Secure E-Health using Images Steganography

Manikandan T\textsuperscript{1}, Muruganandham A\textsuperscript{2}, Babuji R\textsuperscript{3}, Nandalal V\textsuperscript{4} and Mazher Iqbal JL\textsuperscript{5}

\textsuperscript{1}Professor, Department of Electronics and Communication Engineering, Rajalakshmi Engineering College, Chennai.
\textsuperscript{2}Professor, Department of Electronics and Communication Engineering, Rajarajeswari Engineering College, Bangalore
\textsuperscript{3}Assistant Professor, Department of Electronics and Communication Engineering, R.M.K Engineering College, Chennai
\textsuperscript{4}Professor, Department of Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, Coimbatore
\textsuperscript{5}Professor, Department of Electronics and Communication Engineering, Veltech Dr.RR and Dr. SR University, Chennai.

* Corresponding author’s e-mail: manikandan.t@rajalakshmi.edu.in

Abstract. The main aim is to secure the medical records by ensuring safe communication between the sender and the receiver by adding multiple layers of security. This project is a combined approach of both encryption and steganography to give security the utmost importance. In the sender, only the authorized person can send the secret image to the receiver. In the first stage, an image steganography system is processed using confidential medical X-ray images which are hidden under the cover images. The encryption method used is based on Random Number Generator and the pixel indicator, in other words, by moving the position of the pixel in the image to encrypt the image on the transmitting side. Whereas on the receiver side, this project proposes a method to authenticate the receiver by incorporating Email Authentication and OTP Verification to decrypt the encrypted image.

Keywords-Security, Medical Image, Encryption, Steganography, OTP, Email authentication.

1. Introduction

Information Security is the practice of defending information from unauthorized access. Security systems include information hiding and cryptography. In cryptography, the secret message is encoded in another unknown message in which sender and receiver only know the technique to decrypt the secret message back. But there is a disadvantage in this technique that is the other member who can able to that something is hidden inside the text so this led to the decoding of the secret message other than the sender and receiver. To overcome this disadvantage, the Steganography technique was introduced. In Greek, Steganography stands for covered writing. Steganography is the method in which a secret message is hidden under another message so that the hidden secret message can be concealed. Steganography is of two types. One is Technical Steganography and the other one is Linguistic Steganography. This is based on the spatial domain as it explains the LSB technique where the cover image is used to hide the secret data. This paper is structured as follows: Section 2 deals about the review of literatures; Section 3 describes about the proposed methodology; Section 4 demonstrates the results and discussion and finally, Section 5 gives the conclusion.
2. Review of Literatures

The works related to the areas of steganography and encryption, to send the secret image securely by using a cover image, is described in this section:

Bhargavi et. al proposed a multi-layered approach based on cryptography to ensure safe transmission of images considered to be clandestine which states that the cover image embeds the secret image by alternating the LSBs of the cover image in-exchange with the secret image [1]. The unauthorized user or the intruder cannot see the secret image and be able to modify it so that they won’t observe the secret image which is embedded when transmitting over the Internet.

Raniprima et. al developed steganography of digital image along with encryption which is based on the principle of Rubik's cube. It is a hybrid approach of the above two listed paper as they have an effective and desired result and effectiveness as the suggested plan is tested using histogram survey, the effect of avalanche, attack of brute-force, optical attack, statistical attack of analysis of chi-square, and study of dimension and embedding location dissimilarities [2].

George Amalarethinam et. al modelled encryption and decryption of image in known-key cryptography which shows that the image chosen to be encrypted is made into a format resembling a rectangle shape i.e. m*n where the rectangle image is then converted into single-byte blocks and then the magic rectangle replaces the block. Then, the Magic Rectangle’s (MR) parameters of control are chosen randomly. The image is then encrypted by known-key algorithms of cryptography [3].

Pooja Rani et. al developed an image security system using encryption and steganography proposed a study which is a hybrid approach of all the three possible way of ensuring secured transmission i.e. encryption compression and steganography as it still not being 100% efficient and to date is a problem for image transmission which make transmission in places like satellite and military difficult as security is a major concern here [4].

Saini et. al developed a hybrid method for security in images by combining both the concepts of encryption and steganography which proposed a study that shows the hybrid of cryptography and steganography where MAES which is an updated version of AES is used to overcome the drawbacks of both AES and DES [5]. In the case of MAES up to 256 bits can be used and this method follows a principle of encrypting the image by depending on the LSB and not the MSB which makes it secure than other previously proposed methods.

Ahmed et. al developed a model aiming at the integrity of data using steganography and hashing approaches in which the latest implemented technique for encryption is suggested which are embedding the text data into the digital image using a hashing technique [6]. This hashing is simple compression of one form of data into another compressed form which is done using an AES and an MD5 algorithm for compressing text into simpler formats that are implemented to increase the robustness and quality of the encryption.

Abood et. al developed a literature survey on image steganography based on medical data which states that steganography is both a science as well as an art of imperceptible transmission that came as a rescuer by giving maximum security through different techniques [7]. Image steganography based on medical data is a unique category of image steganography. It has come a distant way to make the transmission of images related to medical data secure and to assure that it does not affect the analyzed reading of the image. Security and safety are the most important aspect of transmission now. While sharing and sending images or documents over the internet, the sender needs clear assurance of privacy, secrecy, and safety, as nowadays communication is not only made restrictions on chatting but it also plays a very important role in various lines and sector of image transmission and communication [8,9,10,11,12]. This work focuses on the different algorithms used in the steganography of medical image and finds out the best on various parameters such as being robust, PSNR (Peak Signal to Noise Ratio) value, MSE (Mean Squared Error) value, and payload capacity.

3. Proposed Methodology

Secure E-Health using Image Steganography is a hybrid of several methods that have been proposed. The proposed system helps the user to send data safely by providing multiple layers of security. These
securities make it hard for an intruder to access the file or open it. Thus, the intruder can’t understand what is transmitted which increases robustness. The secret image is encrypted by random pixel generator method and embedded into the cover image to create a Steganography image using MATLAB 2021 and this is authenticated using credentials such as User ID, Password, and OTP verification which is done using a tool called Pega. The main objective of this work is to provide sufficient and secure transmission of the image assuring complete encryption. This work also proposes to authenticate the sender and receiver multiple times to confirm the identity. In the encryption part, the secret image is encrypted by interchanging the pixels based upon an algorithm called random pixel generator. The key used is random and only the sender and receiver know it. The user ID and password were retrieved by using the Pega Database, which is sent via email. The OTP is sent by the Pega tool to the mobile number of the authenticated sender. The same two-level authentications are incorporated in the receiver end also. Thus, the proposed paper helps to transmit images securely and safely from sender to receiver. The various blocks involved in the proposed system at the transmitter and the receiver are given in Figure 1 and Figure 2, respectively.

![Figure 1. Transmitter Block Diagram](image)

On the transmitter side, the authenticated user verifies his identity using Email Authentication and OTP Verification. Email Authentication is done by sending the login credentials of the authorized user to the sender’s mail id using the Pega tool. OTP Verification is done by sending the OTP to the sender’s mobile number. After successful authentication, the sender will be able to send the secret image. MATLAB is used in the backend which is implemented with the process of Encryption and Steganography. Encryption and Steganography are completely processed by the transmitter end where the secret image is first encrypted using the principle of XOR Cipher Encryption then the Image Steganography is done using the LSB method finally generating a stego image, and this is done using MATLAB.
On the receiver side, the same process of decryption happens, followed by the two-level verification using email authentication and OTP generation using Pega. This ensures that only the authorized receiver can receive and view the secret image sent by the sender.

3.1 Algorithm Used

1. The various techniques are available. 1. LSB
2. Encryption

3.2 Advantages

- It can be applied differently in the digital image, audio, and video file.
- Fingerprint and RFID giving added advantage towards the security

It’s the most reliable system compared to the existing system.

3.3 LSB

LSB represents the least significant bit. It is image steganography technique that works with the least significant bit values of pixels. This method does not result in any distortion of the image during data integration. The Least Significant bit value differs but this change is hidden from the human eye. The image will not deform using the LSB technique, this will encrypt a lot of data behind the image, this is the main advantage of LSB. It causes some shortcomings as it is less robust, sometimes changes in the image can lead to a loss in the data i.e. less secure data transfers to the recipient safely without allowing someone to access the secret data. To hide the message inside a picture by substituting the least significant bit of the picture is known as LSB Steganography. With the help of alteration, the first bit to the right of an image insert out secret data this also make the image invisible, but if our message is too big, it will begin to alter the second rightmost bit and so on and a hacker may able to identify the image changes.

3.4 Encryption

The process of encoding the message which only can be understood by certain people is known as Encryption. This uses an algorithm to encrypt data and then decrypt the data using the key in the
receiver end. Plaintext refers to the message found inside an encrypted message. It is classified as ciphertext because it is encrypted and unreadable. Simple types of encryption can be as simple as changing letters. Cryptographers added more steps as cryptography advanced, making decryption more difficult. Complex encryption systems can be created by combining wheels and gears. Mechanical encryption has been replaced by computer algorithms.

Encryption uses algorithms to mix up your data. They are then sent to the recipient, who can decrypt the message with a key. There are numerous kinds each involving divergent ways to scramble and decipher the information.

Key generation: Keys are produced using random number generators or computer algorithms that imitate random number generators. A further elaborated process that computers will create keys is by making use of mouse movements to fabricate special seeds. In Modern forward confidentiality, systems include the creation of a new key for each session to attach another layer of security.

XOR Cipher Encryption: An additive cipher is the XOR cipher. It is also referred to as exclusive disjunction based on the xor operation in logic. OR is also known as modulus 2 addition as a logical operation. When the input differs, the output is true in the XOR operation. To put it another way, the XOR operation means either one, but not both, or zero. The XOR cipher encrypts data using the XOR logical operation. A random key is generated first. The key is then used to perform.

4. Results and Discussion

The security of the transmitted data is ensured by steganography and the message can be accessed by an authorized person only with a user ID, password, and OTP authentication. The Secret Image is encrypted using the pixel exchange to which the message is put into the Cover image using LSB substitution which finally produces a stego Image. The Secret image is taken out of the stego image using the reverse methodology and it is ensured that no data is lost during this process. MATLAB and Pega tools are used for the implementation of this work. The generated stego image for a input sample image at the transmitter and decrypted secret image at the receiver are shown in Figures 3 and 4, respectively.

![Figure 3. Sender side](image-url)
Figure 4. Receiver side

In the above figure, we have analyzed the histogram values for the pixels of the secret image before the transmission and after the reception, the result both are moreover similar and the image received is the same as sent. The performance metrics such as PSNR, MSE and SSIM of the proposed work is compared with the existing works is given in Table 1. From Table 1, it is evident that the proposed work is significantly improves the PSNR, MSE and SSIM than the existing works.

Table 1. Comparison of the proposed work with existing works

| Authors                  | PSNR (dB) | MSE     | SSIM  |
|--------------------------|-----------|---------|-------|
| Poojarani et. al (2015)  | 30.65     | 0.965   | 0.759 |
| Ahmed Hambouz et. al (2019) | 48.58    | 0.420   | 0.95  |
| George Amalarethinam et. al (2015) | 14.94    | 0.963   | 0.625 |
| Saini et. al (2013)      | 25.96     | 0.968   | 0.724 |
| **Proposed work**        | **48.94** | **0.352** | **0.958** |

5. Conclusion

Steganography's main use is to hide secret messages (i.e. secret image) inside the cover image without showing many variations to the actual image. All the steganography types have less restriction on the capacity for the data that has to be covered in the colour image. The Entire idea of this work is to get the Image received by the authentic user alone and this is done by confirming one’s identity by user id password and OTP verification which is to increases the security at the ends and makes intrusion in the channel a challenge.

6. References

[1] Hambouz A *et al.* 2019 Achieving Data Integrity and Confidentiality Using Image Steganography and Hashing Techniques *Proc. 2nd Int. Conf. on new Trends in Computing Sciences*, Amman, Jordan, pp. 1-6.

[2] Abood MH 2017 An Efficient Image Cryptography using Hash-LSB Steganography with RC4 and Pixel Shuffling Encryption Algorithms *Annual Conference on New Trends in Information & Communications Technology Applications*, Baghdad, Iraq, pp. 86-90.

[3] Bhargavi K, Thota Sri Harish Reddy and Thota Bhaskara Reddy 2016 Multilevel Crypting Approach for Ensuring Secured Transmission of Clandestine Images *Proc. Int. Conf. on Electrical, Electronics, Communication, Computer and Optimization Techniques*, Mysuru, pp. 302-306.

[4] Raniprima S and Hidayat B 2016 Digital Image Steganography with Encryption Based on Rubik’s Cube Principle *Proc. Int. Conf. on Control, Electronics, Renewable Energy and Communications*, Bandung, Indonesia, 2016, pp. 198-201.

[5] Amalarethinam DIG and Geetha JS 2015 Image encryption and decryption in public key cryptography based on MR *Proc. Int. Conf. on Computing and Communications Technologies*, pp. 133-138, doi: 10.1109/ICCCT2.2015.7292733.

[6] Pooja Rani and Apoorva Arora 2015 Image security system using encryption and steganography *International Journal of Innovative Research in Science, Engineering and Technology*, Vol. 4(6), pp. 3860-3869.
[7] Saini JK and Verma HK 2013 A Hybrid Approach for Image Security by Combining Encryption and Steganography Proc. Int. Conf. on Image Information Processing, Shimla, India, pp. 607-611.

[8] Kouser R, Manikandan T and Kumar V 2018 Heart disease prediction system using artificial neural network, radial basis function and case based reasoning Journal of computational and theoretical nanoscience, vol. 15, pp. 2810-2817.

[9] Manikandan T and Bharathi N 2016 Lung cancer detection using fuzzy auto-seed cluster means morphological segmentation and SVM classifier Journal of Medical Systems, vol. 40(7), pp. 1-9.

[10] Manikandan T and Bharhathi N 2011 Lung cancer diagnosis from CT images using fuzzy inference system Communications in computer and information science, vol.250, pp.642-647, ISBN: 978-3-642-25733-9.

[11] Karthikeyan S, Manikandan T, Nandalal V, Mazher Iqbal JL and Jai Jaganath Babu 2019 Survey on Despeckling Filters for Speckle Noise Removal in Ultrasound Images Proc. 3rd Int. Conf. on Electronics Communication and Aerospace Technology, ISBN: 978-1-7281-0167-5, pp. 605-609.

[12] Balasubramanian V, Saphagirivasan V, Selvaganesh M and Manikandan, T 2021 Adoption of an integrated near field communication and natural language processing system toward improvement of telehealth solutions Biomedical Engineering - Applications, Basis and Communications, vol. 33(1), pp. 2050041.