p. 27, 2012.

[10] A. Putera Utama Siahaan, M. Mesran, and I. Solihin, "Implementation of super playfair in messaging," in *Proceedings of the Joint Workshop KO2PI and the 1st International Conference on Advance & Scientific Innovation*. ICST (Institute for Computer Sciences, Social-Informatics and ..., 2018, pp. 109–118.

[11] S. H. Ahmed, A. M. Ahmed, and O. H. Ahmed, "Combining steganography and cryptography on android platform to achive a high-level security," *Journal of Engineering & Applied Sciences*, vol. 12, no. 17, pp. 4448–4452, 2017.

[12] A. Kumar and R. Sharma, "A secure image steganography based on rsa algorithm and hash-lsb technique," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 7, pp. 363–372, 2013.

[13] M. N. Srayyih Almaliki, "Multilevel secure digital image steganography framework using random function and advanced encryption standard," *Journal of Computational and Theoretical Nanoscience*, vol. 16, no. 11, pp. 4812–4825, 2019.

[14] G. Shrivastava, M. Chouhan, and M. Dhawan, "A modified version of extended plafair cipher (8x8)," *International Journal Of Engineering And Computer Science*, vol. 2, no. 956-961, 2013.

[15] S. S. Srivastava, N. Gupta, and R. Jaiswal, "Modified version of playfair cipher by using 8x8 matrix and random number generation," in *IEEE 3rd International Conference on Computer Modeling and Simulation*, 2011, pp. 615–617.

[16] O. N. A. Hanosh and B. Salim, "11× 11 playfair cipher based on a cascade of lfsrs," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 29-35, p. 11, 2013.

[17] S. Hans, R. Johari, and V. Gautam, "An extended playfair cipher using rotation and random swap patterns," in *2014 International Conference on Computer and Communication Technology (ICCCT)*. IEEE, 2014, pp. 157–160.

[18] V. Verma, D. Kaur, R. K. Singh, and A. Kaur, "3d-playfair cipher with additional bitwise operation," in *IEEE International Conference on Control, Computing, Communication and Materials (ICCCCM)*, 2013, pp. 1–6.

[19] S. Dhenakaran and M. Ilayaraja, "Extension of playfair cipher using 16x16 matrix," *International Journal of Computer Applications*, vol. 48, no. 7, 2012.

[20] A. P. U. Siahaan, "Rail-fence-cryptography-in-securing-information," *INA-Rxiv*, 2017.