International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-3 Issue-3, August 2013

A New Technique for enhance Image Protection Using Digital Watermarking

Vinay Sahu, Kamlesh Lahre

Abstract*—This paper focuses mainly on the image security sharing techniques for safe transmission purpose. This algorithm will be applied to images. We encrypt the secret key with an encryption method based on keys. This work presents a method that combines image watermarking and encryption technique for safe image transmission purpose. In this method we embed the original image with patient information before encryption by using lossless watermarking method then apply encryption algorithm for encryption of embedded image using private key so that both image and patient information is completely encrypted . In this paper, Image Watermarking using Least Significant Bit (LSB) method has been used for embedding the information. In receiver side when the message is arrived then we applied the inverse methods in reverse order to get the lossless original image and patient information comparison to other methods. We have applied and showed the results of our method to medical images.

***Index Terms*— Decryption, encryption, watermarking, image protection.**

I. INTRODUCTION

In recent years of internet world, many people transmit their secret information through the Internet. The transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over the net. The works presented in this paper how encryption and watermarking algorithms give security in medical imagery. In order to do this, the images can be encrypted in their source codes in order to apply. In this paper we propose a new technique to cipher an image for safe transmission. Our research deals with image encryption and watermarking. There are several methods to encrypt binary or grey level images [1], [2], [3], [4]. In this paper we propose a technique for safe transmission image and deals with image cryptography, watermarking .To embed the image in the patient information we have used a lossless watermarking technique. The watermarking objective is to embed invisibly message inside the image. For secure image this technique is very useful for image transmission through the internet. This technique we can use in different many area. 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 that embedding of patient information to encrypted image considered like noise. 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 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. So that security level is also high [4], [6]. In this paper we present special encryption technique of visual cryptography, Least Significant Bit technique and combination method. The amount of digital medical images has increased rapidly in the Internet. The necessity of fast and secure way to transmit them over the net. This approach bases the protection on digital watermarking, aimed at secretly Embedding a message into the image. In order to decrease the processing time, the main objective is to guarantee the protection of medical images during transmission, and also once this digital image is archived. We are therefore faced with a real security problem when sending data .For Ethical reasons, medical imagery cannot be sent when such a Risk is present, and has to be better protected. Encryption is the best form of protection in cases such as this. Many different Techniques for the encryption of image exist. In this tutorial I will present Combination of image encryption.

II. SPECIAL ENCRYPTION TECHNIQUE

Special encryption technique needs only the characteristics of human vision to decode the encoded images. It does not require any kind of complex computation to decode the encoded image. Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The security gained through visual cryptography requires proper distribution of the shares. Mainly this visual cryptography focuses on the security aspects to safeguard the secret image from two or more cover images so that any attacker cannot retrieve any data. Therefore it is necessary to study all the recent technologies that are evolved and written as a literature to understand the concept of visual cryptography in a better way most secret sharing schemes are based on cryptography such that the encryption and decryption processes need high computation costs. Visual secret sharing schemes hide the secret image into several share images and distribute these share images to participants. With no computation, human beings are able to obtain the secret image by stacking the share images [7], [8].

III. LEAST SIGNIFICANT BIT TECHNIQUE

The most common method of watermark embedding is least significant-bits. The benefits of the LSB are its simplicity to embed the bits of the message directly into the LSB plane of cover-image. The simplest of the LSB techniques is LSB replacement.

Manuscript published on 30 August 2013.
***Correspondence Author(s)**
Vinay Sahu , M Tech Scholar , Department of Engineering ,Dr. C. V.R. U., Bilaspur (C.G), India.
Kamlesh Lahre , Assistant Professor , Department of Engineering, Dr. C. V.R. U., Bilaspur (C.G), India.

LSB replacement flips the last bit of each of the data values to reflect the message that needs to be hidden. Suppose the first eight pixels of the original image have the following grayscale values:

11010010	01001010	10010111	10001100
00010101	01010111	00100110	01000011

To hide the letter A whose binary value is 01000001, we would replace the LSBs of these pixels to have the following new grayscale values:

11010010	01001011	10010110	10001100
00010100	01010110	00100110	01000011

In this process watermark is being embedded in the image by using LSB techniques. The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error measurement methods which compare quality of the image. MSE represents the cumulative squared error. Whereas PSNR represents a measure of the peak error [9].To calculate the PSNR, the mean-squared error is first calculated using the following equation:

$$MSE = \frac{\sum X,Y\left[I_1(x,y) - I_2(x,y)\right]^2}{X * Y}$$

Where X and Y are the number of the number of rows and columns in the input images, respectively and I_1(x, y) is the original image, I_2 (x, y) is the Watermarked image. The PSNR is calculated using the following equation:

$$PSNR = 10\log_{10}\left[\frac{M^2}{MSE}\right]$$

Where M represents value in the image, its value is 255 for 8 bit.

IV. DESCRYPTION METHODS

In this section we describe how it is possible to combine the techniques of visual cryptography for security of image. A new problem is trying to combine in a single step, compression and encryption. 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.

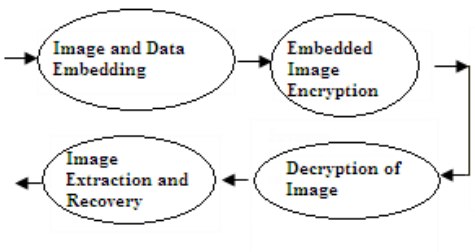

Fig. 1.Sketch of proposed scheme.

In this method we embed the image with patient information by using LSB lossless data embedding technique then encrypt the embedded image with encryption technique 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. Decryption is the process of converting. The proposes scheme is shown in below fig.1.

V. RESULT

We present now the results of the combination of encryption and watermarking methods The Fig.2 (a) is the original image. We embedded the original image with patient information and got fig. 2(b) and applied encryption on fig.2 (b) and got fig. 2(c) and then sent the fig 2(c) to the receiver side.

Fig 2(a)

Fig. 2(b)

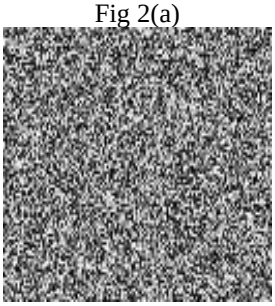

Fig 2(c)

Fig. 2: a) master medical image, b) Embedded image, c) encrypted signature image

VI. CONCLUSION

In this paper we have presented a method that combines approach of cryptography, watermarking is used. In this method the image is embedded using watermarking method with patient information and then embedded image is encrypted. In the Previous methods partial encryption, less security and more noise is found so we applied embedding of image with patient information before encryption so that we found less noisy image and for complete cover of both image and patient information, we applied encryption after embedding and we got more secured and less noisy medical image. Future work includes extending the method based on descending order of pixel grey level values and appending more number of bits for each character, which makes the method as more advance.

ACKNOWLEDGMENTS

My express thanks and gratitude to all the departments' and sponsors who give me an opportunity to present and express my paper on this level.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

REFERENCES

1. C-C Chang, M.S. Hwang, and T-S Chen. "A new encryption algorithm for image cryptosystems". The Journal of Systems and Software, 58:83–91, 2001.
2. W. Puech. "Image Encryption and Compression for Medical Image Security" proceeding of IEEE Image Processing Theory", Tools & Applications, 2008.
3. Ming Yang, Lei Song, Monica Trifas, Dorothy Buenos-Aires, Lei Chen, Jaleesa Elston, "Secure Patient Information and Privacy in Medical Imaging IEEE ".
4. Xinpeng Zhang]ieee signal processing letters, "Reversible Data Hiding in Encrypted Image" vol. 18, no. 4,pp.255,2011
5. M. Naor, and A. Shamir, "Visual Cryptography", Advances in Cryptology – Eurocrypt'94 Proceeding, LNCS vol. 950, pp. 1-12, 1995.
6. 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, 2008.
7. M. Naor, and A. Shamir, "Visual Cryptography", Advances in Cryptology – Eurocrypt, 94 Proceeding LNCS Vol. 950, pp. 1-12, 1995.
8. M. Naor and A. Shamir, "Visual Cryptography II: Improving the Contrast via the Cover Base", Cambridge Workshop on Protocols, 1996.
9. Puneet Kr Sharma and Rajni, "Analysis of image watermarking using least significant bit algorithm" International Journal of Information Sciences and Techniques (IJIST), Vol.2 No.4, July 2012.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)