Middle-East Journal of Scientific Research 19 (6): 821-825, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.19.6.1464

Secure Transmission of Multiple Specialized Closet Sharing Scheme

B. Sundarraj

Department of Computer Science & Engineering,
Bharath University, Chennai-600073, India

Abstract: Medical imaging, though very advanced and widespread, has been facing drawbacks with regard to integrity and confidentiality. A relevant literature survey brings into notice that there is no single exhaustive method to deal with all the issues. In tele diagnosis it is required that a medical image is distributed among a group of medical experts. However, disclosing all the information of an important patient's medical condition to each of the clinicians is a security issue. A specialized secret sharing scheme is proposed in which digitized, archived and compatible medical images are shared among n clinicians such that at least k of them must gather to reveal the diagnosable medical image. It also emphasizes on the process of hiding textual medical information in these images in order to meet not only the security issue but also suffices the storage requirements during transmission. It is a novel technique for a secure transmission of confidential and important medical information over an insecure network effectively.

Key words: Visual Cryptography · Confidentiality · Text hiding · Polynomial interpolation

INTRODUCTION

Security has become an inseparable issue as information technology is ruling the world now. Cryptography is the study of mathematical techniques and the related aspects of information security such as confidentiality, data security, entity authentication and data origin authentication.

The integrity and confidentiality issues have been satisfied by some of the researchers so far in literature findings [1, 2, 3, 4]. Both fragile and robust watermarking techniques are used for integrity control and EPR hiding. The involvement of medical images call for satisfying important issues like that of the integrity and the confidentiality.

Another robust technique abased on genetic algorithms to embed the watermark or textual around the region of interest was proposed by Shih and Ta Wu in 2005. They embed the signature image and the fragile watermark into the frequency domain of non-ROI part of a medical image. Woo *et al*. (2005) [4] used a multiple watermarking method consisting of an annotation part and a fragile part. In this the encrypted EPR can be embedded in an annotation watermark and tampering can be detected using a fragile watermark. Security can be improved by hash-block-chaining watermarking approach in the fragile watermarking. A method that attaches digital signature and EPR into the medical image was indicated by the works of Zhou *et al*. (2001) [5]. LSB replacing technique has been used to embed the signature. A secure data hiding technique based on the bipolar multiple-base conversion to allow a variety of EPR data to be hidden within the same mark image was presented by Chao et al in 2002. The mark of a hospital used to identify the origin of an EPR could be used as a mark image. There is a good scope of separation and restoration of hidden data by authorized users in this.

Another noted technique of reversible Steganography can be used to hide EPR in medical images. This work was published by Nayak (2009) [6]. Their method doesn't evaluate confidentiality and authenticity of the medical image. Moreover, embedding capacity of their method depends the number of pixels of the medical image. Steganography can be used for EPR hiding and this was indicated by Lou in 2009. However, Integrity and confidentiality of the medical image is not satisfied by their work. Hu and Han in 2009 used Cryptography for transforming medical images into noise

Corresponding Author: B. Sundarraj, Department of Computer Science & Engineering,
Bharath University, Chennai-600073, India.

like form for protection. However, noisy images have a great likelihood of attracting malicious user's attention and EPR hiding is not considered. Each method outlined above satisfies different security requirements (confidentiality, authenticity, EPR hiding) for medical image sharing. A method will be proposed for ensuring the secrecy of a medical image, which satisfies the following requirements.

- Electronic patient records should be hidden in medical images thereby reducing storage requirements and network bandwidth.
- Confidentiality of the medical images should be maintained.
- A single individual should not be allowed to diagnose political leaders or high-ranking military officers since it is not adequate to trust only one.

Previous Research: Visual cryptography is a technique that enables us to encrypt data in a way that decryption can be done easily by human eye without any computer aid. This being the domain of this paper some related concepts have been discussed below.

Shamir's Secret Sharing Scheme: Shamir, a pioneer in the field of visual cryptography, proposed a scheme back in year 1979. According to it a secret of any form is divided into n number of shares. Out of these n shares at least k or more shares when gathered are sufficient to get back the share intact [7]. Its known as the (k, n) secret sharing scheme. In the present scenario a medical image is to be distributed among a set of clinicians hence the image is converted into noise like shares and distributed among all of them. In order to maintain the secrecy and in case of trust violation even if one less than k clinicians gather it would be impossible to retrieve the secret. This threshold value then depends on various internal factors as well.

Steganography: Steganography is a technique of hiding messages such that no one, apart from the sender and the recipient know about the message, a form of security through obscurity. Medical images are shared among n participants in this work. Since the main issue is hiding a text or an image in it, Steganography plays a vital role of an efficient embedding technique. The embedding process encrypts the medical image and the shares that are generated are noisy giving out no hint of the hidden text. This is a reversible process since decryption is needed to get back the hidden contents. If any k or more participants gather, the medical image can be revealed. It is assumed that at least k clinician is an adequate security measure to view the medical image to diagnose.

Polynomial Interpolation: Shamir's method of (k, n) secret sharing is based on a polynomial approach. The image or the text that is being hidden is done so by generating polynomials for every share that is being created. Zhao's method to generate unique keys helps in providing unique shares to every participant. Interpolation of the keys values and the polynomial values would give back the polynomial during decryption and the constant part of the polynomial would be the secret. The pixel values of the medical image are used to generate the polynomial of (k-1) order or less.

The dealer selects a large prime number p and a (k?1) degree polynomial is constructed as in (1) to compute shares using the secret:

Research Method: Overview of this paper consists of the following modules:

- KEY GENERATION
- EMBEDDING
- SHARING
- RECONSTRUCTION

Key Generation: In order to maintain the uniqueness of the shares, every participant is provided with a unique key. This key is generated based on Zhao's method. This method ensures,

- Unique shares by using unique x values,
- C values are calculated independently by both the dealer and participants before the sharing procedure. Thus an insecure channel between the dealer and participants is sufficien [8]t,
- Even if one gathers any k shares from the network, one cannot recover the secret image unless corresponding x values for those shares are known.

Algorithm:

- A 'secret shadow' is chosen uniquely by each participant.
- A dealer chooses primes p & q and computes N=pq.

- Then the dealer chooses integer g from $[N^{1/2}, N]$ where g is relatively prime to p & q and publishes {g, N}.
- The participant chooses randomly s_i [2, N] and computes Ri= g^{si}mod N and provide own R_i to dealer.
- Now the dealer makes sure $R_i \neq R_j$ and chooses S_0 [2, N] where S_0 is relatively prime to (p-1) & (q-1).
- Then the dealer computes $R_0 = g^{s0}$ mod N and publishes $\{R_0\}$ and finally computes $X_i = R_i^{S0}$ mod N for each participant.

Embedding: The medical image is first embedded with the text i.e., EPR (Electronic Patient Record). EPR is taken from a text file which is read and every character is converted into the corresponding ASCII codes. The number of characters that can be embedded into an image depends on the size and the bit depth of the image. The next step is to generate a polynomial which incorporates both the image pixels and the ASCII code. This polynomial is generated randomly thereby creating a share that is different from the other. This can also be used for embedding an image into another image. Thus the encryption of this sort provides scope for hiding a considerably large amount of text into an image and also for hiding an image into another image.

Sharing: In the sharing phase the embedded image i.e., the image with the hidden text is divided into n noise like shares [9]. All the shares are of the same size as that of the medical image. With the available attributes of an image i.e. bit depth and size the image pixels are taken as follows:

$$M = \{m_i \mid m_i \in [0, (2^b - 1)], i = 1,2,...,W * H\}$$

The EPR values are ASCII characters of length L which are represented as follows:

$$E = \{e_i \mid e_i \in [0, 251], i = 1,2,...,L\}$$

With both the image pixel values and the ASCII values of the Electronic Patient Record (EPR) the polynomial and shares are obtained (say) as follows:

$$F(x) = (1+2x) \bmod 257$$

The unique x values are used to obtain Shared pixels:

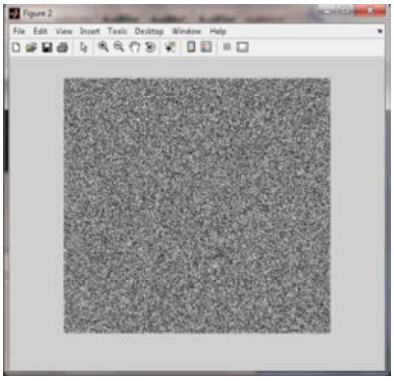
(1, F (1)) = 3
(2, F (2)) = 5

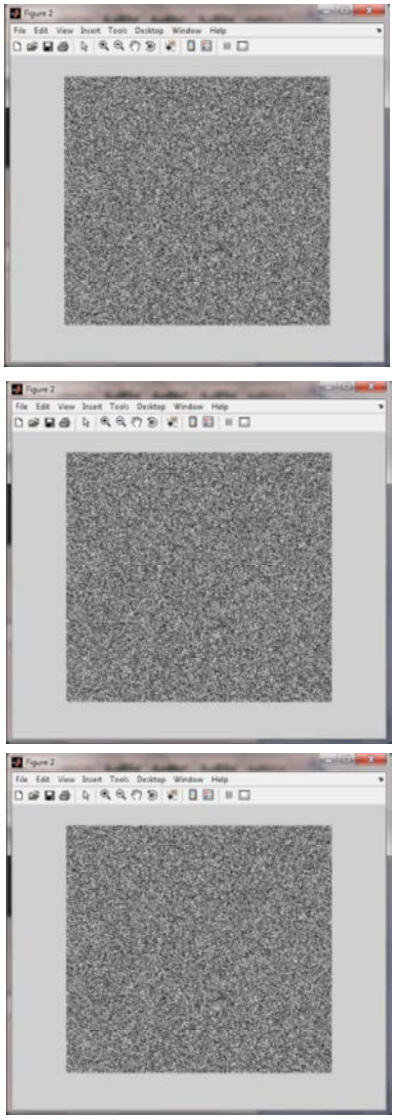
Reconstruction: With the individual and unique keys and the shares given to the participants the original image and EPR can be retrieved. Lagrange's interpolation technique extracts the secret by getting back the polynomial. The constant part of the polynomial is the secret [10]. Every part of the image and the text in every share created so it is convenient to interpolate the polynomials of at least k shares to get back the secret. Even in the case of embedding an image into another image both the images can be retrieved separately.

Simulation Results: In this section examples are provided to illustrate the effectiveness of the proposed method. A medical 2D X-Ray medical image has been taken and an EPR has been hidden inside it [11].

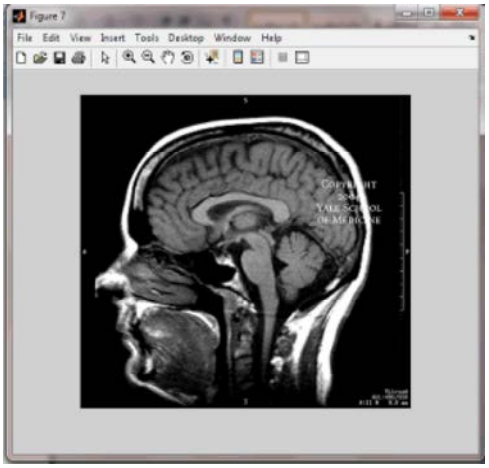
Medical Image

FARABI HOSPITAL
patient name: Raja
Date of birth:18-08-1991
Patient age:21
Patient Address:~~~
Patient Weight:60 kg.
Blood Pressure:Normal
Cause for admission:Encephalitis

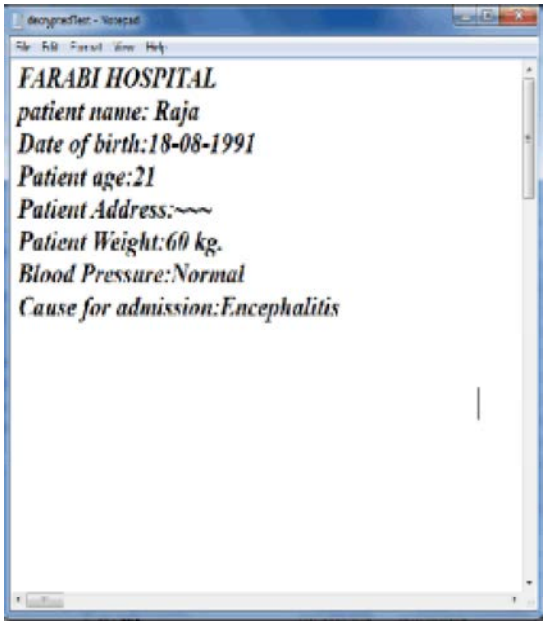




Obtained shares



Reconstructed secret image



Decrypted EPR

During decryption process the secret medical image and the text are retrieved without much distortion to it.

CONCLUSION

In this paper important medical information in textual form (EPR) are hidden into a secret medical image. This image is then divided into n noise like shares which are unique. In order to avoid any adverse security threats only k or more such shares are sufficient to recover the original text and the image. In case of image embedded in an image both the images can be retrieved efficiently. The recreated image and the recovered text have almost no change from that of the original [12-15].

REFERENCES

1. Acharya, R.U., P.S. Bhat, S. Kumar and L.C. Min, 2003. Transmission and storage of medical images with patient information. Computers in Biology and Medicine, 33: 303-310.
2. Lou, D.C., M.C. Hu and J.L. Liu, 2009. Multiple layer data hiding scheme for medical images. Computer Standards and Interfaces, 31: 329-335.
3. Shih, F.Y. and Y. Ta Wu, 2005. Robust watermarking and compression for medical images based on genetic algorithms. Journal of Information Sciences, 175(3): 200-216.

4. Woo, C.S., J. Du and B. Pham, 2005. Multiple watermark method for privacy control and tamper detection in medical images. In: Proceedings of APRS Workshop on Digital Image Computing, Australia, pp: 59-64.
5. Zhou, X.Q., H.K. Huang and S.L. Lou, 2001. Authenticity and integrity of digital mammography *images*. IEEE Transaction on Medical Imaging, 20(8): 784-791.
6. Nayak, J., P.S. Bhat, U. Rajendra Acharya and M. Sathish Kumar, 2009. Efficient storage and transmission of digital fundus images with patient information using reversible watermarking technique and error control codes. Journal of Medical Systems, 33: 163-171.
7. Kumaravel, B. Anatha Barathi, 2013. Personalized image search using query expansion, Middle-East Journal of Scientific Research, ISSN: 1990-9233, 15(12): 1736-1739.
8. Kumaravel, A. and R. Udayakumar, 2013. Web Portal Visits Patterns Predicted by Intuitionistic Fuzzy Approach, Indian Journal of Science and Technology, ISSN: 0974-6846, 6(5S): 4549-4553.
9. Kumaravel, A. and K. Rangarajan, 2013. Algorithm for Automation Specification for Exploring Dynamic Labyrinths, Indian Journal of Science and Technology, ISSN: 0974-6846, 6(5S): 4554-4559.
10. Kumaravel, A. and Oinam Nickson Meetei, 2013. An Application of Non-uniform Cellular Automata for Efficient Crytography, Indian Journal of Science and Technology, ISSN: 0974-6846, 6(5S): 4560-4566.
11. Mustafa Ulutas, Güzin Ulutas and Vasif V. Nabiyev, 2010. Medical image security and EPR hiding using Shamir's secret sharing scheme. The Journal of Systems and Software, 84(2011): 341-353.
12. Chao, H.M., C.M. Hsu and S.G. Miaou, 2002. A data-hiding technique with authentication, integration and confidentiality for electronic patient records. IEEE Transactions on Information Technology in Biomedicine, 6(1): 46-53.
13. Pattanayak, Monalisa. and P.L. Nayak, 2013. Green Synthesis of Gold Nanoparticles Using Elettaria cardamomum (ELAICHI) Aqueous Extract World Journal of Nano Science & Technology, 2(1): 01-05.
14. Chahataray, Rajashree. and P.L. Nayak, 2013. Synthesis and Characterization of Conducting Polymers Multi Walled Carbon Nanotube-Chitosan Composites Coupled with Poly (P-Aminophenol) World Journal of Nano Science and Technology, 2(1): 18-25.
15. Parida, Umesh Kumar, S.K. Biswal, P.L. Nayak and B.K. Bindhani, 2013. Gold Nano Particles for Biomedical Applications World Journal of Nano Science and Technology, 2(1): 47-57.