International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-2 Number-3 Issue-5 September-2012

Medical Image Protection using steganography by crypto-image as cover Image

Vinay Pandey[1], Manish Shrivastava[2]
IT department LNCT, RGPV, Bhopal, India

Abstract

This paper presents securing the transmission of medical images. The presented algorithms will be applied to images. This work presents a new method that combines image cryptography, data hiding and Steganography technique for denoised and safe image transmission purpose. In This method we encrypt the original image with two shares mechanism encryption algorithm then embed the encrypted image with patient information by using lossless data embedding technique with data hiding method after that for more security. We apply steganography by encrypted image of any other medical image as cover image and embedded images as secrete image with the private key. In receiver side when the message is arrived then we apply the inverse methods in reverse order to get the original image and patient information and to remove noise we extract the image before the decryption of message. We have applied and showed the results of our method to medical images.

Keywords

Data Hiding, Data Embedding, Data Extraction, Decryption, Denoising, Encryption, Steganography.

1. Introduction

The need of fast and secure transmission is vital in the medical world. Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over the net. In this paper we propose a new technique to cipher an image for safe and denoised transmission. Our research deals with image cryptography, data hiding and steganography. There are several methods to encrypt binary or grey level images [1,2,3].

Watermarking can be an answer to make secure image transmission. For applications dealing with images, the watermarking objective is to embed invisibly message inside the image [1]. To embed the encrypted image in the patient information we have used a lossless watermarking technique.

A secret sharing scheme shares a secret into a number of shares so that the cooperation of a predetermined group of shareholders reveals the secret whereas the secret reconstruction is impossible for any unauthorized set of shareholders. Visual cryptography is a kind of secret sharing in which the secret reconstruction can be done only by the human visual system [4].

In previous method owner encrypts the original uncompressed image using an encryption key to produce an encrypted image and then a data hider embeds additional data into the encrypted image using. a data-hiding key But there was a problem To decrease the transmission time, the data compression is necessary. Since few years, a new problem is trying to combine in a single step, compression, and encryption and data hiding .So far, few solutions have been proposed to combine image encryption and compression for example. Nowadays, a new challenge consists to embed data in encrypted images. Since the entropy of encrypted image is maximal, the embedding step, considered like noise, is not possible by using standard data hiding algorithms. A new idea is to apply reversible lossless data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. there was another problem if either of data hiding key or encryption key is leaked then the intruder can extract or decrypt the message and can see the patient information through data hiding key or decrypt the message through encryption key. To resolve this problem we use steganography by using crypto-image of other medical image so we finds that the other encrypted image covers the embedded image and if any hacker decrypt the image then He will assume that the decrypted other medical image is real one[3][5].

In the Section 2, firstly we present encryption algorithm two share mechanism, Section 3, we describe the steganography. Section 4, we describe the combination method. Section 5 describes the result for encrypted and embedded images using our proposed algorithm. Section 6 describes the conclusion.

2. Visual Cryptography

According to the algorithm, each pixel of the binary-valued secret image is expanded into 2*2 pixels, To share a white pixel of the secret image, one row from the first 6 rows of 2*2 pixels randomly. Similarly, the two shares of a black pixel are determined by a random selection from the 6 last rows of 2*2 pixels. As a result, an M*N pixels secret image is expanded into two 2M*2N pixels share-images. Considering security of the method, presence of only one share image reveals nothing about the corresponding secret image, i.e., each 2*2 pixels block of one share-image may correspond to either a white pixel or a black pixel of the secret image [6][7].

3. Steganography

Steganography is used to convey secret messages under the cover of digital media such as images. Although only the most insignificant components are altered, many analytical techniques can reveal existence of the hidden message by detecting statistical difference between the cover and stego objects [8].

In most of the information hiding systems, the cover media undergoes some distortion due to embedding of secret message data. That is some irreversible (permanent) distortion is caused to the cover media, even after the hidden message is extracted. In some applications like, medical images, military, instances where media is used as evidence in courts and law enforcement, in additional imperceptibility, reversibility of the cover media is desired. The masking techniques satisfying this requirement are referred as reversible, lossless, distortion-free or invertible information hiding techniques [9].The basic model is shown in Figure 1.Consider that an encoder consists of a cover image *C* (which acts as a carrier), and the message *M* is the data that a sender wishes to communicate confidentially. embed the message by using a reversible data hiding technique controlled by stego–key *K. K* is a shared secret with the intended recipient whose knowledge of the key enables them to decode the message from the stego-image. In the most general sense, a stego-key can be derived from the design parameters of a particular stenographic method used for embedding information [10].

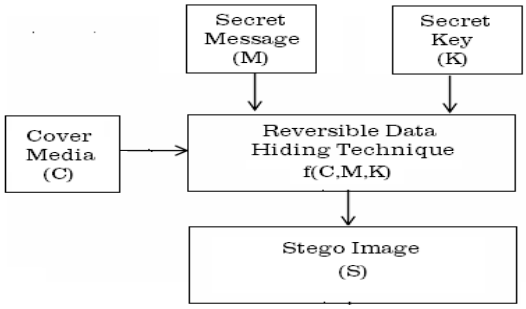

Figure 1: Basic Reversible Information Hiding System Encoder

In this paper we present an approach, in which the stego-key is the algorithm itself. The resulting stego-image obtained after embedding information is represented as *S=f(C,M,K)*. *S* is transmitted over a channel to the receiver where it is processed by the stego decoder using the same key *K.* An interceptor of the stego image is expected to only see the image without any obvious indication of the embedded hidden message. Recovering the hidden message *M* and original image '*O'* from stego-image *S.* the decoding is similar to encoding, and is shown in figure 2 [8].

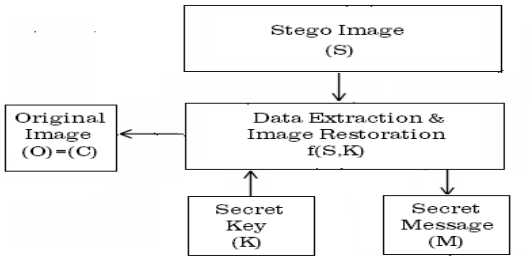

Figure 2: Basic Reversible Information Hiding System Decoder

4. Decryption of the Combination of the Methods

In this section we describe how it is possible to combine the techniques of encryption, data hiding and steganography in image. a new problem is trying to combine in a single step, compression, encryption and data hiding. So far, few solutions have been proposed to combine image encryption and compression for example. Nowadays, a new challenge consists to embed data in encrypted images. Since the entropy of encrypted image is maximal, the embedding step, considered like noise,

is not possible by using standard data hiding algorithms. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption [4].

In This method we encrypt the original image with two share mechanism then embed the encrypted image with patient information by using lsb lossless data embedding technique with data hiding key after that for more security. We apply steganography in embedded image as secrete image and encrypted image of any other medical image as a cover image. In receiver side when the message is arrived then we apply the inverse methods in reverse order to get the original image and patient information and to remove the noise we apply extraction before the decryption. The propose scheme is shown in below figure 3.

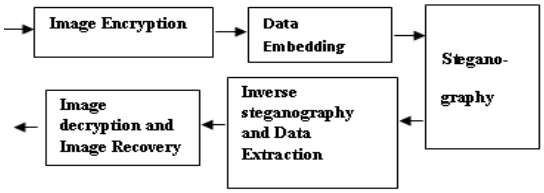

Figure 3: Sketch of proposed scheme

5. Result

The Fig.4(a) is the original image. We encrypt the original Image and get fig. 4(b) and apply data hiding on fig.4(b) with patient information and get fig. 4(c) after that we apply steganography and then we get Stenographic image using crypto image as shown in fig 4(d) and then send the fig 4(d) to the receiver side.

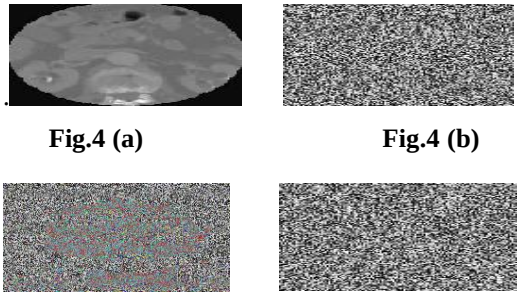

Fig.4 (a) **Fig.4 (b)**

Fig.4 (c) **Fig.4 (d)**

Figure4: a) Original medical image, b) Encrypted image) Watermarked encrypted image, d) Steganograph image

6. Conclusion

In this work a combined approach of cryptography, data hiding and steganography is used. In this method the original image is encrypted using two share method then the encrypted image is embedded using lossless lsb data hiding method with patient information. In the Previous methods less security and more noise is found so we applied steganography for more security and in the receiver side applied reversible data hiding algorithm on encrypted image to remove the embedded data before the image decryption. So that we find more secured and denoised medical image.

7. Acknowledgment

My express thanks and gratitude to all the departments' personals and sponsors who give me a opportunity to present and express my paper on this level. I wish to place on my record my deep sense of gratitude to all reference papers authors for them valuable help through their papers, books, websites etc.

8. Literature Review

In 2011, Reversible data hiding in encrypted image Xinpeng Zhang proposed a method where owner encrypts the original uncompressed image using an encryption key to produce an encrypted image and then a data hider embeds additional data into the encrypted image using. a data-hiding key But there was a problem to decrease the transmission time, the data compression is necessary. Since few years, a new problem is trying to combine in a single step, compression, encryption and data hiding. So far, few solutions have been proposed to combine image encryption and compression for example. Nowadays, a new challenge consists to embed data in encrypted images. Since the entropy of encrypted image is maximal, the embedding step, considered like noise, is not possible by using standard data hiding algorithms. In the previous method also problem of security and noise is found in the image. So in the proposed method A new idea is to apply reversible lossless data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption so that we found less noisy image in the receiver side and for more security we apply steganography method.

References

[1] Puech, William. "Image Encryption and Compression for Medical Image Security." In IPTA'08: 1st International Workshops on Image Processing Theory, Tools and Applications. 2008.

[2] Yang, Ming, Monica Trifas, Lei Chen, Lei Song, D. B. Aires, and Jaleesa Elston. "Secure patient information and privacy in medical imaging." J. Syst. Cybern. Inf 8, no. 3 (2010): 63-66.

[3] Zhang, Xinpeng. "Reversible data hiding in encrypted image." Signal Processing Letters, IEEE 18, no. 4 (2011): 255-258.

[4] Naor, Moni, and Adi Shamir. "Visual cryptography." In Advances in Cryptology—EUROCRYPT'94, pp. 1-12. Springer Berlin Heidelberg, 1995.

[5] Puech, William, Marc Chaumont, and Olivier Strauss. "A reversible data hiding method for encrypted images." In Electronic Imaging 2008, pp. 68191E-68191E. International Society for Optics and Photonics, 2008.

[6] Arti Gupta, Manish Shrivastava," Performance of ANN using Back Propagation Algorithm for Medical Diagnosis System", International Journal of Advanced Computer Research (IJACR), Volume-2,Number-1,Issue-3,March-2012.

[7] Naor, Moni, and Adi Shamir. "Visual cryptography II: Improving the contrast via the cover base." In Security Protocols, pp. 197-202. Springer Berlin Heidelberg, 1997.

[8] Zhang, Weiming, Xinpeng Zhang, and Shuozhong Wang. "A double layered "plus-minus one" data embedding scheme." Signal Processing Letters, IEEE 14, no. 11 (2007): 848-851.

[9] Zhicheng Ni et al. "Reversible Data Hiding", IEEE Transactions on Circuits and Systems for Video Technology, Vol.16, No.3, March 2006.

[10] Arjun, Santosh, and Narasimha Rao. "An approach to reversible information hiding for images." In TENCON 2008-2008 IEEE Region 10 Conference, pp. 1-6. IEEE, 2008.

Vinay Pandey LNCT Bhopal (M.P) Mtech 4rth Semester pursuing in LNCT Bhopal from RGPV University (M.P) India.