International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 06, June-2015

Steganography and Cryptography Approaches Combined using Medical Digital Images

Manish Trehan
M.Tech & Department of Computer Science
Lovely Professional University, Phagwara, India

Sumit Mittu
Assistant Professor & Department of Computer Science
Lovely Professional University, Phagwara, India

***Abstract* -The growth in medical field has led to the transformation of the data from papers into the digital form. As the medical field is moving towards the digital world, security of the medical information/data has become a major concern. The patient information, patient disease diagnosis, etc. are all being stored in the digital images. To make the treatment fast and accurate the digital images are being introduced. This research is about how the data is embedded in the medical scanned images through the combined approach using both cryptography and steganography. The patient information and diagnosis by doctor both serve as the confidential information and hence is treated as secret data. The proposed algorithm attempts to keep this secret data secure and at the same time, make the patient's treatment accurate and fast.**

Keywords: Steganography, Cryptography, LSB Embedding Technique, LSB, MSB

1. INTRODUCTION

Steganography is the science and art of data hidden within data. In Steganography the data is hidden in the image in such a way that only the designated recipient knows about the presence of the hidden message. The process is accomplished by hiding one data in another to conceal whether there is any communication. The steganography used various mediums to hide the data, the simplest is the text but the frequently used is the steganography on image. The steganography is broadly divided into three types they are text, image, and audio/video. The information is hidden purely in images in image steganography. Watermarking and fingerprinting are the two other technologies closely related to the steganography. Steganography is somewhat different from cryptography. Steganography is considered as the dark or first cousin of the cryptography. The cryptography provides privacy to the data on the other hand steganography is used to hide the data and provide secrecy. Cryptography is basically used for the security process. The cryptography is a process which is used to provide the secure communication between two mediums in a form that is not understood by normal human being. This is also used to hide data and to communicate over the internet which is not trusted and the data needs to be saved from various third parties. In cryptography we encrypt the data but in case of steganography we hide the data. Steganography is also considered as true secrecy in the field of security. So, steganography is considered more secure than cryptography. Steganography was widely used in ancient times. For example, the hidden message may be written with invisible ink between the visible lines of the private data or letter. Steganography in modern times uses digital media whether it is in image or audio/video file. Digital media is used to hide messages or data on the internet or in the private communication. Today internet has become mandatory in normal life, but it also has concern for security. So, this security concern has being tackled using steganography. To evaluate the performance of two steganography algorithms (Spatial domain algorithm and Transform domain algorithm) various evaluation parameters are identified based on the quality of these two algorithms and listed below. [1]

- Security: A steganography algorithm is said to be secure if any test performed on it results in no difference between the stego image and the original image.
- Capacity: The capacity of an algorithm can be described as the amount of the data that can be effectively hidden in the present or the selected cover medium by the Steganography algorithm.
- Domain of Embedding: The domain of embedding plays a vital role to determine the overall performance of the Steganography algorithm. Example: In case of spatial domain algorithm, it often offers high capacity of data embedding but it falls down to statistical steganalysis.
- Image supported: There are large number of image formats available. This parameter shows which type of image format is suitable for which Steganography algorithm.
- Time complexity: Time complexity plays a vital role in the Steganography. The time complexity of an algorithm is used for judging the performance of an algorithm for hiding or embedding data into large images and also the implementation of the algorithm in the smaller devices such as mobile device etc.
- Imperceptibility: This parameter basically deals with the image quality. In this image quality should not be compromised by the hidden or embedded data present.
- Independent of file format: There are number of file formats and the most powerful and efficient algorithm is the one that has capability to embed the data in different types of file format.

2. LSB EMBEDDING TECHNIQUE

LSB embedding is a simple technique to implement the steganography. Like other techniques, this technique also embeds the data into the cover image so that it cannot be detected by the normal human vision. In LSB technique, the

data embedding is possible on any bit of the image, but it is performed on preferably least significant bits. The bits of every pixel of the image are used and this method is important for using a looseless compression to protect the hidden information. The LSB technique generally uses three bits from every pixel (represented with 24 bits) where bits of the secret data are stored to hide secret data in the image. For example, the basic data embedding through LSB technique is presented below:

Secret data bits01100101 are embedded into an 8-bit depth image and 8pixels are selected from top left corner of the image.

Original bitmap*:*
01100101 10101011 11101110 00100011
00111000 01101111 11101110 11100111

Bitmap after embedding secret data*:*
10100100 01101011 10001011 01100010
11111000 11101111 11001110 11100111

In this technique the last bit of the first pixel, third pixel and fourth pixel is changed in order to make the last bit's value equal to the corresponding bit of the secret data 01100101 to be embedded in the image. By this approach the data is embedded into the image which results in loss of some data but it is indistinguishable to the human vision as its variation in the color is relatively very small.

3. LITERATURE REVIEW

Several contributions have been made in the field of information security. In recent year both steganography and cryptography achieve a diversified level of security. Different steganography techniques like patchwork, spread spectrum,[1] has been implemented on various image file type like BMP,GIF,JPEG etc formats with different combination of other techniques like LSB with BMP, LSB with GIF,JPEG compression[1]. So many work is done with technique named as least significant bit(LSB) with concern of various issues such as quality, security and data capacity[2]. As defined above, steganography is all about hiding data in an image so the security feature cannot be ignored. The work done named as dual image steganography, in which steganography used within steganography focused on enhancing security and payload capacity. Other technique which enhances the basic LSB named as Smart LSB Pattern Substitution algorithm [10]. The basic concept of cryptography and steganography is explained. It proposes 3 different types of patterns to embed secret data bits into the image bytes. Also, the hiding capacity can be increased by up to 4 times by configuring the hiding capacity level. Based on this work analysis we proposed a new algorithm which covers up the various limitations and give new ways to handle medical scanned images with a hybrid solution using steganography and cryptography.

4. PROPOSED WORK

A new hybrid algorithm is being proposed which is an enhancement to the medical field. In these both, techniques cryptography and steganography are used to increase the security of the data of the patient which is stored in the digital image of the patient X-ray.

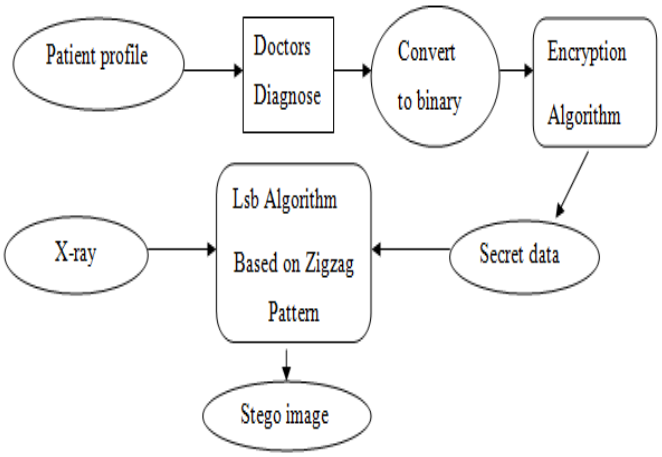

Fig.1. Model of proposed work

Embedding Algorithm

- Read the text message into the string form.
- Encrypt the text message using the AES encryption technique.
- Convert the encrypted text into the binary form.
- Read the cover image into the 1D array i.e. binary form.
- Select the last bit of the image and place the last bits in an array.
- Convert 1d array to 2d array in 3*3 forms.
- Logical grids of 3*3 are made having the last bit replaced with the MSB of the encrypted text.
- Now again from new grid make an array and replace these bits with the image last bits row vice.
- Data is embedded resulting into the creation of the stego image.

Extracting Algorithm

- Read the stego image into 1D array form.
- Convert the decimal values into binary form.
- Select the last bit of the stego image converted decimal and make an array of these bits.
- A grid of 3*3 is made and result is stored in 2D array.
- Convert this 2D array into 1D array.
- Convert these binary values into a string.
- Decrypt this string using AES decryption algorithm, which results in the original text.
- The cover image and the original text regain.

5. RESEARCH METHODOLOGY

The approach is divided into two modules: embedding data and extraction of data from the patient scanned x-ray. The first module contains two main techniques: cryptography and steganography. In this the patient instead of any paper report is provided with the x-ray scanned containing the patient history and diagnosis. The second module contains the stego extraction, decryption algorithm and one added technique by which the doctors diagnose and patient history both is stored in the database for future reference. The flow of the research is:

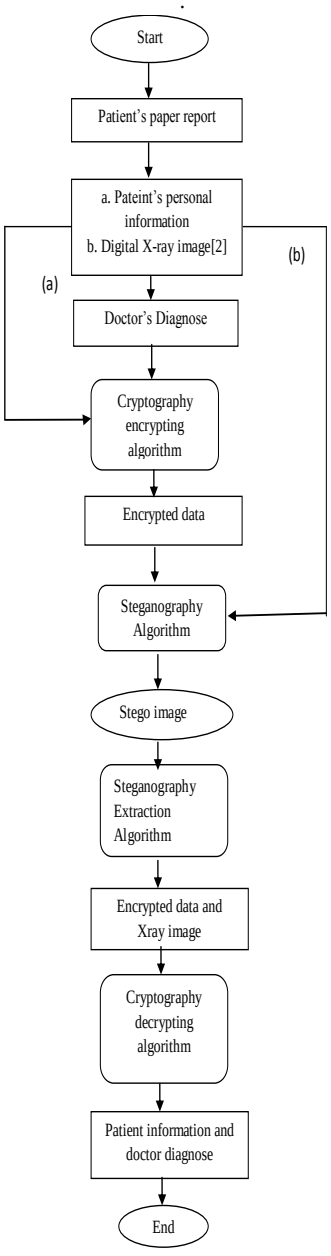

Fig.2. Research flow.

6. CONCLUSION

The proposed approach is a dedication to the medical field. The research is on making patient information more secure and disease diagnosis more accurate. The research concerns with using the two important security mechanisms- cryptography and steganography, on single platform. To make the patient's information more secure with the hospital, the approach explained in the research is about making doctors treatment more secure by providing the diagnose of the previous doctors. As the hospitals are getting digitized, all the data of the hospital are stored in the digital images like CT-SCAN and X-rays. This approach can be an asset to the medical field and can increase the security of the patient data.

ACKNOWLEDGMENT

The paper is written under guidance and support of my department who encouraged me in completion of the work. I would like to thank everyone who helped and motivated me by which the work is made possible.

REFERENCES

[1] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005.

[2] M. Pavani , S. Naganjaneyulu , C. Nagaraju," A Survey on LSB Based Steganography Methods", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 8 pp. 2464-2467 ,August, 2013

[3] A. Joseph Raphael, Dr.V Sundaram, "Cryptography and Steganography- A Survey."International Journal of Computer Technology and Applications" Vol 2 (3), pp. 626-630, (2011).

[4] Siva Janakiraman, Suriya.N, Nithiya.V, Badrinath Radhakrishnan, Janani Ramanathan and Rengarajan Amirtharajan "Reflective code for gray block embedding" Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering , pp. 215 March 21-23, 2012

[5] Khalil Challita and Hikmat Farhat. "Combining steganography and cryptography: new directions."International Journal of New Computer Architectures and their Applications *(IJNCAA)* 1.1 pp. 199-208. 2011:

[6] Hayfaa Abdulzahra, Robiah Ahmad , Norliza Mohd Noor. "Combining Cryptography and Steganography for Data Hiding in Images." Applied Computational Science pp. 128 2014

[7] Usha B A , Dr. N K Srinath , Aditya Nanjangud , Abhineet M Deshpande , Anthony Rebello "A Survey on Patient Information Protection Using Cryptographic and Data Hiding Techniques" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 4, pp. 6334-6336 April 2014.

[8] Vinay Pandey Manish Shrivastava "Secure Medical Image Transmission using Combined Approach of Data-hiding, Encryption and Steganography" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 12, pp. 54-57 December 2012

[9] Ketki Thakre, Nehal Chitaliya "Dual Image Steganography for Communicating High Security Information." International Journal of Soft Computing and Engineering (IJSCE) Volume-4, Issue-3 pp. 7-12 July 2014

[10] Sumit Mittu and Rajeev Sobti "Conveying Secret Messages through Album Art in MP3 File*s"* Proceedings of International Conference on Computing Sciences WILKES100 – ICCS 2013 ISBN: 978-93-5107-172-3 Elsevier Publications, 2013.