ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 4, April 2014

A Survey on Patient Information Protection Using Cryptographic and Data Hiding Techniques

Usha B A[1], Dr. N K Srinath[2], Aditya Nanjangud[3], Abhineet M Deshpande[4], Anthony Rebello[5]

Assistant Professor, Department of CSE, R V College of Engineering, Bangalore, India [1]

Professor and Dean PG Studies, Department of CSE, R V College of Engineering, Bangalore, India [2]

UG Final Year, Department of Computer Science & Engineering, R V College of Engineering, Bangalore, India[3,4,5]

Abstract: This paper describes the need to protect patient information in digital form and some of the methods that exist to do so. The methods described utilize cryptographic and data hiding concepts, which are explained in brief. The paper summarizes the basic functionality a patient information protection system must offer and explains the basic methodology adopted in most of the existing methods.

Index Terms: Patient information protection, reversible data hiding, patient privacy, tele-medicine.

I. INTRODUCTION

Medical information such as patient medical history and related patient information is moving on to digital media to take advantage of the benefits of technology such as high resolution images like CT-SCAN and X-RAY results, as well as fast transmission of the information between doctors, patients and specialists. However, this introduces new threats such as breach of privacy and tampering of results. Patients are given the privilege of 'doctor – patient confidentiality', and have the right to determine how and when their health information is shared. If such information is disclosed to an employer, insurer, or the general public, it can result in discrimination or embarrassment. Thus, it is important to transmit and archive such information while maintaining confidentiality and availability.

For a diagnosis, it is better to give the doctor complete information and more importantly, the right information. While transferring data, there is a threat of modification which can alter such data. Thus, integrity of the information is also important. Additionally, when hard copy reports are given to doctors, they are enveloped with the patient id (if not directly written on the report itself). In such cases, there is a chance of two reports being swapped. The paper addresses these issues in section II.

Cryptography is the art of protecting information by transforming it into an unreadable form such that one can make sense of it only by converting it back into the readable form. To do so, a key is required. The process of making the information unreadable is called "Encryption", and the process of making it readable is "Decryption". If both processes use the same key, it is classified as "symmetric" and if not, "asymmetric". Steganography is the art and science of invisible communication. This can be done by hiding some information within some other information. It differs from cryptography, as cryptography keeps the content or information a secret, but steganography actually hides the information, keeping its existence a secret [1].

Thus by applying cryptography and steganography, the existence of the data and the data itself is protected. With medical information, cryptography and steganography can be used together to protect patient information and the medical results as well.

II. A BASIC PATIENT INFORMATION PROTECTION SYSTEM

A system which addresses patient privacy concerns must first establish what it tries to protect, the available methods and how to do so. A basic system to do so has been described below.

A. Information that needs to be protected

The information that needs to be protected is the patient's personal details, the medical history (including past test results) and all current test reports.

B. Methods to protect such information

There are two broad ways of protecting the information.

1. Do not associate any identification information directly with any diagnosis, results or reports: By not associating any id with the reports, an unauthorized person who gets a hold of the data cannot associate an identity to it. Thus, the patient's privacy is still maintained.

2. Perform encryption on the medical information: By encrypting the reports, even if the attacker gains access to the reports, interpreting it will be difficult. This however relies on the strength of the encryption algorithm and proper management of the key between concerned parties such as the doctor, patient etc.

C. Method details and drawbacks

Not associating any identification information with the diagnosis leads to the possibility of two reports belonging to two different patients being swapped. If the identification is not on the report, then it has to be on something enveloping the report. Take for instance, the structure of a filename which identifies the patient. The document itself has no information about identifying the

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 4, April 2014

patient but the filename does. If the filenames of two files were swapped, then the reports themselves are also swapped. This can lead to wrong diagnosis of both patients. Encryption on the medical information which contains the identity would seem better. However, it relies completely on proper key management and the strength of the encryption.

Thus, both have their strengths and weaknesses. However, the first method can still be improved by not associating the identification "directly". Using a data hiding scheme, the identification data can be embedded in the report. This makes sure that the report itself contains the information about a patient while not disclosing it directly. While diagnosing, the data can be retrieved to check which patient it is for. Furthermore, the report with embedded data can be encrypted for stronger security. The attacker would need to decrypt the information and extract the hidden data to cause damage.

Thus it is established that both cryptography and steganography together can be used to protect medical information in digital form. Cryptography used to encrypt the reports and steganography to embed the identification.

III. ENCRYPTION OF COVER IMAGE AND HIDING DATA

Section II concluded with using both cryptography and steganography to improve security. The order in which this is done can also improve the security. The general order seems to be encryption and then embedding of data [2][3][4]. A medical image say M is first encrypted, and data D is then embedded into it. The advantage of this approach is that decrypting to get back M would require accurate removal of D and reconstruction of those portions where D was present. This is accomplished using a technique called "Reversible Data Hiding" [5][6][7]. The basic idea is to be able to get back the same information that was replaced when data was embedded there. There are quite a few approaches to achieve reversible data hiding, some of which take advantage of properties such as entropy and standard deviation[5][6][7]. The methodology to encrypt and embed data has been well explained in [4]. The image is first encrypted with an asynchronous stream cipher proposed by the author. The key is then ciphered using an asymmetric algorithm. And lastly, the enciphered key is embedded into the previous encrypted image. The algorithms for encryption and data hiding are fully present in [4]. The advantage is that the image and the key are securely sent together, and the method proposed is robust to noise.

[2] uses [4] as a reference and follows in the same path of encrypting the image and then embedding data. The image is first split into two images using two shares mechanism of visual cryptography. Splitting the image into two would give more space and thus be able to embed more data [4]. One such example is using visual cryptography two share mechanism to do so [2]. Using another medical image, which may not belong to the patient, might lead to better security [2]. The reason being, if security is breached, then the attacker decrypts an image, he or she will assume that to be the information being protected. Unfortunately, this depends on the attacker taking the bait.

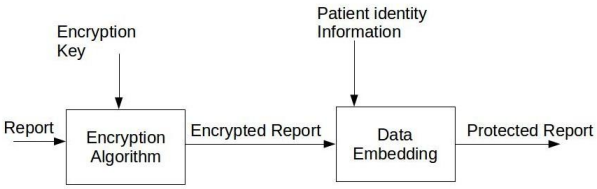

Fig.1. Encryption and Data Hiding stage

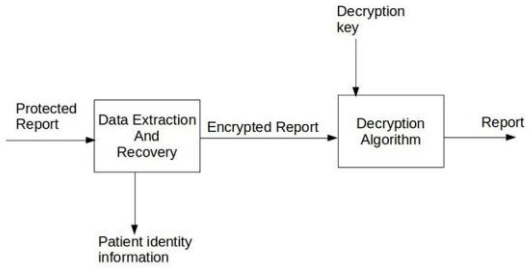

Fig.2. Data extraction and decryption stage

There are techniques of embedding data directly into encrypted images such that decrypting the images without removing the embedded data will give an image "similar" to the original image. However, it would be favorable in the current situation to embed data in such a way that decrypting it without removing data yields a quite different image. Thus, only by extracting the data and repairing the portions where data was embedded (reversible data hiding) , will the decryption yield the correct image. This is useful when both the cover image and the data are important. Here, the encrypted report being cover image and the data being patient identity information. If more focus is given to embedding data such as the patient identity information, and there is no need for encryption of the cover image, then the data can be embedded in the areas that are not of interest [8]. In such a case, data can be extracted, and recovery is not necessary as it doesn't interfere with a diagnosis. Although care must be taken that it successfully finds the regions of interest and embeds the data in areas except it. In such a situation, unless perfectly guaranteed, the reversible data hiding scheme seems safer.

IV. GENERALIZED METHODS OF PATIENT INFORMATION PROTECTION

Fig. 1 describes the encryption and embedding stage. It takes a report which is considered to be an image, and encrypts it using an encryption key. This encrypted report is then passed to the data hider that embeds the patient identity information. The result is the "protected copy" of the report or simply "protected report". The figure just describes the embedded data to be patient identity information. But as part of key management, the encryption key can also be embedded.

Fig. 2 describes the extraction and decryption stage. It takes the "protected report" and first extracts the embedded data. During extraction, it also recovers the original cover image data. After recovering the encrypted report, it is then decrypted using the decryption key. In case of symmetric

encryption it is the same as the key used to encrypt the image. The encryption and decryption components can be implemented using any cryptographic scheme. A two – share visual cryptography scheme can be used [2] .Stream ciphers can also be used [2]. The Advanced Encryption Standard (AES) algorithm in Electronic Code Book (ECB) mode was used as the cryptographic module for the task [6]. Stream ciphers are robust to moderate noise like JPEG compression with high quality factor [2]. Instead of sequentially performing encryption and then data hiding on the entire image, it can be performed together say, on each block being encrypted [6]. For every block that is encrypted, one bit of cipher text is modified to hide the data. During decryption, the hidden data is extracted, but those bits have already overwritten the original data. By encrypting the image, the total entropy of the image had increased. Hence, for each marked cipher text, the decryption function is applied for the marked text being 0 and the marked text being 1. The local standard deviation of the two blocks are compared and the lesser one is selected.

V. CONCLUSION

Hospitals and clinics are translating hard copies into digital form for faster retrieval and transfer. This paper has addressed the need for security when in such form. A few approaches to ensure privacy have been looked at and encryption followed by data hiding is a promising approach. The data hiding scheme to be used should be reversible and should embed the data in such a way that decryption of the stego image yields a result with minute similarity to the cover image. When hiding the data, the patient identity is the most important as it needs to be associated with the report but not publicly known, to ensure privacy.

REFERENCES

[1] T. Morkel, J.H.P. Eloff, M.S. Olivier, "An Overview of Image Steganography" ICSA Research group
[2] Vinay Pandey, Manish Shrivastava,"Medical Image Protection using steganography by crypto-image as cover image", International Journal of Advanced Computer Research,vol. 2, issue 5, September 2012
[3] Vinay Pandey, Angad Singh, Manish Shrivastava, "Medical image protection using cryptography, data-hiding and steganography", International Journal of Emerging Technology and Advanced Engineering, vol. 2, issue 1, January 2012
[4] W. Puech, "Image Encryption and Compression for Medical Image Security", 1st International Workshops on Image Processing Theory, Tools and Applications, Tunisie, IPTA'08
[5] Xinpeng Zhang, "Reversible Data Hiding in Encrpyted Image" IEEE Signal Processing Letters, vol. 18, no. 4, April 2011
[6] W. Puech, "A Reversible Data Hiding Method for Encrypted Images", IS&T/SPIE Electronic Imaging 2008 - Security, Forensics, Steganography and Watermarking of Multimedia Contents, 2008
[7] Zhicheng Ni, Yun-Quing Shi, Nirwan Ansari, Wei Su, "Reversible Data Hiding" IEEE Transactions on Circuits and Systems for video technology, vol. 16, no. 3, March 2006
[8] Ming Yang, Monica Trifas, Lei Chen, Lei Song, Dorothy Buenos-Aires, Jaleesa Elston, "Secure Patient Information and Privacy in Medical Imaging " Systemics, Cybernetics and Informatics, vol. 8, no. 3, 2010.