IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

AN APPROACH TO MITIGATE THE PRIVACY ISSUES IN SMARTPHONE HEALTHCARE SYSTEM THROUGH VISUAL CRYPTOGRAPHY

Reena Prasad*, Dr. Tripti Arjariya
M. Tech. Scholar CSE Department, Bhabha Engineering and Research Institute, Bhopal (M. P.)
India
CSE Department, Bhabha Engineering and Research Institute, Bhopal (M. P.)
India

DOI: 10.5281/zenodo.48839

ABSTRACT

Smartphone Healthcare Systems are the immerging pervasive technology which provides the healthcare services at any location through mobile phones. It contributes to access the Electronic Medical Records (EMR) from and to the practitioners, researchers, patients, pathologist and doctors to treating their illness. The emerging technologies help to ease the treatment through discussing the doctors at any location according to the availability of time schedule. These EMR contains the private information of the patients. Therefore exchanging the EMR's must be secured at network as well as storage medium. However, number of privacy issues poses challenge to the Smartphone healthcare systems. Most of these records are available at the storage of the electronic device, common accessible database or shared cloud. Exchanging and storing of these data must be accessed securely and privacy should not be leaked without knowing the patients. In this paper a Visual cryptography based approach for Smartphone healthcare system has been proposed and implemented to preserve the privacy and ensuring the authentic accessing the EMR through the knowledge of patients. Authentication is based on the image key selected by the authentic parties.

KEYWORDS: Visual Cryptography, EMR, M-healthcare, Permutation.

INTRODUCTION

Smartphone healthcare systems have played a part in the dramatic improvement in the health services that occurred during the 20th century. Their role in the human life is greatly important. During the past few decades, health services and healthcare systems have improved greatly to provide the ease of treatment and preserving the privacy of patient.

Smartphone healthcare system shares the electronic medical records to consult with doctor for proper treatment. Most of the EMR are in the Image form which contains the private information of the patients. Leakage of these records or careless handling of EMR leaks the privacy of the patients. This feels insecure to the patients and due to the human nature patient feels nervous to consult with others. Hence, a secure Smartphone healthcare system is required to protect the privacy issues.

This paper proposed a secure approach for Smartphone healthcare system on the basis of Visual Cryptography. Visual Cryptography is an approach to encrypt a secret image through converting it into layers. Layers would be in such manner that it becomes unreadable for unauthorized user. Authentic user may reveal secret image back through stacking a sufficient number of layers in a particular manner.

In this paper an approach has been developed to mitigate the privacy issues in mobile healthcare systems on the basis of visual cryptography. In this technique first the electronic medical record is decomposed into n layers. These layers are stored in such a way that doctor may superimposed the original image through stacking the layers stored at doctor's module with the layers stored at patient's module.

Backgroung and Literature

Visual cryptography commonly known as secret sharing of images has been introduced by Adi Shamir in 1979. Author stated that decompose the secret image S_i into n layers and send to destiny. At destination superimposed any k layers from n layers to obtain the original secret image S_i.

2 out of n visual cryptography

M. Naor and A. Shamir [7] proposed 2 out of n visual cryptography scheme in which minimum 2 layers are required to superimpose the original image.

Horng et al. [8] proposed an approach through which n-1 parties may superimpose the original image. In 2 out of n visual cryptography scheme 2 shares are enough to decode the secret image which may also provides the information such as underlying distribution to calculate the third share. Underlying distribution such as knowing the pattern of black pixel in 2 layers allows to determining the position of black pixel in third party layers. Through getting the enough shares they may superimpose the original image.

n out of n visual cryptography

The n-out-of-n visual cryptography can be best described by considering a 3-out-of-3 -VCS case. The basis matrix S_0 is designed as:

$$L_0 = \begin{matrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{matrix}$$

Similarly the basis matrix L_1 is:

$$L_1 = \begin{matrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{matrix}$$

For the above basis matrices, the relative difference α and contrast β are computed as:

$$\alpha = 1/4$$
$$\beta = 1$$

2 out of 2 visual cryptography

Due to the importance of both parties in Smartphone healthcare system, 2 out of 2 Visual Cryptography is suited best for preserving privacy of Electronic Medical Records (EMR).

According to the image color visual cryptography schemes are categorized into two categories Black N White Visual Cryptography and Color Visual Cryptography.

Wen Tsai Che Lee [9] proposed an authentication system in context of visual cryptography based on the binary adocument images. Author used binary images that must follow portable network graphics format.

George Abboud [10] combined the concept of Stegenography with visual cryptography to share the hidden messages. Author's concept raises the complexity of computation of original image through superimposing the layers.

Commonly EMR consist of black and white images and text rather than color images. For preserving the privacy of electronic medical records into Smartphone healthcare system Black N White visual cryptography is suited best.

An approach of visual cryptography which is based on two criteria pixel expansion and encoding of layers is insignificant for Smartphone healthcare systems due to the limited storage.

Smartphone-Healthcare System based on Visual Cryptography

According to the need of privacy in healthcare systems we have to develop a prototype model on the basis of visual cryptography for secure storage of images in Smartphone. We have also plane to use compression algorithm for the optimization purpose.

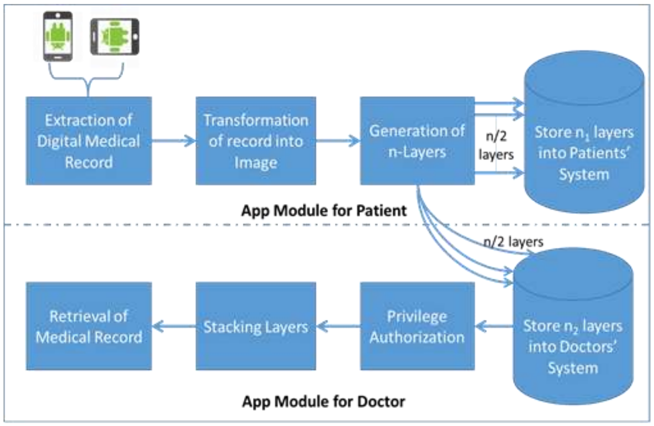
Extraction of Digital Medical Record
Transformation of record into Image
Generation of n-Layers
n/2 layers
Store n_1 layers into Patients' System
App Module for Patient
n/2 layers
Retrieval of Medical Record
Stacking Layers
Privilege Authorization
Store n_2 layers into Doctors' System
App Module for Doctor

Figure: Proposed Model for Smartphone Healthcare System

Proposed system works in two module one for the patient and another one for the doctor. Patient's module extracts the EMR from the mobile storage and transforms it into image. After that decomposed these images into n layers in which half stored into patient's android device and another half stored into doctor's device. When doctor want to views the EMR, doctor's module authorize the privilege and superimposed the layers to retrieve the original EMR.

Image Decomposition-

Value of the pixel in the image of the electronic medical record is indicated as I(x, y) before processing and as L(x, y) after processing. For black and white EMR the values of aforementioned two functions are either 0 or 1.

The image is encrypted through the visual cryptography scheme discussed in this paper. Each pixel is encrypted through the key used for the encryption. Encryption key used is also the image selected by the patient's module and shared by the doctor's module. Then only the person knowing the key image may decrypt the image. Image selected as the key must be of the black and white pixel only. In another term key image should be black and white image having only black and white pixel values either 0 or 1.

Original image is decomposed into n parts in context of the size of the key image. And then each part is encrypted through altering the pixel value. If pixel value of K(x, y) in the key image is 0 then the corresponding pixel value of the original image I(x, y) is used as pixel value of E(x, y) in encrypted image. If pixel value of K(x, y) in the key image is 1 then the corresponding pixel value of I(x, y) in the original image is flipped and used as pixel value of E(x, y) in the encrypted image.

$$V_E(x,y) = \begin{cases} V_I(x,y), & if\ V_K(x,y) = 0 \\ V_I(x,y), & if\ V_K(x,y) = 1 \end{cases}$$

Where-

V_I(x, y) = value of pixel I(x, y) of original image
V_K(x, y) = value of pixel K(x, y) of key image
V_E(x, y) = value of pixel E(x, y) of encrypted image

Finally, image is decomposed into 2 layers in which one is stored at patient's module and another is at doctor's module. Image decomposition has been done through decomposing each pixel into 2*2 matrixes which contains the

4 values. If the pixel is black then first layer of it contains the $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$ matrix value and second layer contains the $\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$ matrix value or vice versa. If the pixel value is white then both the layers contains the similar value matrix. First layer contains $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$ and second layer contains the $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$ or vice versa.

The layers of decomposed image is then transmitted and stored in two different databases. One is at the patient's module and another is in the doctor's module.

Priviledge Autherization-

It has been done at doctor's module when he wants to visualize the original EMR. During the authentication process, the doctor selects the key image from the different available key images in the doctor's module and sends request to patient's module. Patient's module check that requested key image is legitimate or illegitimate and then authenticates the doctor. Further it sends the remaining layer of the original image.

Stacking Layers -

Both layers are overlaid to each other to create the original image.

Retrieval of Electronic Medical Record

Here permutation of finite set of x-bits has been applied. Permutation is a bijective function $\pi: X \rightarrow X$ which has an inverse function (π^{-1}). Inverse permutation is used to decrypt and obtain the original image.

Evaluation and Result Analysis

The results will show that the time taken by proposed work is less than the previous work. There is a large difference between numbers of comparator. Finally the proposed work is better than the previous methods. Our system also useful for each application of Smartphone where image related issues has been increases. And Patient can store Electronic Medical Record (EMR) own Smartphone without considering Smartphone privacy issues for healthcare systems.

Figure: Original Image of Hand X-ray before Processing

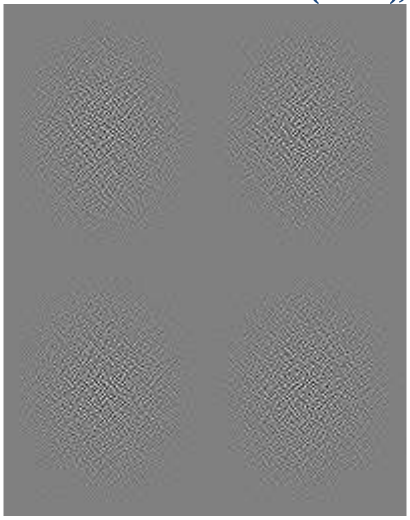

Figure: Layer-1 of Hand X-Ray Decomposed through Developed System

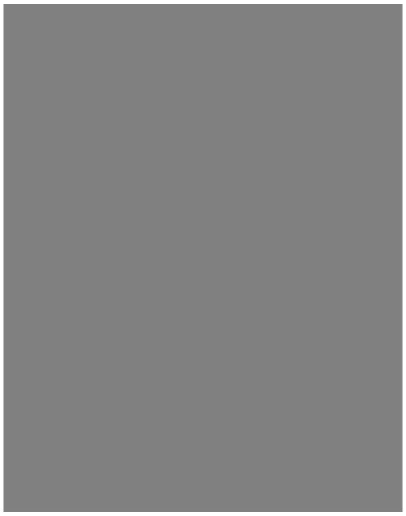

Figure: Layer-2 of Hand X-Ray Decomposed through Developed System

CONCLUSION AND FUTURE WORK

Smartphone healthcare systems have great importance in human life. Privacy of Electronic Medical Record (EMR) in Smartphone healthcare system is a crucial issue.

In this paper an approach based on the cryptographic scheme has been proposed and implemented. It preserves the privacy of the patient through providing the secure storage and authentic access. It also uses the encryption which protects the EMR privacy at the network when patient share it through the doctor. One image key is used for both authentication and encryption which reduce the processing. Ease to remember the key due to the remembrance of the image is easier rather than the text password. This scheme also may be applied on the shared database, cloud or memory storage of the electronic device.

REFERENCES

[1] 2013 Mobile Trends Report

[2] K. Renaud and D. Gálvez-Cruz, “Privacy: Aspects, Definitions and a Multi-Faceted Privacy Preservation Approach”, in Information Security for South Africa (ISSA), pp. 1-8, 2010.

[3] S. Sadki and H. El. Bakkali, "Enhancing privacy on Mobile Health: An Integrated Privacy Module", in Fifth Int. Conf. on Next Generation Networks and Services (NGNS), Casablanca, Morocco, pp. 245-250, 2014.

[4] X. Xuan, Y. Wangy, and Li Shanping, "Privacy Requirements Patterns for Mobile Operating Systems", in IEEE 4th International Workshop on Requirements Patterns (RePa), Karlskrona, Sweden, pp. 39-42, 2014.

[5] S. Avancha and A. Baxi, "Privacy in Mobile Technology for Personal Healthcare" ACM Computing Surveys, Vol. 45, No. 1, November 2012.

[6] A. S. Akotkar and C. Choudhary, "Secure of Face Authentication using Visual Cryptography", in Int. J. of Innovative Science and Modern Engineering (IJISME), Vol. 2, Issue 5, 2014, pp. 13-15.

[7] Naor, M. and A. Shamir. Visual cryptography, Advances in cryptology. Eurocrypt '94 Proceeding LNCS, 950:1–12, 1995.

[8] Horng, G, Chen, T. and Tasi, D.S. Cheating in Visual Cryptography, Designs, Codes and Cryptography, 2006, pp219–236

[9] Wen Tsai Che Lee, Authentication of binary images in png format based on a secret sharing technique. Proceedings of IEEE International Conference on System and Engineering, pages 506-510, July 2010.

[10] Yampolskiy R.V. Abboud G, Marean J, Steganography and visual cryptography in computer forensics. Proceedings of 5th IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, pages 25-32, 2010.

[11] Leemon Baird, "Visual Cryptography", [Online]. Available: http://www.leemon.com/crypto/VisualCrypto.html