Grenze International Journal of Engineering and Technology, Jan Issue

Analysis and Implementation of Security Mechanism to Embed Medical Records in the Medical Image for Secure Transmission and Authentication

Rashmi Naveen[1], Deepa[2] and Chinmai Shetty [3]
[1-3]NMAM Institute of Technology / Department of Information Science & Engineering, Nitte, India
Email: rashmin@nitte.edu.in, deepashetty17@nitte.edu.in, chinmai@nitte.edu.in

***Abstract*—Information transmission over the net is a very common process and securing the information plays an important role. It is important to protect the sensitive information in Medical field as well. By considering safety hazards and exposure threats, it is very difficult to provide security to medical data. To maintain the relationship between medical firm and the public, medical firms must give assurance about the security of people's health records. In this paper, combined Cryptography and Steganography technique has been analyzed for securing patient information with the help of medical image. The patient information has been embedded into the medical images without affecting the image quality. Patients Records of varying sizes are analyzed with Blowfish and AES encryption techniques and embedded using LSB and Random Padding algorithms. The values of Peak signal to noise ratio (PSNR) are observed in different scenarios which shows blowfish technique under random padding gives better results without influencing image quality.**

***Index Terms*— data hiding, cryptography, LSB, AES, steganography, blowfish.**

I. INTRODUCTION

Over the decade, a lot of applications based on network are discovered such as on-line shopping, stock trading business, net-banking and bill payment etc. These transactions take place over the connection-oriented (wired) or connection-less / virtual connection (wireless) networks which asks for the need of secure connections, secrecy and integrity of the data. Many organizations are adopting the security principles and ethics. Health care sector is also one among them. Confidentiality and authentication of patient's records which are collected and stored across the different health sectors is of more concerned. Confidentiality obstruct health organization from revealing their patient's sensitive information to maintain trust relationship between organization and their patients. With this relationship, by ensuring security, organizations must make sure that patients are revealing all their health related information freely to physicians. This sensitive information is very essential for diagnosing problem clearly, preventing misconceptions, and discrimination. Patient's sensitive information can include most of their personal details, about their mental and physical health. It may be their age, family problems, financial problems, relationship concerns. Hence health sectors must ensure security of patient's personal details so that patient confidently share the information by assuming that his/her information won't be revealed. If privacy is violated, the patient may be confronted with potential problems as well as financial loss.
Encryption is one of the method used to ensure the guaranteed way of securing the sensitive information. There

Grenze ID: 01.GIJET.7.1.507_1

are many ciphering algorithms that perform substitution and transformation of plaintext into unreadable form. This method is Cryptography. There is also way to hide the information in digital files, this process is Steganography. Overall cryptography and steganography provides confidentiality of information but they have some drawbacks. Steganography fails when the presence of the text in the multimedia file is found out by the intruder [1]. Cryptography fails when the cipher-text is cracked by the intruder. With the Steganalysis and cryptanalysis techniques, it is possible for an attacker to reveal the confidential information. Hence the need arises to develop more secure technique. Combination of steganography and cryptography techniques results in a very powerful technique to secure data and helps in keeping it confidential [2].

II. Literature Survey

A. Cryptography

Cryptography makes use of mathematical functions on the plain text to convert it into unreadable form which ensures security, authentication and integrity of confidential information[3]. The main objective is to make information impossible to read by an eavesdropper. Cryptographic algorithms are divided into symmetric and asymmetric network cryptographies [3]. Symmetric algorithms are used to convert the plaintext to cipher text and cipher text to original messages (plaintext) by using the same secret key. While Asymmetric algorithms uses public-key to exchange key and then uses the secret key algorithms to ensure secrecy of stream of data [3]. In asymmetric cryptography, there is are two kinds of keys, one key is public-key which is known to public, and is used to encrypt data to be sent by the sender to a receiver who owns the respective secret-key. In order for transmission to occur, secret and public keys are both different and they need to be exchanged between the sender and the receiver. Maintaining privacy while interacting with end user so that third party can not able to learn it is the main objective of cryptography.

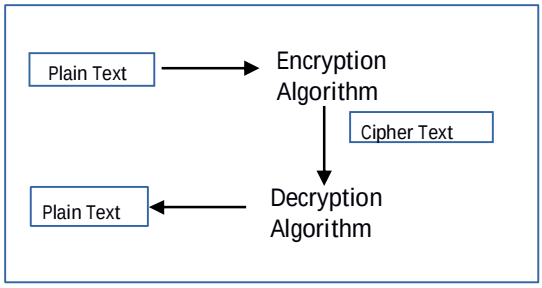

Fig. 1 Cryptography Model

B. Steganography

Steganography is derived from Greek language which means “secrecy writing” [4]. It is the process of concealing the secret in the other non-confidential information. The main objective of steganography is to send sensitive information through another media. Two important properties of effective steganography are: indiscernible to identify and sufficient volume to embed information [5]. This implies that the one can’t recognize that something is hidden in the media. In the cryptography, visible encrypted message may grab an attention of intruder, no matter how complex is the decryption of it. But in case of steganography, as the message is embedded in the other media, there is no way for an intruder to identify it. Different steganography techniques varies depends on their imperceptibility level and amount of information to be embedded in a cover.
Even the main intention of both Steganography and cryptography is security, but the way they are providing it varies. In the proposed work, integrated crypt-stego technique is used to ensure the security of patient's information.

III. Methodology

In the implementation we have made use of blowfish algorithm and AES for encrypting the plain text, and LSB algorithm and the random padding algorithm for image steganography. Initially documents of four different sizes related with patient's records are encrypted using the blowfish and AES algorithm each. Then, these encrypted text documents were embedded into an image file with a .jpg extension. The results of the embedded image files were stored and PSNR value were calculated for the same. The LSB algorithm as well as random padding was used to implement image steganography. The main requirements include transparency, hiding capacity and

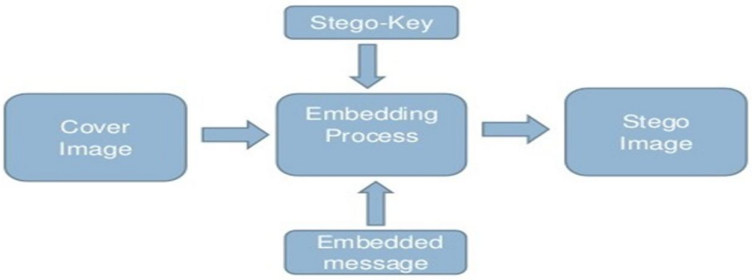

Fig. 2 Steganography System Model

robustness. Figure 3 shows the proposed cryptography-steganography combined model at sender side. At the receiver side, reverse procedure is carried out to obtain the plaintext.

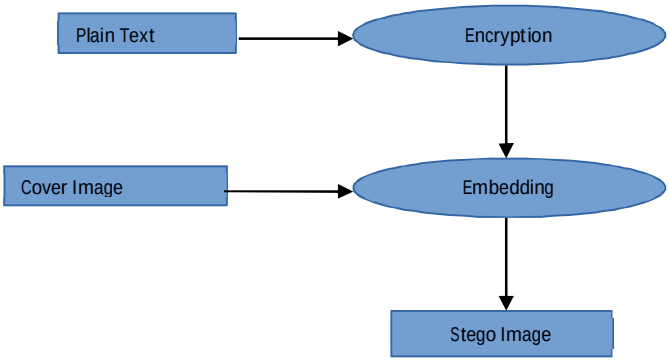

Fig. 3 Crypt-Stego System Model (At Sender side)

t is a symmetric block cipher [6]. In the symmetric algorithms, single key is used by the sender and the receiver to encrypt and decrypt the message. This key is known only to the sender and receiver. A block cipher is crypt-technique that works on a block of data at a time [6]. Processing is done on a single block at a time for encryption as well as for the decryption. Variable length key is used to encrypt the text. Blowfish is used since it is fast, simple to implement and very effective.

A. AES

AES or Advanced Encryption Standard is one more way of encrypting the information. AES is also a symmetric block cipher; that can process data blocks of 128 bits, using the key size of 2^7 bits, 192 bits, and 2^8 bits. The AES algorithm defines different types of transformations that are performed on information. This info is stored in an array. The first step of putting the info in an array is done; then transformation is performed for a number of times. The number of rounds is determined by the length of the key. Say,14 rounds for 256-bit keys, 12 rounds for 192-bit keys and 10 rounds for 128-bit keys [7]. AES algorithm is combined with steganography to provide extra layer of security [9].

B. LSB Algorithm

LSB or Least Significant Bit Steganographic method in which the information is hidden inside an image. Here the least significant bit is replaced with the secret message. Images are made of pixels each have their own RGB values, this technique makes use of these pixels by replacing every least significant bit of every byte with the encrypted/cipher text which may or may not result in minor distortion. These distortions are not visible to naked eyes. Comparison of different steganography techniques is done in [10] after re-conciliating it with RC4 and 3DES encryption techniques.

C. Random Padding

Random padding is a technique in which the image is converted in to flat array of pixels and the text is hidden in between them. Pixels are chosen randomly to embed text with the help of random function for pixels. Different

key sizes are used to produce random numbers for the pixel selection. Reverse procedure is applied to extract the text from an image.

IV. Result and Conclusion

A. Result

Figure 4 and figure 5 shows the result of proposed algorithm for two images. Figures shows both original images and the stego images after inserting the 20 KB text are shown below. Encrypted text files of different lengths are obtained by Blowfish and AES encryption. And the same files are analyzed for the two steganography methods- LSB and Random Padding. It shows Random Padding gives better result as compared with the LSB steganography algorithm for both types of encryption methods. Proposed algorithm is implemented in python and matlab for the encryption and image steganography respectively.

B. Performance Analysis

To measure the performance of proposed algorithm and existing algorithm, the metrics used is Peak Signal to Noise Ratio. It calculates the mean square error in the original images and stego images. Depends on the mean square error, peak signal to noise ration is obtained. High PSNR value indicates high image quality.
Table 1 shows the analysis of PSNR values obtained for the proposed method when experimented with Skull Cap Image.
And Table 2 shows the analysis of PSNR values obtained for the proposed method when experimented with Skull Fracture Image.
Result shows that the proposed algorithm when combined with blowfish encryption gives better results as compared with existing algorithm.

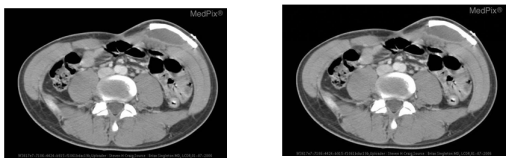

Fig. 4a Skull Cap Original and Stego Images

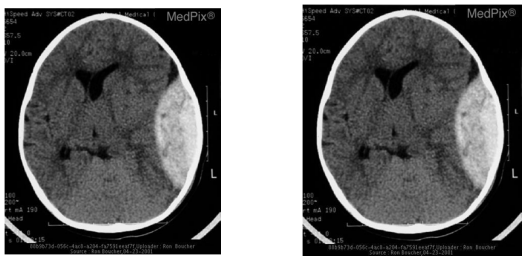

Fig. 5a Skull Fracture Original and Stego Images

TABLE I. PSNR VALUES FOR EXISTING AND PROPOSED ALGORITHMS WITH VARYING TEXT WHEN APPLIED ON SKULL CAP IMAGE

File Size	20kb	40kb	60kb	80kb
LSB	51.16	50.81	50.59	50.01
Random Padding	62.14	61.75	61.56	60.98

TABLE II. PSNR VALUES FOR EXISTING AND PROPOSED ALGORITHMS WITH VARYING TEXT WHEN APPLIED ON SKULL FRACTURE IMAGE

File Size	20kb	40kb	60kb	80kb
LSB	52.35	52.14	51.50	50.75
Random Padding	63.30	63.088	62.30	61.60

V. Conclusion

In this paper we have studied about Cryptography and Steganography as well as their combination. Both Steganography and Cryptography provides security but they have their own pros and cons. Hence combination of these two provides extra layer of security. First, we encrypt the message and then that message is embedded into an image. In the proposed work, LSB and Random padding steganography algorithms are compared. Result shows that the proposed algorithm provides better security for varying text with different cover images as it is impossible for an intruder to identify the difference between an original image and stego image.

References

[1] Mr. Falesh M. Shelke, Ms. Ashwini A Dongre, Mr. Pravin D. Soni, "Comparison of Different techniques for steganography in images", International Journal of Application or Innovation in Engineering And Management, Vol 3, Issue 2, February 2014, ISSN 2319-4847

[2] Md. Khalid Imam Rohmani, Mr. Amit Kumar Goyal, Manisha Mudgal, "Study of Cryptography and Steganography System", International Journal of Engineering and Computer Science, Vol 4, Issue 8, August 2015, ISSN 2319-7342

[3] Vishnu S Babu, Prof. Helen K J, "A Study on combined Cryptography and Steganography",International Journal of Research Studies in Computer Science and Engineering, Vol 2, Issue 5, May 2015, ISSN 2349-4859

[4] Sara Khosravi, Mashallah Abbasi Dezfoli, Mohammad Hossein Yektaie, "A new steganography method based HIOP (Higher Intensity Of Pixel)algorithm and Strassen's matrix multiplication", Journal of Global Research in Computer Science, Vol. 2, No. 1, 2011

[5] Priya Thomas, "Literature Survey on Modern Image Steganographic Techniques", International Journal of Engineering Research and Technology, Vol 2, Issue 5, May 2014, ISSN 2278-0181

[6] Ajit Singh, Swati Malik, "Securing Data by Cryptography with Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Isuue 5, May 2013, ISSN 2277-128x

[7] Mr. Gurjeevan Singh, Mr. Ashwani Singla and Mr. K SSandha, "Cryptography Algorithm Comparison forSecurity Enhancement in Wireless Intrusion DetectionSystem", International Journal of MultidisciplinaryResearch, Vol.1 Issue 4, pp. 143-151, August 2011.

[8] Hemalatha .M, Prasanna.A, Dinesh Kumar R, Vinoth kumar D - "Image Steganography Using HBC and RDH Technique" International Journal of Computer Applications Technology and Research Volume 3– Issue 3, 136 - 139, 2014, ISSN: 2319–8656

[9] N. Rashmi and K. Jyothi, "An improved method for reversible data hiding steganography combined with cryptography," *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, 2018, pp. 81-84. doi: 10.1109/ICISC.2018.8398946.

[10] N. Rashmi, "Analysis of Audio Steganography combined with Cryptography for RC4 and 3DES Encryption," *2020 Fourth International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, India, 2020, pp. 210-214, doi: 10.1109/ICISC47916.2020.9171142.