Volume 2, Issue 12, December 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure Medical Image Transmission using Combined Approach of Data-hiding, Encryption and Steganography

Vinay Pandey
IT Department, LNCT RGPV Bhopal
M.P., India

Manish Shrivastava
IT Department ,LNCT RGPV Bhopal
M.P., 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 data hiding encryption and Steganography technique for denoised and secure image transmission purpose. In this method we embed the original image with patient information by using lossless LSB data hiding method then apply two shares encryption algorithm for encryption of embedded image so that both image and patient information is completely encrypted after that for more security and cover completely to embedded encrypted image .We apply steganography by medical image of any other as cover image and embedded encrypted image 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 denoised original image and patient information. We have applied and showed the results of our method to medical images.***

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

I. 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 secure and denoised transmission. Our research deals with image encryption, data hiding and steganography. There are several methods to encrypt binary or grey level images [1,2,3]. Watermarking can be an answer to merge image with patient information. For applications dealing with images, the watermarking objective is to embed visibly or invisibly message inside the image. [1] To embed the image in the patient information we have used a lossless LSB 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 methods 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 But there was a problem To decrease the transmission time and recover the image and patient information. To reduce 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, it is not possible by using standard data hiding algorithms. A new idea is to apply reversible lossless data hiding algorithms on image before encryption is done. there was another problem that the image and patient information is not completely hidden so with the help of image analysis intruder can decrypt the image or 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 other medical image and if any hacker get the image then He will assume that the other medical image is real one. [3][5]

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

II. 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 patterns of 2*2 pixels randomly. Similarly, the two shares of a black pixel are determined by a random selection from the 6 patterns 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. The key is used for encryption and decryption of image [6][7]

III. STEGANOGRAPHY

Steganography is used to convey secret messages under the cover of digital media such as images. Although only the least significant 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 and secret image 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. [9].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 steganographic method used for embedding information [10]

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,[8]

A .Least Significant Bit Substitution

Here we are using LSB steganography, the least significant bits of the cover media's digital data are used to conceal the message. The simplest of the LSB steganography techniques is LSB replacement. LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be hidden. Consider an 8-bit greyscale bitmap image where each pixel is stored as a byte representing a greyscale value. Suppose the first eight pixels of the original image have the following greyscale values:

11010010
01001010
10010111
10001100
00010101
01010111
00100110
01000011

To hide the letter C whose binary value is 10000011, we would replace the LSBs of these pixels to have the following new greyscale values:

11010011
01001010
10010110
10001100
00010100
01010110
00100111
01000011.

Note that, on average, only half the LSBs need to change. The difference between the cover (i.e. original) image and the stego image will be hardly noticeable to the human eye.[11]

IV. DESCRYPTION 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 for security of 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, it is not possible by using standard data hiding algorithms. A new idea is to apply reversible lossless data hiding algorithms on image before encryption is done. there was another problem that the image and patient information is not completely hidden so with the help of image analysis intruder can decrypt the image or 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 [3][4][5]

In this method we embed the image with patient information by using LSB lossless data embedding technique then encrypt the embedded image with two-share mechanism then after that for more security ,We apply steganography in embedded encrypted image as secrete image and 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. The propose scheme is shown in below fig.1.

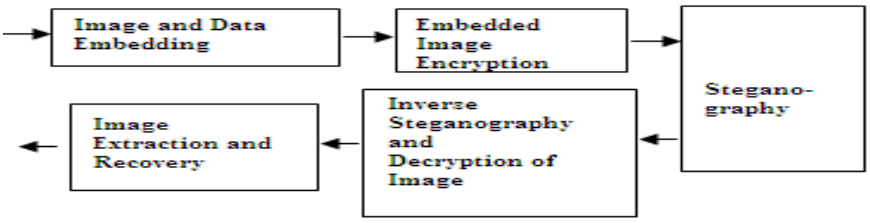

Fig. 1.Sketch of proposed scheme.

V. RESULT

The Fig.2(a) is the original image. We embed the original Image with patient information and get fig. 2(b) and apply encryption on fig.2(b) and get fig. 2(c) after that we apply steganography and then we get stegnographed image using other medical image as shown in fig 2(d) and then send the fig 2(d) to the receiver side.

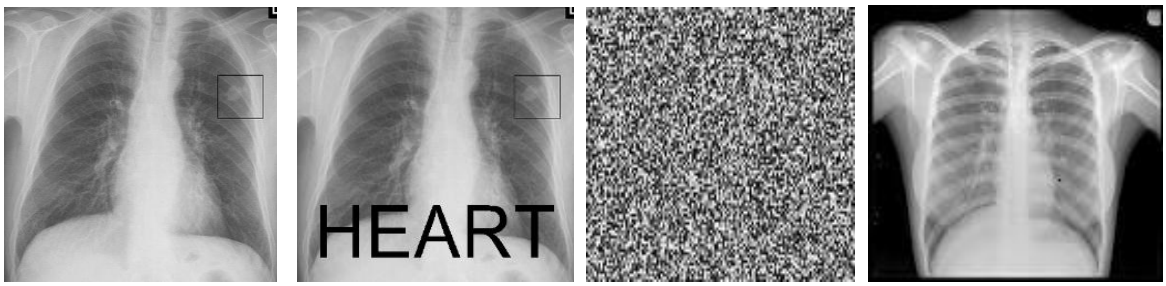

Fig 2(a) Fig. 2(b) Fig 2(c) Fig. 2(d)

Fig. 2: a) Original medical image b) Embedded image c) Encrypted Watermarked image d) Steganographed image using other medical image as cover image

VI. CONCLUSION

In this work A combined approach of data-hiding,encryption and steganography is used. In this method the image is embedded using lossless LSB data hiding method with patient information and then embedded image is encrypted using two share method. In the Previous methods partial encryption, less security and more noise is found so we applied encryption after embedding of image with patient information for complete encryption of both image and patient information and applied steganography for more security so that complete information of the embedded encrypted image is hidden and A new idea is to apply reversible lossless data hiding algorithms on image before encryption is done. So that we find more secured and denoised medical image.

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.

REFERENCES

[1] W. Puech" Image Encryption and Compression for Medical Image Security" PROCEEDING OF IEEE Image Processing Theory, Tools & Applications.

[2] Ming YANG,Lei SONG,Monica TRIFAS,Dorothy BUENOS-AIRES,Lei CHEN, Jaleesa ELSTON," Secure Patient Information and Privacy in Medical Imaging IEEE "

[3] Xinpeng Zhang]ieee signal processing letters, VOL. 18, NO. 4, APRIL 2011 255 Reversible Data Hiding in Encrypted Image

[4] M. Naor, and A. Shamir, "Visual Cryptography", *Advances in Cryptology – Eurocrypt'94 Proceeding, LNCS* Vol. 950, Springer-Verlag,1995, pp. 1-12.

[5] W. Puech, M. Chaumont, and 0. Strauss. A Reversible Data Hiding Method for Encrypted Images. In Proc. SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, volume 6819, pages 68191E-1-68191E-9, San Jose, CA, USA, January 2008.

[6]. M. Naor, and A. Shamir, "Visual Cryptography", Advances in Cryptology – Eurocrypt'94 Proceeding LNCS Vol. 950, Springer-Verlag, 1995, pp. 1-12.

[7] M. Naor and A. Shamir, "Visual Cryptography II: Improving the Contrast Via the Cover Base", CambridgeWorkshop on Protocols, 1996.

[8] Weiming Zhang, Xinpeng Zhang, and Shuozhong Wan. A Double Layered "Plus-Minus One" Data Embedding Scheme

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

[10]An Approach To Reversible Information Hiding For Images Santosh Arjun, IEEE Member, NVIDIA, . Bangalore, India. Narasimha Rao, IEEE Student Member Electronics and Communication Engineering

[11] A steganography algorithm for hiding image in image by improved lsb substitution by minimize detection **1vijay Kumar Sharma ,2vishal Shrivastav**1M.Tech. scholar, Arya college of Engineering & IT , Jaipur , Rajasthan (India) 2 Associate Professor Arya college of Engineering & IT, jaipur, Rajasthan (India)

