A Steganographic Apps-based Patient's Information Encryption-Decryption

Shomitro Kumar Ghosh, Md. Toheen Bhuiyan, Md. Ismail Jabiullah

Abstract: ***A steganographic apps-based patient's information communication system has been designed, developed and implemented in Java programming language that can hide patient confidential data in an image. The Playfair cipher encryption-decryption technique with a set of keywords has been used in this transaction system. For this, the patient's information is first encrypted with the Playfair encryption technique and produces the cipher text that are embedded with an image in a hidden format and then the image is sent to the destination. In the receiving end, the encrypted hidden information is extracted and retrieve the information by using the reverse process. The process has been applied on several patient's information and steganographic images and found the results successfully. This proposed steganographic process is a higher layer of security methods in the communications and can be applied where high security is needed.***

Index Terms: Steganography, Playfair Cipher, Image Steganography, Secret Communication.

I. INTRODUCTION

In a secured electronic communication, steganography is the science of information hiding in an image. It allows the communicants to transact secret information. In this current era of communication, steganography plays a role of influence in the secret electronic transactions in a completely undetectable manner. In a steganography system, there are observed three main issues and they are imperceptibility, capacity and undetectable [1].

Steganography techniques is the process of writing text of data, information on an image in a secret manner by using cryptographic applications that is to be undetected until the data is retrieved in reverse process [2]. Cryptography is the art of scrambling message to make it difficult to understand whereas steganography is the art of hiding information to make it difficult to find [13], [4]. Here, both of the methods are combined to propose and implement a system of secured information communication system that can be applied on sensitive information transactions.

The cryptographic method Playfair cipher generation process is based on the use of a set of letters in the matrix form constructed by using a keyword [5]. Here a keyword is a word without repeating characters. KEYWORD, MONARCHY, COMPUTER are some examples of keywords. This method can only allow the text that contains only alphabets in the plaintext. The Playfair cipher generation process is based on using a 5 x 5 matrix of letters made up of using the letters of the keyword [6], [7]. In this technique, a keyword 'COMPUTER' is used, the matrix is constructed by filling the letters of the keyword from left to right and top to bottom and then filling in the remainder of the matrix with the remaining alphabets in orderly sequence [8]. The construction of the Playfair cipher with the keyword COMPUTER is presented in Table I. The encryption-decryption process is performed here by using the di-letters of the plaintext and the ciphertext respectively. For this, the intended plaintext letters are first prepared as a set of di-letters form and perform the encryption process. The letters are replaced with the following character depending on the basis of their position either column-wise or row-wise and are replaced with the opposite diagonal elements if they are in a diagonal position [9], [10].

Table I: A Playfair Matrix with COMPUTER keyword

C	**O**	**M**	**P**	**U**
T	**E**	**R**	A	B
D	F	G	H	I/J
K	L	N	Q	S
V	W	X	Y	Z

The cryptography process using in the Playfair cipher is presented below. The equation for the encryption process is

$$C = [EKs(P)] \quad \ldots \ldots \ldots (1)$$

And the process of decryption is

$$P=[DKs(C)] \quad \ldots \ldots \ldots (2)$$

Here, C is the ciphertext letter, E is the encryption process, D is the decryption process, Ks is the session key that is the transformation, and P is the plaintext letter.

The generated ciphertext of the patient's information is added in the image so that one cannot easily identify the hidden information and the output can safely transmit to the destination. In this paper, information is first encrypted with the keyword using in the Playfair cipher technique and the produced ciphertext is used in the steganography process to hide the information and then is sent to the intended destination for secured image transactions.

Revised Manuscript Received on July 22, 2019.

[1]**Shomitro Kumar Ghosh**, Department of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh.
[2]**Md. Toheen Bhuiyan**, Department of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh.
[3]**Md. Ismail Jabiullah**, Department of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh.

II. REVIEW WORKS

Image steganography is applied to hide data on an image that is not visible to anyone's eyes. All the image steganography processes to hide data based on the structure of the format of the most commonly used images on the Internet, Graphics Interchange Format (GIF), Joint Photographic Expert Group (JPEG), Portable Network Groups (PNG) and Bit Map Picture (BMP) [11]-[14].

- In steganography the original image that is chosen as a carrier for the secret data is call a cover image.
- In the result image of choosing the right cover image and embedding the secret data inside it is known as Stego image.
- The sender should have an algorithm for creating the Stego image to embed the data, and the receiver should have the matching algorithm to extract the hidden data from that particular Stego image and this is called Stego key.

The main challenge in this image steganography is that many image manipulation techniques might destroy the hidden message on any image, since it will change the feature of the Stego-image, it might as well change the feature of the hidden message inside it, such as cropping might crop the hidden message if it was located in one section of the image or corrupt it, rotation might give the receiver difficulty in finding the hidden message, filtering might destroy the hidden message completely and so on [15]-[18].

III. PROPOSED METHOD

If one needs to send patient's information in a secure manner, then the processes are to send "Patient to Doctor" or "Doctor to Doctor" use steganography techniques for keep secret patient's confidential data. The process is composed of the main three operations and they are encryption using Playfair technique, image composing for the steganography process, and the transmission to the destination [19]. The reverse process is performed in the destination to retrieve the actual patient's information in the system.

For encryption,

(a) At first Patient's information Encrypt with Playfair cipher

(b) Then cipher text and patient's image are attached by Stego Application

(c) In the end, the Stego Image is produced that are to be sent to the destination

For Decryption,

(a) At first received Stego Image

(b) Then Stego Image extract by Stego Application

(c) Next ciphertext and patient's image is retrieved

(d) Now ciphertext is decrypted with Playfair cipher

(e) Finally patient's information is retrieved

A. Flow Diagram

The entire process of the proposed system is depicted in Fig.1.

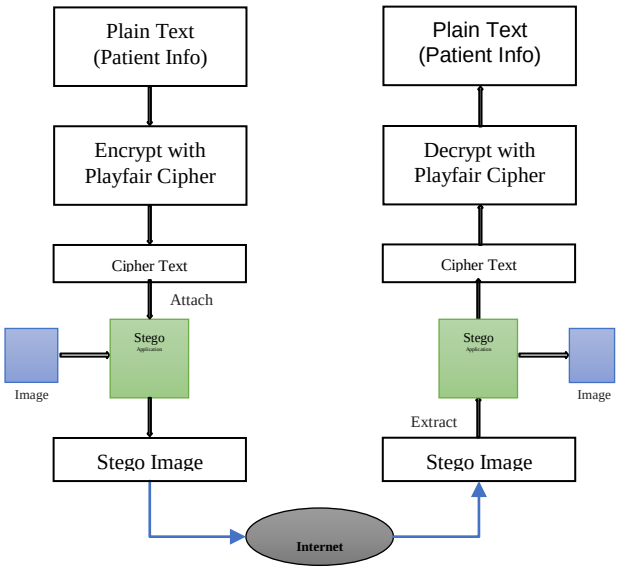


Fig 1: Flow-diagram of the Proposed System

B. Algorithm: The algorithm of the proposed system is presented below.

Step 1: Take information plain text.

Step 2: Encrypt with Playfair cipher

a) Select keyword.

b) Prepare a square matrix of 25 character, where (I/J) in one box.

c) Perform encryption with either row-wise or column-wise or diagonal shape as clock-wise.

d) Found cipher text.

Step 3: Perform with encrypting Stego Application

a) Enter cipher text and an image.

b) Attach cipher text & image.

c) Found Stego Image.

Step 4: This Stego Image send by internet.

Step 5: Received Stego Image

Step 6: Again perform with decryption Stego Image.

a) Enter the Stego image

b) Extract image and cipher text.

c) Take cipher text and move image.

Step 7: Decrypt with Playfair cipher

a) Select keywords

b) Prepare a square shape matrix of 25 character, where (I/J) in one box.

c) Perform decryption with either row-wise or column-wise or diagonal shape as anti-clock wise.

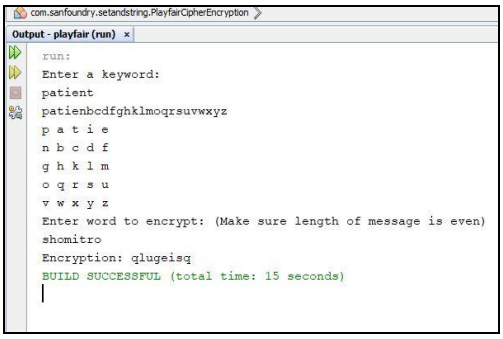
d) Found plain text information.

Step 8: Got information text.

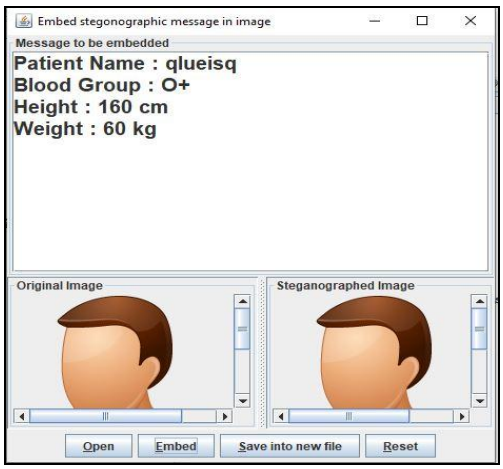
IV. IMPLEMENTATION

The system is implemented and found several outputs for the given set of input information. Selected input and output are given here.

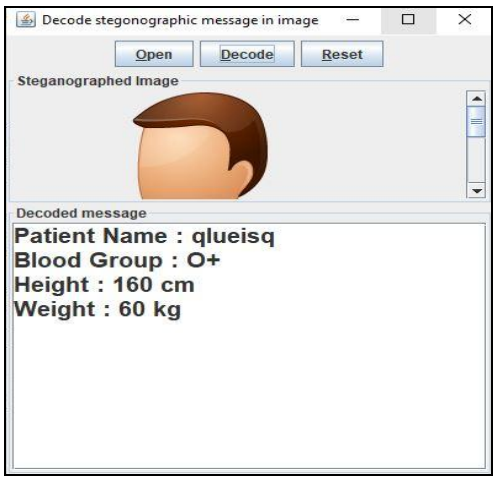
Patient's info as plaintext is encrypted by Playfair using the keyword COMPUTER and the cipher text is produced. This cipher text and person image (Patient's Image) are attached together by Encrypt app, a Stego image is found. This Stego image is then sent to the intended receiver. And the receiver extract Stego image by Decrypt App, finally plaintext (Patient's info) is retrieved. The Playfair cipher, Encrypt App and the Decrypt App are presented in Fig. 2.



2.1 Playfair Cipher



2.2 Encrypt App



2.3 Decrypt App

Fig. 2: Images of the Implantation System

V. RESULT ANALYSIS

The patient's information is encrypted using the Playfair cipher generation technique and the encrypted information is attached with the steganographic images and finally is sent to the destination successfully. For this several inputs are taken and all are analyzed and found the successful results. The complexity of the proposed system depends on the composite complexity both of Playfair cipher and also on the steganographic process.

VI. CONCLUSIONS

A steganographic process of image file and text file is designed, developed and implemented by using Playfair cipher with a keyword. The encryption process of the patient's information is performed by using the Playfair cipher generation technique and the produced ciphertext is attached with the image file and then is sent to the destination. A description of the proposed system is presented here with the logical concepts of steganography and Playfair technique and also discussed from the existing research works how data can be hidden in images. Here, it is focused on very basics of data hiding strategies and embedded to ensure the secrecy of data as well as reliability and robustness. The method is quite useful for all sorts of sensitive medical data and information transactions in steganography process. The success rate of this method can be improved if the related properties are carefully maintained.

REFERENCES

1. Masoud Hariri, Ronak Karimi and Mehdi Nosrati, "An introduction to steganography methods", World Applied Programming, Vol. 1, No. 3, 2011, pp. 191-195.
2. Neil F. Johnson and Sushil Jajodia, "Exploring steganography: Seeing the Unseen", Computer, Vol. 31, No. 2, 1998, pp. 26-34.
3. Mrs. Nitya Khare and Dr. S. Veena Dhari, "A Survey on Playfair Cipher Encryption Technique" IJSRD-International Journal for Scientific Research & Amp; Development, Vol. 5, No.10, 2017, pp. 568-569.
4. Abbas Cheddad, Joan Condell and Paul Mc Kevitt, "Digital image steganography: Survey and Analysis of Current Methods", Signal Processing, Vol. 90, 2010, pp. 727-752.
5. Softonic. (2015) Xiao Steganography. {Online}. Available: https://xiao-steganography.en.softonic.com/
6. Moudhi M. Aljamea, Costas S. Iliopulos and M. Samiruzzaman, "Detection of URL in Image Steganography", Proceedings of the International Conference on Internet of things and Cloud Computing, 2016.
7. Ravindra Babu K, S. Uday Kumar, A. Vinay Babu, I.V.N.S Aditya and P. Komuraiah, "An Extension to Traditional Playfair Cryptographic Method", International Journal of Computer Applications, Vol. 17, No. 5, 2011, pp. 34-36.
8. Safwat Hamad, "A Novel Implementation of an Extended 8x8 Playfair Cipher Using Interweaving on DNA-encoded Data", International Journal of Electrical and Computer Engineering, Vol. 4, No. 1, 2014, pp. 93-100.
9. Daphney Jerly Dsouza, Girish S, "A method of data hiding in QR code using image steganography", International Journal of Advance Research, Ideas and Innovations in Technology, Vol. 4, 2018, pp. 1111-1113.
10. Subhajit Bhattacharyya, Nisarga Chand and Subham Chakraborty, "A Modified Encryption Technique using Playfair Cipher 10 by 9 Matrix with Six Iteration Steps", International Journal of Advanced Research in Computer Engineering & Technology, Vol. 3, 2014, pp. 307-312.
11. Kalyan Das and Debanjan Choudhury, "An Ameliorate Image Steganography Method using LSB Technique & Pseudo Random Numbers", Journal for Research, Vol. 4, 2018, pp. 1-6.

12. Dr S Hemalath, Androse and E Sharmili, "An Efficient Method For Text And File Encryption For Secure Data Transmission Through Audio Steganography", International Journal of Trend in Scientific Research and Development, 2018, pp. 25-31.
13. Sandeep.y, K.A.Naveen Kumar and G.Reddy Gangadri, "A Novel Modified Play-Fair Image Steganography by Using 9 by 4 Matrixes", International Journal of Scientific & Engineering Research, Vol. 8, 2017, pp. 2008-2015.
14. Salman A. Khan, "Design and Analysis of Playfair Ciphers with Different Matrix Sizes", International Journal of Computing and Network Technology, No. 3, 2015, pp. 117-122.
15. Sahil Lotlikar, Ashish Gupta, Jayesh Thorat and Sandhya Kadam, "Image Steganography and Cryptography Using Three Level Password Securit", International Journal for Research in Applied Science & Engineering Technology, Vol. 5, 2017, pp. 1370-1374.
16. Alaa Kadhim Farhan, Rasha Subhi Ali and Sura Mazin Ali, "Secure Location Map and Encryption Key Based on Intelligence Search Algorithm in Encryption and Steganography to Data Protection", International Journal of Mechanical Engineering and Technology, Vol. 10, 2019, pp. 8-24.
17. Arun R, Nithin Ravi S and Thiruppathi K, "Intra Block and Inter Block Neighboring Joint Density Based Approach for JPEG Steganalysis", International Journal on Soft Computing, Vol. 3, No. 2, 2012.
18. Khaled Aedh Alaseri and Adnan Abdul-Aziz Gutub, "Merging Secret Sharing within Arabic Text Steganography for Practical Retrieval", IJRDO - Journal of Computer Science and Engineering, Vol. 4, 2018, pp. 1-17.
19. Md. Ahnaf Tahmid Shakil and Md. Rabiul Islam, "An Efficient Modification to Playfair Cipher", ULAB Journal of Science and Engineering, Vol. 5, No. 1, 2014, pp. 26-30.

AUTHORS PROFILE

Shomitro Kumar Ghosh is currently pursuing his B.Sc. degree in Computer Science and Engineering from the Daffodil International University, Dhaka, Bangladesh. His research interests are in Network Security, Information Security, Data Security, Cryptography, Steganography, Image Processing, Artificial Intelligence, Machine Learning, Data Mining, Augmented Reality, Neural Networks and Virtual Reality.

Md. Toheen Bhuiyan is currently pursuing his B.Sc. degree in Computer Science and Engineering from the Daffodil International University, Dhaka, Bangladesh. His research interests are in Network Security, Cryptography, Steganography, Information Security, Data Security, Artificial Intelligence, Machine Learning, Image Processing, Data Mining, and Virtual Reality.

Md. Ismail Jabiullah received Ph.D. degree in Computer Science and Engineering from the University of Dhaka, Bangladesh. His Ph.D. topic was in Cryptography and Network Security. He is currently a Professor in the Computer Science and Engineering Department at the Daffodil International University, Dhaka, Bangladesh. He has published 39 research articles in reputed journals and more than 78 research papers in the International Conferences. He authored more than 26 books. His research interests include Network Security, Information Security, Cryptography, Cyber Security, Cryptocurrency, Steganography, Wireless Network, Mobile Network, Artificial Intelligence, Machine Language, Deep Learning, Software Security, Satellite Network, Image Processing, Software Testing and Neural Networks. He serves as a reviewer for various reputed journals and conferences annually.