Medical Image Encryption by Using Crypto-Data hiding and Segmentation

Vinay Pandey[1], Dr. Sudhir Kumar Meesala[2], Nilesh Gupta[3]

[1]*Asst. Prof. CSE Department, Chouksey Engineering College, CSVTU, Bhilai, India*
[2]*Asst. Prof. CSE Department, Chouksey Engineering College, CSVTU, Bhilai, India*
[3]*Asst. Prof. CSE Department, Chouksey Engineering College, CSVTU, Bhilai, India*

Abstract: This paper presents the problem of protecting the transmission of medical images. The presented algorithms will be applied to images .This work presents a new method that combines image encryption, data hiding and segmentation technique for safe medical image transmission purpose. This method is based on the combination of public and private keys ciphering. The medical image and patient information is embedded then we segment the embedded image into two parts using segmentation. The encryption algorithm with public and private key is applied to the two parts of embedded image. We segment the embedded message into two parts and then first part is encrypted by receiver public key using RSA algorithm and second part is encrypted by sender private key using RSA algorithm and then we desegment the encrypted parts and send the message to the receiver . In receiver side when message is arrived then receiver segment the message in two parts and decrypt the first part by receiver private key using RSA algorithm and second part by sender public key using RSA algorithm. Then apply desegmentation and extraction so that we can find original message. So message is more secured because in single image we use two different key in two parts of image using segmentation without key sharing .We have applied and showed the results of our method to medical images.

Keywords: Encryption, Data hiding, Decryption, segmentation, Steganography.

I. INTRODUCTION

The amount of digital medical images have increased rapidly in the Internet. The necessity of fast and secure diagnosis 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 segmentation. There are several methods to encrypt binary or grey level images [1,2,3]. Image segmentation is the process of dividing an image into sections, regions, or parts [5] [6].

In past existing method sender encrypts the original image using an encryption key to produce a ciphered image, and then a data-hiding method Embeds additional data into the ciphered image using data-hiding key But there was a problem of sharing the key to the receiver because when sender sends the key either by embedding with the encrypted image or by other way like mail and telephone then anyone will get the key then he can decrypt the message. To resolve this problem we use public and private key method using segmentation. [7]. In the Section 2, firstly we present segmentation. Section 3, we describe data hiding 4, RSA algorithm Encryption Section 5, we describe the combination method. Section 6 Expected outcomes.

II. SEGMETATION TECHNIQUE

A. The Segmentation Method

Segmentation is one of the early methods in image analysis. segmentation is the process of dividing a digital image into many sets . Implementation of image segmentation expand from filtering of noised images, binary imaging, visualize objects in satellite images and many other fields. [8]

III. DATA HIDING /WATERMARKING

Data-hiding can be a method to make safe image transmission .For applications related with images, the data-hiding objective is to embed a message inside the image. Information can be hidden with success in text, image, audio/image, and protocol file formats. There are two main groups of information hiding techniques: techniques in the spatial domain and techniques in the transform domain. Spatial domain techniques generally involve manipulation of pixel intensity. Lossless image formats are most suited for spatial domain techniques .The most well-known technique of information hiding in the image domain is Least Significant Bit (LSB) algorithm. In this algorithm, the least significant bit, which will affect pixel color the least, is examined and either changed or not changed so that it matches the bit that is to be embedded. The algorithm can either adjust every least significant bit or, for greater security, adjust only every nth bit with *n* being known only to the message recipient thus Providing and additional level of security. [9]

IV. PUBLIC KEY CRYPTOSYSTEM

In public key cryptosystem, decryption and encryption can be separated and communication parties needn't prior exchanged keys can establish a secure communications since the key for decryption and encryption are different. This is a good solution to the traditional cryptography system in network communication. The features of public-key cryptosystem as follows. For every user produces a pair of keys (public key and private key) and public key is public while private key is confidential. It is very difficult from public key to conclude private key. When A and B communicate, A can obtain B's public key in any way then use the key to encrypt information. The encrypted messages can be sent through any unsafe way. After receiving the cryptograph, B can use his own private key to decrypt the cryptograph and recover the communication information expressly.[10]

The method for RSA algorithm is as follows.[10][11]
(1) find two large primes p, q;
(2) n = p * q, z = (p - 1) * (q-1);
(3) select a number e which is less than n and prime to z, so that e and z have no common factors;
(4) select another number d, where (e*d - 1) is divisible by z;
(5) the public key is (n, e) and the private key is (n, d);
(6) for a message m, if the cipher text is c, decryption and
encryption process as follows.
encryption: c = m ^ e mod n.
decryption: m = c ^ d mod n.

V. DESCRIPTION OF COMBINATION OF THE METHODS

In this section we describe how it is possible to combine the techniques of encryption, data hiding and segmentation in image. Indeed, we constructed a new method with encryption, data hiding algorithm with segmentation for the image, the encryption based on public private key for the image with segmentation method. For example, if a medical doctor *M* wants to send by network, a medical image to a specialist *S*, it should be made in a safe way. To do that, we embed the medical image and patient information .the doctor *M* can segment medical image in two parts and then first part is encrypted by receiver public key using RSA algorithm and second part is encrypted by sender private key using RSA algorithm and then we desegment the embedded encrypted image to the receiver . In receiver side when message have arrived then receiver segment the message into two parts and then decrypt the first part by receiver private key using RSA algorithm and second part by sender public key using RSA algorithm Then apply de segmentation and extraction to recover the original image. We have applied and showed the expected results of our method to medical images.

VI. EXPECTED OUTCOME

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

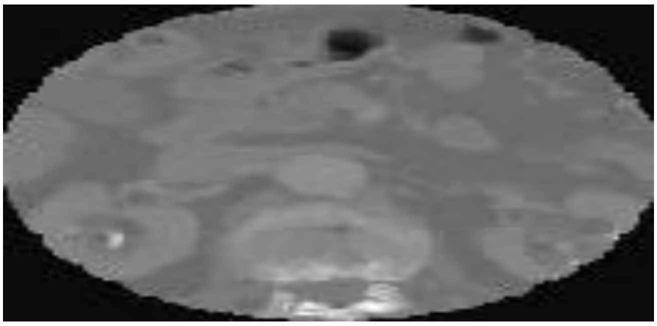

Fig.1 The original image

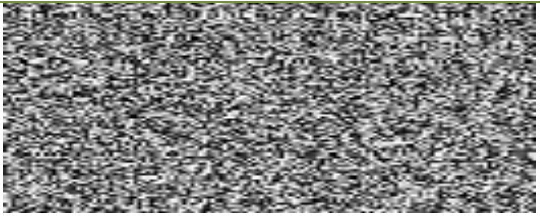

Fig.2 The embedded image

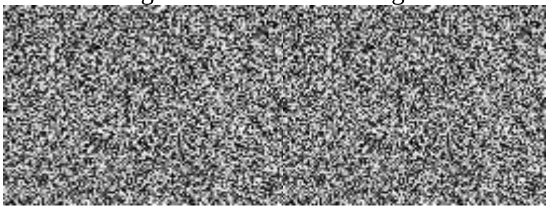

Fig.3 The segmented then encryted image

Fig.4 The encrypted desegmented image

VII. CONCLUSION

In this method A mix approach of encryption, watermarking and segmentation is applied. So in the Previous method less security and more noise is found so we have applied more security and In the receiver side we have applied reversible combined method on encrypted desegmented image 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]. 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.

[5]. W. Puech, J.J. Charre, and M. Dumas. Transfert s´ecuris´e d'images par chiffrement de Vigen`ere. In NimesTic 2001, La relation Homme - Syst`eme : Complexe, Nˆımes, France, pages 167–171, Dec. 2001.

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

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

[8]. AN APPROACH TO REVERSIBLE INFORMATION HIDING FOR IMAGES Santosh Arjun, IEEE Member, NVIDIA, Bangalore, India. Narasimha Rao, IEEE Student Member Electronics and Communication Engineering