Study of Medical Image protection and authentication by Steganocryptographic Techniques

A.AKSHAYA
SSN College of Engineering
Chennai, India
[1]lafemmeakshi6@gmail.com

C.VINOTHKUMAR
SSN College of Engineering
Chennai, India
[2]vinothkumarc@ssn.edu.in

Abstract – Privacy and safety of medical image security is an important issue during its storage and transmission. To address this issue there are two widely used techniques namely Steganography and Cryptography. Steganography is used to embed hidden content in unremarkable cover media so as to make it undetectable by an unintended user. On the other hand, cryptography is used to scramble a message data so that it cannot be understood. This paper presents a study of various methods for integrating together cryptography and steganography through image processing for medical image security. In this, the patient information is encrypted with cryptographic algorithm and then it is embedded in the cover image by using data embedding algorithms. In receiver side when the message is arrived the inverse methods in reverse order are applied to extract the patient information.

Keywords: Medical image, Cryptography, Steganography, Steganocryptography.

I. INTRODUCTION

Cryptography is the science of converting a data (plaintext) into a secret code called cipher text so as to address various aspects of information security such as confidentiality, authentication and data integrity. Symmetric (or) Secret key cryptography and Asymmetric (or) Public key cryptography are the basic cryptographic schemes used that employ complex computational algorithms for encryption and decryption. Rivest Cipher5 (RC5), Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are some such algorithms have been used in the past. Most of encryption methods are used to encrypt the textual information such as patient details as well as the images for the sake of privacy.

Steganography is a technique by which the very existence of a message is hidden so that an unintended user is unaware of its presence. Information can be hidden in carriers such as images, audio files, text files and videos. When the message is hidden in the carrier a stego-carrier is formed for example a stego-image which will be perceived to be as close as possible to the original carrier or cover image. The most commonly used Steganographic technique is the Least Significant Bit (LSB) Insertion.

One of the simplest methods used for inserting data into digital signals in noise free environments is the Least Significant Bit Insertion. In this method, the message bits are encoded in the least significant bit of every byte in an image. This does not introduce any significant changes in the image since the value of each pixel is changed only slightly. Hence the altered image would look identical to the original image.

In a typical Steganocryptographic system the plaintext is encrypted by symmetric or asymmetric key encryption algorithms into a cipher text. Then this cipher text is embedded onto the cover image by LSB Steganography technique. The output i.e. the stego image is then transmitted to the recipient. The recipient extracts the message from the carrier image in the reverse process. The message can only be extracted if there is a shared secret key between the sender and the recipient. This makes the system highly secured.

Digital image Steganography can be broadly divided into two categories namely spatial domain techniques and frequency domain techniques. While spatial domain techniques can be easily modelled and mathematically analysed, the frequency domain technique proves to be more robust, stable and invisible.

The rest of this paper is organized as follows. Section 2 describes the spatial domain Steganocryptographic techniques while section 3 describes the frequency domain technique. Experimental results with further discussions are included in section 4. Finally in section 5 conclusions are made.

II. SPATIAL DOMAIN STEGANOCRYPTOGRAPHIC TECHNIQUES

A. LSB-XOR Technique

An improvement on basic LSB substitution would be to use a pseudo-random number generator to act as a secret key with which the message is XORed. Security would be improved, as intermediate parties cannot decipher the message without the knowledge of the key used.

Algorithm Steps for LSB-XOR Encryption:

Step 1: Convert the message data from decimal to binary.
Step 2: Read the cover image and convert it from decimal to binary.
Step 3: Generate a binary key of the same length as the binary message using a pseudo random generator.
Step 4: Break the message byte into bits.
Step 5: Perform bitwise XOR between the key and binary message string to obtain a new key.
Step 6: Take first 8 byte from the cover image and replace the LSB by one bit of the new key.
Step 7: Repeat and replace for all bytes of cover image.

Algorithm Steps for LSB-XOR Decryption:

Step 1: Convert the stego image from decimal to binary.
Step 2: From each byte extract the LSB.
Step 3: Perform XOR between the extracted bit sequence and the key to get the message string in binary.
Step 4: Convert the binary message string to decimal and then to ASCII code to get the hidden message.

B. Catmap Transform Based LSB-XOR Technique

The Arnold Cat Map is used to change the positions of the pixel values of the original image. The result after applying the Arnold Cat Map will be a shuffled image that contains all of the same pixel values of the original image. When the transformation is repeated enough times, the original image will reappear. Mathematically, the Arnold Cat Map, 'A' is represented as the following:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \mathrm{A} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

Choose p=1, q=1,

$$\mathrm{A} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

The level of security can be increased by applying Catmap transform 'n' times to scramble the pixels of the cover image before performing the LSB-XOR Encryption to hide a message onto the cover image. After data hiding, inverse Catmap transform is applied 'n' times so as to descramble the pixels to their original location. The resulting image is the stego image and it appears exactly like the cover image. In order to decrypt the hidden message, the receiver should know the value of 'n' and also the pseudorandom key generated by the sender during LSB-XOR Encryption for data hiding.

Algorithm Steps for Catmap Transform based LSB-XOR Encryption:

Step 1: Read the cover image.
Step 2: Apply Catmap transform to the cover image 'n' times
Step 3: Convert the Catmap transformed image from decimal to binary.
Step 4: Perform XOR based LSB encryption to hide a message onto the binary Catmap transformed image.
Step 5: Apply inverse Catmap transform to obtain the stego image to be transmitted.

Algorithm Steps for Catmap Transform based LSB-XOR Decryption:

Step 1: Read the stego image and apply Catmap Transform 'n' times.
Step 2: Convert the transformed image from decimal to binary.
Step 3: From each byte extract the LSB.
Step 4: Perform XOR between the extracted bit sequence and the key used during LSB-XOR encryption to get the message string in binary.
Step 5: Convert the binary message string to decimal and then to ASCII code to get the hidden message.

C. AES Algorithm Based LSB-XOR Technique

Advanced Encryption Standard algorithm developed by Rijndael, is a symmetric key encryption algorithm. The algorithm consists of 128-bit block size, with key sizes of 128, 192 and 256 bits. AES operates on a 4×4 array of bytes, termed as state. Large number of transformations is defined on a state, and it uses a special key. The key is developed from the Encryption algorithm. The number of rounds depends on the block and key size. All the transformations used are invertible, which makes decryption possible [10].

In this method, AES algorithm is first applied to the cover image and then the message is hidden in the cover image by LSB-XOR encryption technique. Inverse AES algorithm is applied to get the stego image that is undistinguishable from the cover image

Algorithm Steps for AES based LSB-XOR Encryption:

Step 1: Read the cover image and convert it from decimal to binary.
Step 2: Read the message and divide it into 1x16 sized blocks.
Step 3: Perform AES encryption for the blocks and combine all the blocks.
Step 4: Perform LSB-XOR encryption to hide the AES encrypted message onto the cover image to get the stego image.

Algorithm Steps for AES based LSB-XOR Decryption:

Step 1: Read the stego image and divide it into 1x16 sized blocks.
Step 2: From each byte extract the LSB
Step 3: Perform XOR between the extracted bit sequence and the key used during LSB-XOR encryption to get the encrypted message string in binary.
Step 4: Convert the AES encrypted message from binary to decimal.
Step 5: Perform inverse AES and convert to ASCII to get the actual hidden message.

III. FREQUENCY DOMAIN STEGANOCRYPTOGRAPHIC TECHNIQUES

A. DWT Based Steganocryptographic System

A one dimensional discrete wavelet transform is a repeated filter bank algorithm. The input is convolved with a high pass filter and a low pass filter. The result of the latter convolution is a smoothed version of the input, while the high frequency part is captured by the first convolution. The reconstruction involves a convolution with the syntheses filters and the results of these convolutions are added [11]. The forward 2-D discrete wavelet transform can be implemented using a set of up-samplers, down-samplers, and recursive two-channel digital filter banks.

In this frequency domain technique the message to be hidden is first encrypted to get the cipher text. Any one of the above discussed encryption technique can be used for this. Then DWT is applied to the cover image to decompose it to many subbands. The cipher text is hidden in the high frequency DWT coefficients by LSB-XOR technique. Finally the stego image is obtained by applying the IDWT. At the receiver side,

DWT is applied to the stego image to extract the encrypted bit stream from the high frequency coefficients. This bit stream is suitably decrypted to obtain the original plain text.

Algorithm for DWT based Steganocryptographic encryption:

Step 1: Read the cover image and apply DWT to it.
Step 2: Encrypt the message using AES.
Step 3: Hide the encoded bitstream at the high frequency coefficients of the wavelet transformed cover image.
Step 4: Apply IDWT to obtain the stego image.

Algorithm for DWT based Steganocryptographic decryption:

Step 1: Apply DWT to the stego image.
Step 2: Extract the hidden data bits from the high frequency coefficients.
Step 3: Apply inverse AES to the bitstream to obtain the actual hidden data.

IV. EXPERIMENTAL RESULTS

The above techniques are applied to various test medical images to hide a secret message. The PSNR between cover image and stego image as well as the Correlation Coefficient between hidden message and extracted message have been calculated for each of the techniques using the formulas given below:

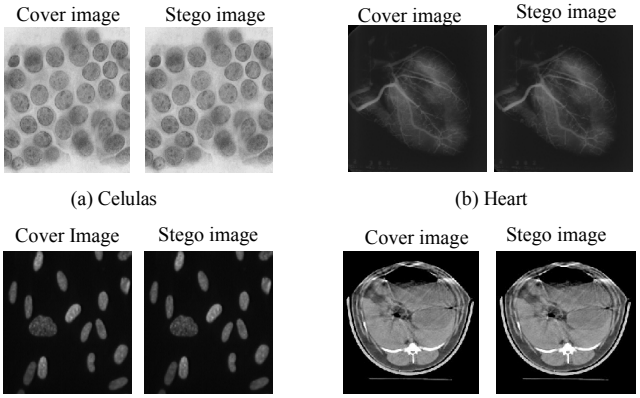
$$\mathrm{MSE} = \frac{1}{\mathrm{N}}\sum_{\mathrm{i}=1}^{\mathrm{N}}\left(\widehat{\mathrm{Y}}_{\mathrm{I}} - \mathrm{Y}_{\mathrm{I}}\right)^2 \quad (1)$$

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{MAX}_{\mathrm{I}}^2}{\mathrm{MSE}}\right) \quad (2)$$

$$\rho(\mathrm{x},\mathrm{y}) = \frac{\sum_{\mathrm{i}=1}^{\mathrm{n}}(\mathrm{x}-\bar{\mathrm{x}})(\mathrm{y}-\bar{\mathrm{y}})}{\sqrt{\sum_{\mathrm{i}=1}^{\mathrm{n}}(\mathrm{x}-\bar{\mathrm{x}})^2\sum_{\mathrm{i}=1}^{\mathrm{n}}(\mathrm{y}-\bar{\mathrm{y}})^2}} \quad (3)$$

N - Size of the image
$\widehat{Y_I}$ - Stego image
Y_I - Cover image
MAX_I - Maximum pixel value of the image
ρ(x,y) - Correlation Coefficient
x - Hidden message
y - Extracted message
$\bar{x}$,$\bar{y}$ - mean of x and y respectively

The effect of noise on these systems is also modeled and the correlation between the extracted data in noisy and noiseless transmission is calculated.



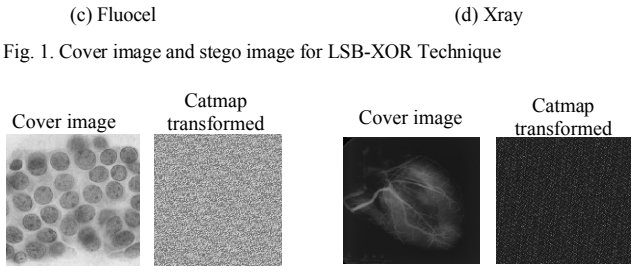


Fig. 1. Cover image and stego image for LSB-XOR Technique

Fig. 2. Cover image, Catmap transformed image and Stego image for Catmap Transform based LSB-XOR technique

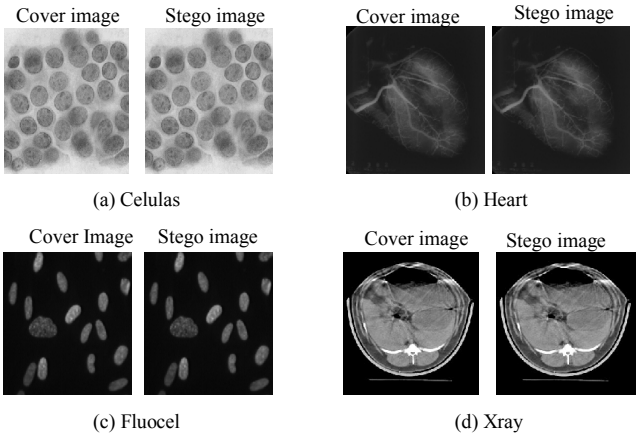
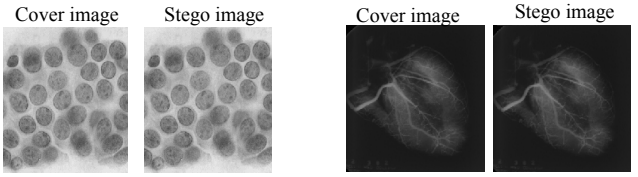
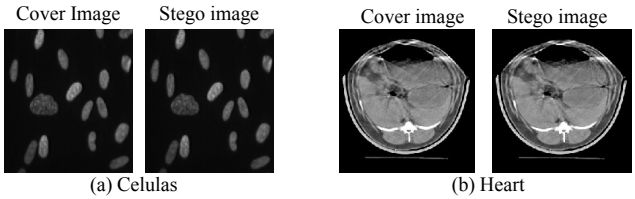


Fig. 3. Cover image and stego image for AES algorithm based LSB-XOR Technique





(a) Celulas (b) Heart (c)Fluocel (d) Xray

Fig.4. Cover image and stego image for DWT based Steganocryptographic system

TABLE I. CORRELATION COEFFICIENT AND PSNR FOR ALL THE TECHNIQUES

Images	LSB-XOR		Catmap Transform based LSB-XOR		AES based LSB-XOR		DWT based Technique	
	ρ	PSNR	ρ	PSNR	ρ	PSNR	ρ	PSNR
Celulas	0.5237	78.0349	0.8550	18.9164	0.3046	73.2853	0.1395	79.4832
Heart	0.7459	77.3193	0.3590	22.3367	0.0537	73.3290	0.2933	82.4935
Fluocel	0.9961	77.9705	0.9312	19.8159	0.0968	73.9911	0.1423	81.2441
Xray	0.9765	90.2750	0.5706	11.4729	0.0970	73.4626	0.2211	82.4935

From Table I, The level of security and amount of error introduced are analysed for each. The security level in Catmap transform based LSB-XOR encryption has improved compared to the LSB-XOR encryption since the locations of the hidden message is random in the former and hence the computations involved for a third party to crack the hidden message would be more. Higher level of security is attained at the cost of a large increase in MSE. The AES based LSB-XOR encryption has a better security level compared to both the LSB-XOR encryption and Catmap transform based LSB-XOR encryption. This is because a third party cannot crack the hidden message unless the private key used for AES is known. At the same time AES based LSB-XOR encryption yields better MSE and PSNR values than the Catmap transform based LSB-XOR encryption. The MSE values are comparable to those obtained for LSB-XOR encryption. Hence, this technique which combines both cryptography and Steganography for data hiding in medical images proves to be better than the other two techniques.

However, the experimental results show that the spatial domain techniques fail in the presence of waveform attacks such as noise. The frequency domain technique proves to be robust in a noisy transmission environment.

V. CONCLUSION

This paper presents a study of various Steganocryptographic techniques for medical image protection and authentication. The result shows that the frequency domain technique is more robust against waveform attacks such as noise when compared to the spatial domain technique. Amongst the spatial domain techniques, the AES based LSB-XOR method proves to have a higher security level without compromising on the MSE. Hence, by using AES to encrypt the message and hiding the encrypted message onto the cover image in frequency domain we attain a system that is both highly secure as well as robust.

REFERENCES

[1] Vinay pandey, Angad Singh, Manish Shrivastava, "Medical Image Protection by Using Cryptography Data-Hiding and Steganography", International Journal of Emerging Technology and Advanced Engineering, 2012 Volume 2, No. 1, pp. 106-109.

[2] Chi-Kwong Chan, L.M. Cheng, "Hiding data in images using LSB substitution", Pattern Recognition – The Journal of the Pattern Recognition Society, 2004, pp. 469-474.

[3] Johnson, N. F. and Jajodia, S, "Exploring steganography: Seeing the unseen", IEEE Computer Magazine, 1998, pp.26-34.

[4] Shuhong Jiao, Robert Goutte, "A Secure Transfer of Identification Information in Medical Images by Steganocryptography", Int. J. Communications, Network and System Sciences, 2010, pp. 801-804.

[5] Yicong Zhou and Sos Agaian, "A Lossless Encryption Method for Medical Images Using Edge Maps", 31st Annual International Conference of the IEEE EMBS, 2009, pp. 3707-3710.

[6] Bourbakis. N, Rwabutaza. A, Yang. M, Skodras. A. N, Ewing. R, "'A synthetic stegano-crypto scheme for securing multimedia medical records and their associations", 16th International Conference on Digital Signal Processing, 2009, pp. 1-8.

[7] Mei Jiansheng1, Li Sukang1 and Tan Xiaomei, "A Digital Watermarking Algorithm Based On DCT and DWT", International Symposium on Web Information Systems and Applications, 2009, pp. 104-107.

[8] Adnan Mohsin Abdulazeez Brifcani and Wafaa Mustafa Abduallah Brifcani, "Stego-Based-Crypto Technique for High Security Applications", December, 2010, International Journal of Computer Theory and Engineering, Vol.2, No.6, pp. 835-841.

[9] M.U. Celik, G. Sharma, A.M. Tekalp and E. Saber, "Lossless generalized-LSB data embedding", *IEEE Transactions on Image Processing*, vol. 14, no.2, pp. 253-266, 2005.

[10] M. Zeghid , M. Machhout , L. Khriji , A. Baganne , R. Tourki, "A modified AES based algorithm for image encryption" World Academy of Science, Engineering and Technololgy, 2005, vol. 7, pp 80-85.

[11] M. Fahmy Tolba, M. AI-Said Ghonemy, Ismail Abdoul-Hameed Taha, Amal Said Khalifa, " High Capacity Image Steganography using Wavelet-Based Fusion",IEEE, 2004, pp.430-435.