ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

Secure Sharing Hospital Data Using Visual Cryptography.

Chitra Kalpesh Vasvani, Snehal Kolte

Assistant Professor, AISSMS College of Engineering, Pune, India

Assistant Professor, AISSMS College of Engineering, Pune, India

ABSTRACT : Security of the advantages does not exclusively rely upon a person's safety effort. Information access by unapproved clients must be avoided. We aggregately approach the issue of security and execution as a protected information transmission issue. Securely sharing electronic wellbeing records has pulled in thought in therapeutic condition. We discuss essential issues related to electronic wellbeing records sharing and offer how to share a restorative picture of electronic wellbeing records in light of visual cryptography(VC) and riddle bestowing to mystery expression of experts for comfort in scattered system. Moreover, our recommendation is associated with certifiable system "openEMR" (Electronic Medical Records) and evaluated in respect of execution and security.

KEYWORDS :Cryptography, Steganography, Security, Performance.

I. INTRODUCTION

Most applications are just as secure as their fundamental framework. Since the outline and innovation of middleware has enhanced relentlessly, their discovery is a difficult issue. Therefore, it is almost difficult no doubt regardless of whether a PC that is associated with the web can be viewed as dependable and secure or not. The inquiry is the means by which to deal with applications that require an abnormal state of security, for example, center saving records of patient and web managing an account. In a core Hospitalization system, there is a chance of encountering forged signature for transaction. And in the electronic health record system, the records of patient may be hacked and misused. Thus security is still a challenge in these applications. Here, we propose a technique to secure the patient information and to prevent the possible forgery of records and misuse of documents. Picture handling is a procedure of preparing an input image and to get the output as either improved form of the same image and/or characteristics of the input image. Visual Cryptography (VC) is a technique of encoding a secret image into shares with the end goal that stacking an adequate number of shares uncovers the secret image. Steganography techniques, on the other hand, tend to hide the existence of the message itself, which makes it difficult for an observer to figure out where the message is.

II. OBJECTIVE OF THE WORK

To increase both the security and performance. To achieve reliability, security, integrity of the data. To ensure a control the file fragments, where each of the fragments only once for the purpose of improved security. The proposed scheme ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker.

III.LITERATURE SURVEY

[1]Zhili Zhou1, Ching-Nung Yang, [2017] have represented coefficients of (k-1)-degree polynomial are used for embedding secret image pixels and permutation-only ciphers are insecure, in all of the existing (k, n)-SIS schemes, one may recover some partial secret pixels from (k-1) shadows. Thus, the threshold properties of those schemes are compromised.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

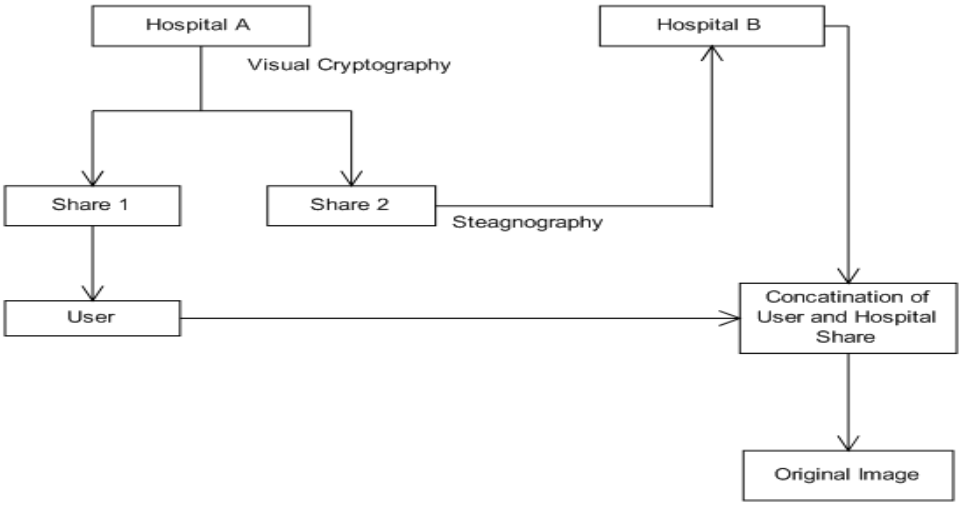
Vol. 6, Issue 11, November 2018

[2] JitendraSaturwar, D.N. Chaudhari, [2017] An image watermarking model based on progressive visual cryptography is propose dto decide optimal number of shares. A study on implementation of meaningful shares in combination with visual cryptography scheme for secret images is carried out for implementation of algorithm.

[3] Naoki Kita, Kazunori Miyata1, [2018] The magic sheet decrypts multiple secret images depending on a given share. The shares are printed on transparencies, and decryption is performed by physically superimposing the transparencies.
[4] Yuqiao Cheng, Zhengxin Fu, Bin Yu, [2018] visual secret sharing scheme to encode a secret QR code into several shares. In contrast with other techniques, the shares in our scheme are valid QR codes that can be decoded with some specific meaning by a standard QR code reader, thereby avoiding raising suspicion in potential attackers.
[5] AbulHasnat, Dibyendu Barman,SatyendraNath Mandal, [2017] Number of parts is generated from one image. The parts are sent to the receiver and receiver reconstructs the original image by stacking all the share images. Generation of parts is different for different types of binary, gray and color images. K out of K visual cryptography scheme by Naor and Shamir is a well known visual cryptography algorithm.

IV. SYSTEM APPROACH

We design a new concept called secure electronic health records in the Hospital for Optimal Performance and Security that collectively approaches the security and performance issues. The proposed scheme ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker. Hospital system provides the facility of having service of getting details of patient reports and other records. In case of individual operation it does not mean to have patient records security but it provides flexibility to get the details with authentication. In some cases socially it is not secure. Suppose A and B are the two hospitals and later time A gets adverse to B request for all the documents of patient and then after getting the details B modifies the records and send it to patient for different kind of reason. In this case B is cheated by A. In the proposed method it is ensure that transaction is only possible when hospital and user are available. To overcome these issues we provide authentication that is cryptography and steganography techniques used. It also ensure that nobody can misuse the information stored in the database because Shares are random noise like images and nobody can get any clue from a single share even he apply enormous amount of computing power and time. In the proposed method gray images of both the user are taken as input and processed for further use.



System Architecture

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

V. CONCLUSION

When sharing information in Electronic Health Record system dealing with crucial data of patient, significant topics are the method to communicate between the institutions and save Electronic Health Records. To secure secrete sharing the records by using VC and steganography. Keeping and maintaining the records centrally and securely access everywhere and any time.

REFERENCS

[1]Zhili Zhou1, Ching-Nung Yang, "Secret Image Sharing based on Encrypted Pixels" IEEE.2017.
[2] Aaditya Jain, SourabhSoni, "Visual Cryptography and Image Processing Based Approach for Secure Transactions in Banking Sector," 2017 2nd International Conference on Telecommunication and Networks (TEL-NET) 2017.
[3] JitendraSaturwar, D.N. Chaudhari, "Secure Visual Secret Sharing Scheme for Color Images Using Visual Cryptography and Digital Watermarking," IEEE Transactions on Cloud Computing,Vol. 1, No. 1, 2013.
[4] Naoki Kita, Kazunori Miyata1, "Visual cryptography with common shares," IEEE Globecom Workshops, 2018.
[5] Yuqiao Cheng, Zhengxin Fu, Bin Yu, "Improved Visual Secret Sharing Scheme for QR Code Applications," IEEE Transactions, 2018.