International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Ballot Agency Performance under Data Secure Techniques

Junie Jose[1], Laxmi Gulappagol[2], Dr. Kb Shivakumar [3]

[1]VTU Belgaum, M.tech in Digital Electronics and Communication, Mangalore Institute of Technology and Engineering, Moodabidri. Mangalore, Karnataka, India

[2]Assistant Professor. Department of ECE, Mangalore Institute of Technology and Engineering, Moodabidri. Mangalore, Karnataka, India

[3] Professor and Head of Department of Training and Placement, Karnataka

Abstract: ***Many requests to one network will take large time to get a replay. To reduce this issue, user demand protocol using a ballot agency is proposed. The secure techniques provided by the agency are cryptography, watermarking, and steganography with DCT and LSB methods. These are used for embedding and extraction of the message. User's request to any of the three techniques, the agency will give the corresponding technique with options DCT and LSB. The quality analysis is done after each embedding process using the PSNR value calculation. The result shows promising support to large scale networks.***

Keywords: Ballot agency, Cryptography, Steganography, Watermarking, PSNR value

1. Introduction

Security issues in the transfer of data like images, text, video and audio are now in common. For controlling the issue three secure techniques such as steganography, watermarking, and cryptography are being used. Steganography and watermarking gives a variety of very important methods that to hide important information in an undetectable and/or irremovable way in audio, video and image data.

Steganography is related to securing information in digital media. Here the information will be send with security but others cannot identify the exact information and this is the main difference from the cryptographic technique. Different ways for encryption and decryption are present for keeping the message secret. The problem related to this is the existence of data [1]. The technique used to overcome this issue is steganography. Steganography is the art and science of noting secret data with no one apart from the targeted recipient identifies the existence of the message. Spatial domain and frequency domain are taken into consideration for the steganographic method [4].

Watermarking is another data protecting technique. It is also possible to do using spatial and frequency domain. Watermarking while doing the watermarking in spatial domain, it is more fragile than frequency domain [2].

The important aim of steganography is to hide a message p in some audio, video (cover) or image data q, to obtain new data q', practically indistinguishable from q, by users, in such a way that an attacker cannot detect the presence of p in q'[5],[6].

The necessity of watermarking is to hide a data p in some audio, video (cover) or image data q, to obtain new data q', practically indistinguishable from q, by users, in such a way that an eavesdropper cannot remove or replace p in q'. It is said that the aim of steganography is to hide a data in one dimensional communications and that of watermarking is to hide message in one to many communications.

Cryptography is the third technique, that can secure the text message through the conversion of cipher text. This is in the case of private key cryptography. Cryptography is not a complete hiding technique. First it will convert to other format (cipher text) and then it can send with a private key to another user.

Hiding the very existence of the message in the communicating data is possible through Steganography and watermarking.

2. Methodology

Fig.1 shows the Ballot agency performance .This is done on behalf of the user. On the user demand, corresponding agets will be send by the agency and then the corresponding agent will do the corresponding task.

Figure 1: Ballot agency performance

Steganography and cryptography are the two used method for secured text transmission. Watermarking is specially used for Secured image communication between two users.

In steganographic technique the private key approach is used and for cryptography private key plus cipher text conversion

method is used. Watermarking technique is having a watermark and a cover image and after the embedding process the image will be ready to send to other user. If the receiver is having the extraction algorithm of the same then that person can extract the watermark (watermarked image).

3. Classification of Data Secure Technique

In steganography, watermarking, and cryptography the different secure methods used are LSB (Least Significant Bit) and DCT (Discrete Cosine Transform). The used methodology for the analysis of data hiding techniques is as shown in fig.2 .That is classification of data hiding techniques.

In DCT method the watermark will be inserted to spectral component of image using techniques analogous to spread spectrum communication. Normally in mid frequencies or in lower frequencies, the DCT is performed. For a hacker, it is difficult to detect the watermark, they consist of weak signals. The robustness is more in this method.

The general equation used for the DCT and IDCT technique is given in equation (1) and (2).

$$B_{pq} = a_p a_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos\left[\frac{\pi(2m+1)p}{2M}\right] \cos\left[\frac{\pi(2n+1)q}{2N}\right], \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix} \quad (1)$$

$$\alpha p = \begin{cases} 1/\sqrt{M} \text{ for } p=0 \\ \sqrt{2}/M \text{ for } 1 \le p \le M-1 \end{cases} \quad \alpha q = \begin{cases} 1/\sqrt{N} \text{ for } p=0 \\ \sqrt{2}/N \text{ for } 1 \le p \le N-1 \end{cases}$$

M and N are the row and column size of A, B_{pq} is the DCT coefficient of A and A_{mn} is the matrix notation.

$$A_{mn} = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} \alpha_p \alpha_q B_{pq} \cos\left[\frac{\pi(2m+1)p}{2M}\right] \cos\left[\frac{\pi(2n+1)q}{2N}\right], \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix} \quad (2)$$

$$\alpha p = \begin{cases} 1/\sqrt{M} \text{ for } p=0 \\ \sqrt{2}/M \text{ for } 1 \le p \le M-1 \end{cases} \quad \alpha q = \begin{cases} 1/\sqrt{N} \text{ for } p=0 \\ \sqrt{2}/N \text{ for } 1 \le p \le N-1 \end{cases}$$

$$\text{PSNR} = 10 \log 10 \left(R^2 / \text{MSE}\right) \quad (3)$$

$$\text{MSE} = \frac{\sum_{M,N} * [I_1(m,n) - I_2(m,n)]^2}{M * N} \quad (4)$$

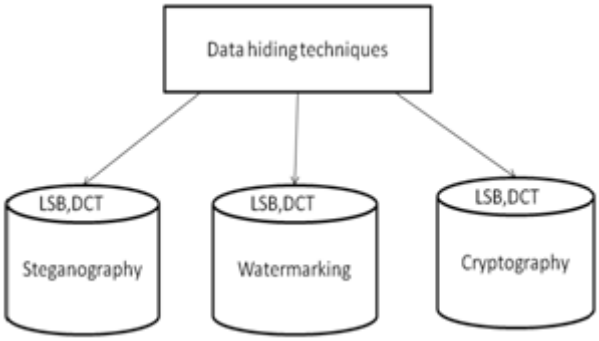

Figure 2: Classification of data hiding techniques

2.1. LSB-Steganography

In this technique the messages will be embedded in the intensity of the pixels directly. LSB technique is the most widely used spatial domain steganographic technique. The main issue of using this method is that if the message is compressed then the embedded data may lose. For the better quality performance LSB technique is improved by using a pseudo random number generator.

2.2. DCT- Steganography

The primary step of this technique is the transformation of image and then the message is embedded in the image. It provides better protection against statistical attacks. Here the image will be divided into 8*8 blocks and DCT transformation on each block is performed.

Here the image of size M*N is divided into 8*8 blocks and two dimensional DCT is performed on each block.

2.3. LSB-Watermarking

The way of using least significant bit is by inversing the binary values of the watermark text and shifting that according to the odd or even number of pixel coordinates. This will be done before embedding the image. The flexibility of the algorithm depends on the length of the watermark text. The different attacks on the image is also applied in LSB technique and the quality of the image is checked by using PSNR values.

2.4 DCT Watermarking

The DCT or Transform domain is another way for watermarking. In this technique the characteristics of Human Vision System (HVS) are better captured by spectral coefficients. For this method, inserts watermark into the spectral components of image using ways analogous to spread-spectrum communication [3].

2.5. DCT Cryptography

Here the message will be converted to cipher text and using a cover image embeds the message plus private key using DCT method. After the embedding process the PSNR value will be calculated. At the end user or at the receiver the extraction process will take place. This is done by using the private key. Then the end user will get the extracted message.

2.6. LSB cryptography

First we have to load the cover image as well as the watermark (text). After the completion of cipher text conversion, cover image and the message plus private key will be embedded using LSB method. Then the PSNR value will be evaluated. The extraction of message will take place at the receiver. For this the private key should be known by the receiver.

4. Experimental Result

Table 1 gives the PSNR values of steganography , watermarking, and cryptographic techniques using DCT and LSB method with different formats of images like .bmp, .tif, .jpg

Table 1: The analysis of different methods of three data secure techniques using PSNR value

Image	Watermarking		Steganography		Cryptography	
	DCT	LSB	DCT	LSB	DCT	LSB
E1.bmp	41.416	50.877	41.1652	75.2081	41.1652	75.1813
Patr1.bmp	40.155	49.4122	40.1537	73.3292	40.15392	73.370
Barbara.tif	40.7344	50.4748	40.7344	74.442	40.7344	74.5256
Mandrill.tif	40.085	49.6645	40.085	73.6588	40.085	73.6756
p.jpg	41.9817	51.2532	41.9811	72.5573	41.9811	72.4128
V17.jpg	41.4147	51.095	41.4146	75.7841	41.4146	75.5401

Fig.3 shows the graphical representation of PSNR values of three techniques using DCT method.

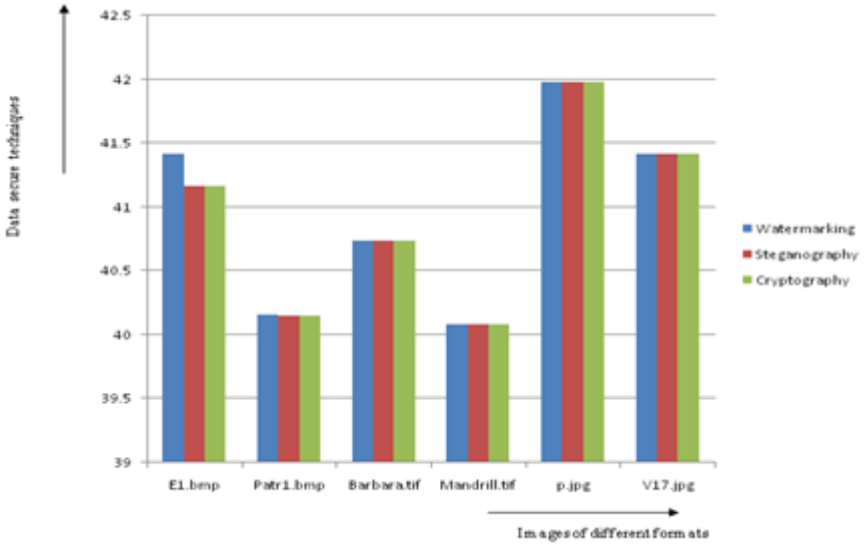

Figure 3: Graphical representation of PSNR values of three techniques using DCT method

Fig.4 shows the graphical representation of PSNR values of three techniques using LSB method.

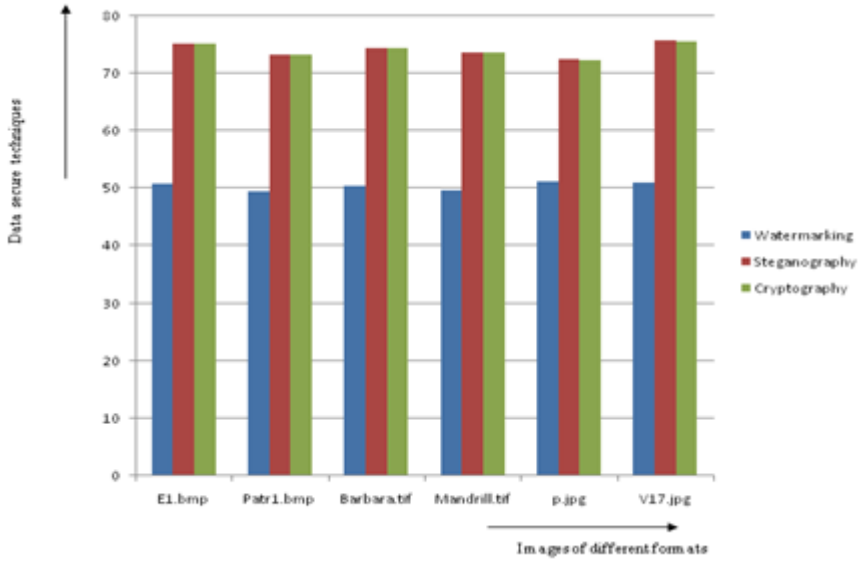

Figure 4: Graphical representation of PSNR values of three techniques using LSB method

Fig.5 shows the overall performance of three techniques using DCT and LSB method

5. Conclusion

Ballot agency performance on user demand for different data secure techniques is performed. From a single platform user can decide which secure method is wanted to do for sending message in . If the receiver has the extraction algorithm of

the demanded method, then it is easy to recover the data or message. For the analysis of steganography, watermarking, and cryptography, the PSNR value found after each embedding process. From the PSNR value calculation, found that, by using DCT method of each data secure techniques having approximately the same PSNR value and by using LSB method, both steganography and cryptographic technique having good performance than watermarking technique

References

[1] Ichiro Satoh, "Mobile Agents" National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan, ichiro@nii.ac.jp .
[2] George Samaras, Marios D. Dikaiakos, Constantinos Spyrou, Andreas Liverdos,"Mobile Agent Platforms for Web Databases: A Qualitative and Quantitative Assessment", Department of Computer Science University of Cyprus.
[3] Luís Moura Silva, Guilherme Soares, Paulo Martins, Victor Batista, Luís Santos, "The Performance of Mobile Agent Platforms", Portugal,(2000).
[4] E. C. Vijil, Security Issues in Mobile Agents, Kanwal Rekhi School of Information Technology Indian Institute of Technology, Bombay.
[5] Rajdeep Bhanot and Rahul Hans, "A Secure and Fault Tolerant Platform for Mobile Agent Systems", International Journal of security and its Application Vol. 9, No. 5 (2015).
[6] Sandhya Armoogum, Asvin Caully, "Obfuscation Techniques for Mobile Agent code confidentiality", Journal of Information & Systems Management Volume 1 Number 1, March (2011).
[7] Tomas Sander and Christian F. Tschudin, "Protecting Mobile Agents Against Malicious Hosts", International Computer Science Institute, Feb 1998, to appear in G. Vigna (ed.), Mobile Agent Security.
[8] Asha Anil, Jesna Anver, "An enhanced approach for securing mobile agents from the attack of other malicious mobile agents", International Journal of Research in Engineering and Technology (2014).
[9] Lotfi Benachenhou, Samuel Pierre,"Protection of mobile agent with a reference clone", Mobile Computing And Network Research Laboratory (LARIM)-(2005).
[10] Giovanni Vigna , "Cryptographic Traces for Mobile Agents", Dip. Elettronica e Informazione, Politecnico di Milano, Italy.
[11] Jian Zhao and Chenghui Luo, "Digital Watermark Mobile Agents", Fraunhofer Center for Research in Computer Graphics.
[12] Laxmi Gulappagol, Swetha S and Ravi M Yadahalli, "Digital Watermarking and Mobile Agent Technologies in Data Hiding Applications" , In May 2013.
[13] Deepak Singla, Rupali Syal, " Data Security Using LSB & DCT Steganography In Images", In 2012.
[14] Shahin Shaikh, Manjusha Deshmukh, "Digital Image Watermarking In DCT Domain", In April 2013.
[15] Abdullah Bamatraf, Rosziati Ibrahim and Mohd. Najib Mohd. Salleh , "A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit", In April 2011.

Author Profile

Junie Jose pursuing M-tech in Digital Electronics and Communication, in Mangalore institute of technology and engineering Moodabidri, in the year of 2014-2016.