HBRP PUBLICATION

Journal of Network Security and Data Mining
Volume 4 Issue 1

A Playfair Cipher-based Secured Patients' Information Transaction System

Md. Ismail Jabiullah[1*], Arindra Dey Arni[2], Bipasha Babul Brishti[3]
Department of Computer Science & Engineering,
Daffodil International University, Dhaka, Bangladesh.

Corresponding Author
E-Mail Id:-*drismail.cse@diu.edu.bd*

ABSTRACT
Secured patient's information transaction between doctors and expert doctors from home and abroad, from remote to global for many reasons. A secured patients' information transaction system has been designed developed and implemented in Java programming language that can be used for patient information communication using Playfair symmetric key cryptographic technique. The proposed system first prepared a table of text space matrix using a keyword without repeating character and then performed encryption on the patient's sensitive information to produce ciphertext and then sent it to the destination. In the receiving end first prepare a text space matrix with the same keyword and then performed decryption on the receiving ciphertext to the retrieve the patients' information as plaintext. This proposed system has been implemented in Java code, produced several outputs for inputs and are analyzed. This can be applied where higher level security services are required.

Keywords: *Cryptography, Encryption, Decryption, Playfair Cipher, Secret communication*

INTRODUCTION

Data is transferred to different urgent work through different way means such as mobile, PC, email and many more. The hacker who collects this important information is doing a lot of damage in different cases many clients are suffering a lot due to the disclosure of information in business, Education Information or any other emergency. This is a way need many ways for hide information. Data Security is not only important for an organization it also plays an important role in security an individual's personal information. Patients' information is considered as National ID, patient's name, address, gender, blood group, height and weight, contact, Medical report, Medical image etc. Patient's information refers to a patient's identity. All information that could be used to identify, find, or connect with a doctor, what is the disease of the patient and what is the treatment for his disease. It is much more important to keep a patient's information secret.

A patient's relationship with a doctor is intimately involved. For better treatment, for emergency cases, it is needed to communicate the patients' information need to communicate among the local doctor to specialized doctor, in home and abroad. When we send a patient from one city to another city or from one country to another country for better treatment, a lot of time is wasted and a lot of money is spent, also the patient can suffer a lot. That's why we can send the patient's medical report without sending the patient. Because it is often seen that there are some hackers or some enemies who do not want go to the doctor for this correct information and the doctor will give the treatment correctly for the disease which may cause harm to the patient. Many times, the patient may die for this we are

using cryptography so that they get the correct information quickly and this will benefit both the patient and the doctor. That's why a research has been done to prepare a system of secret key cryptography technique to communicate patients' information secretly among the patient to distant doctors or specialist i.e., transact them between the remote doctor to specialized doctor home and abroad.

In this paper, a secret key symmetric cryptographic technique based on Playfair cipher has been designed, developed and implemented in Java programming code to test the sample patient's information on the inputs and the produced outputs. Finally a computational analysis of the proposed system has also been done that can clarify the system's security measures in proper applications on the secured communication channel.

REVIEW WORKS

The present age is the internet age, nowadays in our daily life its technology is used for communication in different work. Data is transferred to different urgent work through different way means such as mobile, pc, email and many more. The hacker who collects this important information is doing a lot of damage in different cases, many clients are suffering a lot due to the disclosure of information in business, Education Information or any other emergency. That's way need many ways for hide information.

Secret key cryptographic techniques are the art of hiding a message for keeping meaning of the message very secret in an unsecured communication way. It fills a comparative need to cryptography, however as opposed to encoding information essentially conceals it from the client.

In this digital world need of data encryption is very much important to protect the user data from intended user. Cryptography was the two technique that make secure the data from intended user that want to threat the normal user by many side like harm the user or keeping eyes on others working/progress. This can be classified into different approaches such as file, text and message file depending on the cover media that is used to embed the hidden data [1-12, 14]. QR codes could also be used for secured data communication. Text file cryptography is one of the oldest information hiding techniques, which is considered as the hardest cover media to use for cryptography purpose due to less redundant information available inside the text files for hiding the data [7, 8, 10, 11, 14]. Cryptography is applied to hide data on an image that is not visible to anyone's eyes. All the cryptography processes to hide data based on the structure of the format of the most commonly used message files on the Internet [11-15]. The most popular data formats that widely available on internet used are: doc, docs and txt because it is difficult to identify which particular file contain any hidden information and it is difficult to identify which tool of cryptography is use these data formats to brock the technology. The cipher codes are used for variety of applications like secret communication, copyright protection, marketing, business, and education, etc. In a study on physical access control based QR codes [2], researchers established a physical authentication method using a mobile phone and QR code.

In this paper, information is first encrypted with the keyword based symmetric key cryptographic technique using in the Playfair cipher generation process and the produced ciphertext is used to hide the intended information from the unwanted users and then is sent to the intended destination patient or specialized doctors

for secured message of information transactions very securely.

PROPOSED SYSTEM METHOD

A symmetric key cryptographic system is a technique of concealing information that in computer science refers to hiding data in a manner so that unwanted user cannot recover the message from the message file. It can be secretly exchanged for information between the communicants through the open communication media. The proposed system method can be performed by the following way:

- Collect patients' personal information and medical information.
- Collect local medical doctor's opinion and prescription.
- Select a keyword and then prepared a keyword matrix with the English alphabets
- Performed encryption operation using Playfair symmetric key cryptographic process on the patients' all information.
- The targeted ciphertext is produced and is sent to the destination.
- In the receiver site, first prepare the keyword matrix of English alphabets
- Perform the decryption process on the received ciphertext using Playfair symmetric key cipher technique
- The plaintext of the patients' information is retrieved as the output of the process.

Encryption Process

The encryption process of the proposed system is presented below:

1. Collect patients' personal information and medical information.
2. Collect local medical doctor's opinion and prescription.
3. Select a keyword and then prepared a keyword matrix with the English alphabets
4. Performed encryption operation using Playfair symmetric key cryptographic process on the patients' all information.
5. The targeted ciphertext is produced and is sent to the destination.

The whole method is depicted in the following Figure 1(a).

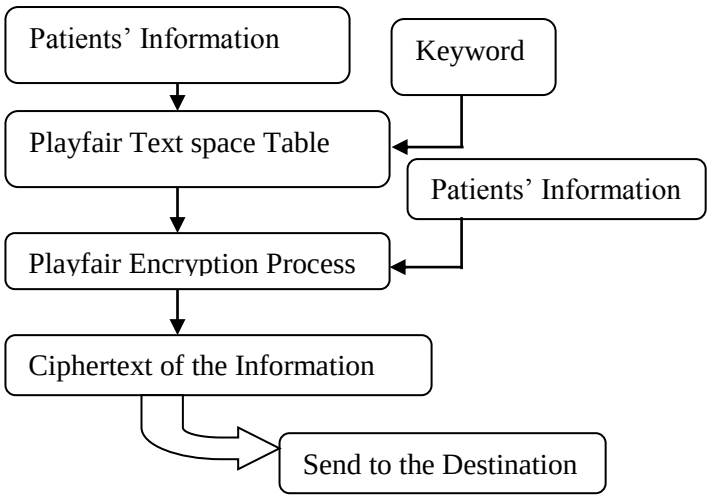


Fig.1(a):-*Encryption Process of the Proposed System*

Decryption Process

The decryption process of the proposed system is presented below:

1. In the receiver site, first prepare the

keyword matrix of English alphabets
2. Perform the decryption process on the received ciphertext using Playfair symmetric key cipher technique
3. The plaintext of the patients' information is retrieved as the output of the process.

The whole method is depicted in Figure 1(b).

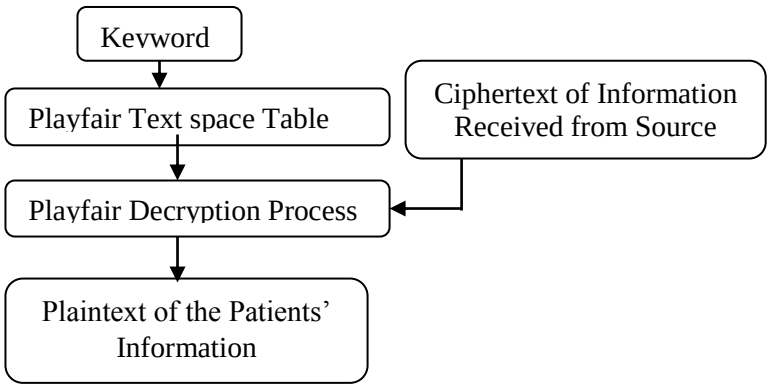


Fig.1(b):-*Decryption Process of the Proposed System*

Algorithm

The algorithm of the proposed system is presented below:

Step 1: Take patients' information as plaintext for the cryptographic system.

Step 2: Perform encryption operation using Playfair cipher with appropriate keyword

(a) Select keyword and prepare a Playfair text space table

(b) Perform encryption operation

(c) Found ciphertext of the information

Step 3: The output ciphertext of the patients' information is sent to the destination by the Internet.

Step 4: Received ciphertext

Step 5: Perform decryption operation on the ciphertext

(a) Received keyword (through KDC) and prepare a Playfair text space table

(b) Perform the decryption operation on the received ciphertext.

c) Retrieved the plaintext of the patients' information

Requirements

To implement the secured proposed system, some hardware and software are required and they are: (a) Processor: i3 7th Generation, (b) RAM: 2 GB (mini) (c) Hard disk: 500 GB, (d) Monitor: 19'' LCD, (e) Windows 10 and (f) Software Java

To prepare a test environment of a designed and developed cryptographic system one can easily investigate several inputs and outputs, grasp a clear idea and put a recommendation on the proposed system.

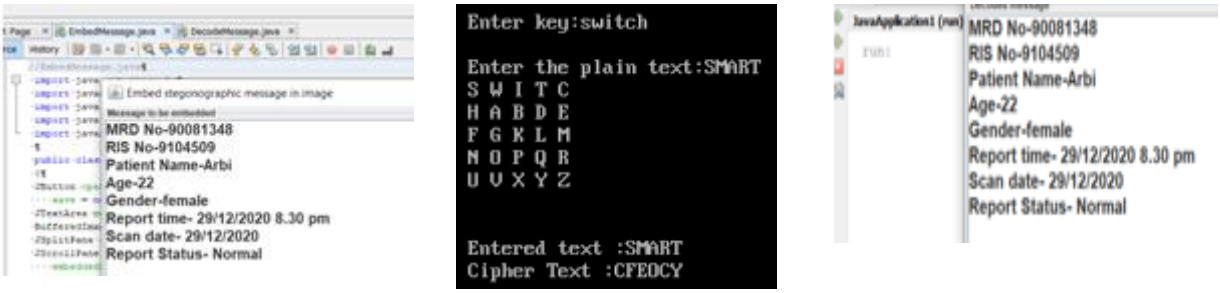
Implementation

The proposed cryptographic system has been implemented using Java programming code with the patients' intended information. Several input-outputs have been found for several keywords. The targeted input/output analysis are found and presented below:

Input/output Analysis

The system is executed in Java programming language codes and found output for the given arrangement of the patients' input information. Chosen input and output are given here. Patient's information as plaintext is encrypted by using the symmetric cipher Playfair with

the keyword and the ciphertext is produced. The output from the program is the ciphertext. This output information is then sent to the intended receiver. In the receiving end, receiver's system extracts the patients' information by performing decryption process. Sample patients' information as plaintext, ciphertext and the retrieving plaintext are presented in Figure 2:



(a) Patient's Information as Plaintext (b) Playfair Ciphertext (c) Retrieved Patient's Information

Fig.2:-*Implemented Input-Output of the Patient's Information*

The patient's information is encrypted using the Playfair cipher symmetric key cryptographic process and encrypts the patients' information and is sent to the destination successfully. For this few information sources are taken and all are analyzed and found the successful results. In the destination, the received ciphertext of the patients' information is decrypted using the Playfair cipher process where the text space table is prepared using the same keyword matrix. The sample input-output screenshots are presented in Figure 2.

Computational Analysis

The computational security analysis of the proposed system has been analyzed and presented so that one easily realize the strength of security and apply the system process in the desired area.

Security Parameter	Performed Status	Security Measures
confidentiality	Yes	Keyword-based encryption
integrity	Yes	Performing encryption process
authentication	Yes	By using Secret key matrix
non-repudiation	No	performing encryption process

CONCLUSIONS

Secured patients' information communication system between doctors to doctors or patients to doctors is very much needed in the telemedicine area in remote area to town both home and abroad as well as globally. Several approaches have been studied with its different issues. A secured secret keyword based Playfair encryption-decryption technique has been designed, developed and implemented using Java programming language. The implemented system has been system analyzed with several sample patients' information and presented. We have also analyzed and presented the security issues of the proposed system. Our proposed method can be applied in any medical diagnostic center, health care center, hospital, or even any doctor can implement this in telemedicine sectors.

REFERENCES

1. Nosrati, M., Karimi, R., & Hariri, M. (2011). An introduction to steganography methods. World Applied Programming, 1 (3), 191–195.

2. Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer*, *31*(2), 26-34.
3. Sandeep, Naveen, K., A., ReddyGangadri, G. (2015). A Novel Modified Play-Fair Image Steganography by Using 9 by 4 Matrixes. *International Journal of Scientific & Engineering Research*.8.2008-2015.
4. Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal processing*, *90*(3), 727-752.
5. Softonic. (2015) Xiao Steganography. {Online}. Available: https://xiao-steganography.en.softonic.com/
6. Aljamea, M. M., Iliopoulos, C. S., & Samiruzzaman, M. (2016, March). Detection of url in image steganography. In *Proceedings of the International Conference on Internet of things and Cloud Computing* (pp. 1-6).
7. Ravindra Babu, K., Kumar, S. U., Babu, A. V., Aditya, I. S., & Komuraiah, P. (2011). An extension to traditional playfair cryptographic method.
8. Hamad, S. (2014). Novel Implementation of an Extended 8x8 Playfair Cipher Using Interweaving on DNA-encoded Data. *International Journal of Electrical & Computer Engineering (2088-8708)*, *4*(1).
9. Dsouza, D. J., & Girish, S. (2018). A method of data hiding in QR code using image steganography. *International Journal of Advance Research, Ideas and Innovations in Technology*, *4*, 1111-1113.
10. Bhattacharyya, S., Chand, N., & Chakraborty, S. (2014). A modified encryption technique using Playfair cipher 10 by 9 matrix with six iteration steps. *International Journal of Advanced Research in Computer Engineering & Technology*, *3*(2), 307-312.
11. Das, K., Choudhury, D., & Bandyopadhyay, S. K. (2018). An Ameliorate Image Steganography Method using LSB Technique & Pseudo Random Numbers. *Journal for Research| Volume*, *4*(09).
12. Hemalath, S., Sharmili, E.(2018). An Efficient Method For Text And File Encryption For Secure Data Transmission Through Audio Steganography. *International Journal of Trend in Scientific Research and Development.*25-31.
13.] Khare, Nitya, and Dhari, S. Veena. (2017). A survey on Playfair cipher encryption technique *IJSRD-International Journal for Scientific Research & Amp.*5(10):568-569p.
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.