Video Steganography in the Field of E-Healthcare

A. Jamuna[*]

Department of Information Science and Engineering, New Horizon College of Engineering, Bangalore, India

***Abstract*: Steganography is the creative art of concealing confidential messages or secret data inside an ordinary file. This helps to prevent the detection of the existence of secret data. Steganography takes data hiding one step ahead than the normal data encryption. Data encryption hides the data, but Steganography hides the existence of the data. In this project we use video as the cover media for hiding the data and therefore stressing on the concept of video steganography in the field of E – healthcare. The main idea of e-healthcare is to provide healthcare facilities to patients where doctor-patient distance is immaterial. In this regard, the Electronic Health Record (EHR) of a patient needs to be just exchanged securely. This EHR includes clinical data such as pharmacy notes, medical insurance details, doctor prescription, laboratory reports, the data with respect to health monitoring like blood pressure, sugar level, heartbeat and other medical records. The conventional way is concealing the EHR in encrypted medical images. This may cause capacity and data loss issues. Whereas the proposed method works on videos that confer enough capacity to conceal the EHR data which can be any format such as text, image, audio or video. AES, Wavelet and Fernet algorithms are used, which makes the EHR data robust against attacks. Therefore, the proposed method is highly capable in e-healthcare scenarios.**

***Keywords*: video steganography, healthcare.**

1. Introduction

Video Steganography is a technique to hide any kind of files into a cover Video file. Steganography is the art and science of embedding hidden information in such a way that no one, apart from the sender and intended recipient, identifies the existence of the message into the cover file. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different invisible information.

This hidden information can be plain text, cipher text, audio or even images. In a computer- based audio Steganography system, secret messages are embedded in digital audio. The secret message is embedded by slightly altering the binary sequence of the sound Existing audio Steganography software can embed messages in WAV, AU, and even MP3 audio files. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images because human air is very perceptible to noise. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide message. The use of the video-based Steganography can be more secure than other multimedia files, because of its size and complexity. Steganography is an age-old practice Steganography in, Multimedia Steganography deals with video, audio, and images all together. To achieve privacy on another level, Steganography is combined with Encryption effectively. A video file is used as a cover medium to hide the secret message. It is less prone for Stefano-analysis as a video file is a combination of text, image and audio. It is a collection of certain frames running at some constant speed and is measured in frame per second. In order to embed a secret message in a video file first, we have to extract the frames from it. In 5 orders to embed the message in video file first, Frame conversion is done. It is a process of converting a video to consequent images or frames and then each or one frame is used as carrier data to conceal the hidden information. After the embedding process, all frames are merged together to produce the stego video. We are using AES algorithm, Wavelet algorithm and Fernet algorithm. Were In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES have been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of ‘future-proofing’ against progress in the ability to perform exhaustive key searches. In mathematics, a wavelet series is a representation of a square-integrable (real- or complex-valued) function by a certain orthonormal series generated by a wavelet. This article provides a formal, mathematical definition of an orthonormal wavelet and of the integral wavelet transform. Fernet guarantees that a message encrypted using it cannot be manipulated or read without the key. Fernet is an implementation of symmetric (also known as “secret key”) authenticated cryptography.

Relevance of the Project:

As the world becomes more anxious about the use of secret communication, and as regulations are created by governments to limit the use of encryption so the importance of steganography becomes prominence day by day. In this paper, we combine the concept of cryptography and steganography. On the other hand, when we really higher amount of data must be embedded in the case of video sequences, there is a more demanding constraint on the real-time effectiveness of the system. The method utilizes the characteristic of the human vision’s sensitivity to color value variations. The aim is to offer the safe exchange of color steganography video across the internet that is resistant to all the steganalysis methods like the statistical and visual analysis. This paper provides an overview

[*]Corresponding author: jamunaa99@gmail.com

of various Video Steganography schemes.

The effective Steganography should have the following characteristics:

Secrecy: Extraction of hidden data from the host medium should not be possible without the knowledge of the proper secret key used in the extracting procedure. Imperceptibility: After embedding the data in the medium, it should be imperceptible from the original medium. High capacity: The maximum length of the hidden message that can be embedded can be as long as possible. Resistance: The hidden data should be able to survive when the host medium has been manipulated, for example lossy compression scheme. Accurate extraction: The extraction of the hidden data from the medium should be accurate and reliable.

Purpose of Study:

The Purpose of this study is to make the healthcare system more effective using e- healthcare facilities where the distance between the doctor and patient is immaterial. Video steganography in this field makes it safer and gives high security for the confidential patient records by concealing within a cover media and hiding even the existence of data. This system enables both patients and hospital administration to share data without any thought of data breaches and thereby achieves data integrity.

Scope of the Project:

The scope of the project is to limit unauthorized access and supply better security during file transmission between the hospital and patients. To meet the wants, approach of Video Steganography is chosen. During this project, the proposed approach finds the acceptable algorithm for embedding the info of any form into a video using steganography that is achieved using a set of algorithmic techniques such as AES, Fernet and wavelet transform, which provides the higher security pattern for transmission of files through a network

Problem Definition:

"To design and implement a system in the field of e-healthcare using video steganography technique in order to secure the electronic health records of any format like text, image audio or video within a video enabling high security and data integrity"

Proposed System:

The Proposed System focuses at the e-health care systems at the e-healthcare systems for the secure transmission of electronic health records and confidential data related to hospital and patients via network and protect them from the middle men or hackers.

Applications:

In the business world Steganography can be used to hide a secret chemical formula or plans for a new invention

Steganography can also be used for corporate espionage by sending out trade secrets without anyone at the company.

Privacy and security concerns over protected health information are the largest barrier to electronic health record adoption; therefore, it is imperative for health organizations to identify techniques to secure electronic health records. Some of the problems in the current e-health records system are that they can be easily modified, stolen or deleted by intruders in the system. After analyzing the results, the researchers concluded that the two most frequently discussed

Objective of the Study:

- The objective of the project is to provide a secure means of data communication using steganography techniques. The project will allow the user to transmit sensitive data within cover media and provide a less suspicious means of data communication as opposed to cryptography.
- Project aims at safeguarding confidential patient and hospital data by preventing the attacks or data thefts during the transportation of data via network by using encryption and steganography.
- Proposes a system based on video-based steganography and encryption authentication system for patients and hospital executives for safe transmission of data.
- The other goal of steganography is to avoid drawing suspicion to the existence of a hidden message.

Existing System:

1. In spite of Improving Technologies, most of the health-care Institutions and hospitals till maintain and use the paper-based health records and are transported using physical means. For the paper records to reach the specified parties, they must either be mailed or converted into electronic formats via emailing or scanning.
2. These traditional ways have many security vulnerabilities. Medical records are the property of the hospital/ patient's medical practitioners. It is the confidential communication between the parties involving medical research papers, medical audits/statistical studies, insurance papers, patient bills, scanning reports, etc.

Limitations:

1. Huge number of data, huge files size, so someone can suspect about the existence of the Steganography.
2. If this technique is gone into the wrong hands like hackers, terrorist, criminals then this can be very much dangerous for all.
3. The size of the secret data hidden inside the video cannot be greater than the cover video capacity.

2. Methodology

A video can be viewed as a sequence of still images. Data embedding in video seems very similar to images. However, there are many differences between data hiding in images and videos, where the first important difference is the size of the host media, since videos contain more sample number of pixels, a video has a higher capacity than a still image and more data can be embedded in the video.

Proposed System uses the following algorithms.

AES Algorithm: AES is based on a design principle known as a substitution- permutation network, and is fast in both software and hardware. AES operates on a 4Ã—4 column-major order matrix of bytes, termed the state.

a) Shift Rows Transformation In shift row transformation, the rows of the matrix are circularly left shifted. Row 0is kept constant; Row 1 is left shifted by 1 byte; Row 2 is shifted by 2 byte and finally last row by 3 byte.
b) Mix Column Transformation Each column in the new formed matrix is multiplied with each column of the predefined matrix.
c) Add Round Key, the resultant matrix is xor-ed with the expanded key generated from the initial key.

Wavelet Transform: As a mathematical tool, wavelets can be used to extract information from many different kinds of data, including – but not limited to – audio signals and images.

Fernet Algorithm: Fernet builds on best practice cryptography methods, and allows developers to provide a simple method of encrypting and authenticating.

Advantages:

1. *Robustness:* Robustness is the ability of the hidden message to remain undamaged.
2. *Security:* The advantage of video steganography, is that messages do not attract attention to themselves. information from the original file during transmit.
3. Tamper Resistance of all the features, this feature is very important.
4. *Flexible:* The proposed system is flexible, enabling all formats of data files to be steganography within a video, thereby providing users flexibility to transport any type files with protection.
5. *Communication:* Steganographic methods hide the encrypted message in cover carriers so that it cannot be seen while it is transmitted on public communication the quality of that medium. Hence it serves as a secure medium to share important files.
6. Simple and Easy to use: The system is designed in such a way that the UI and the functions are easily understandable.

3. Experimental Results

Outcome of Proposed System:

Home Screen of the proposed system with the two separate login authentications for patients or the Hospital staff.

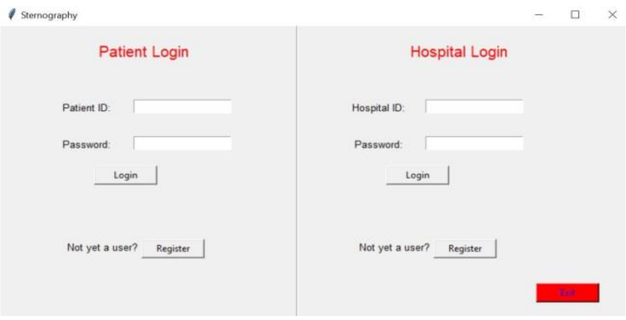
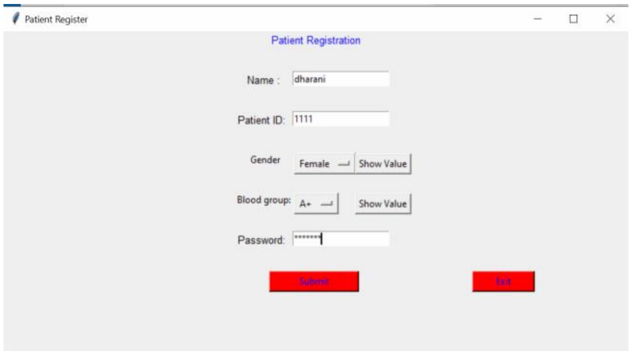


Fig. 1. Home screen

If the user is not a pre- registered with his/her details then the Patient can fill the details into the below shown page and then can log into the system.



Name : dharani

Patient ID: 1111

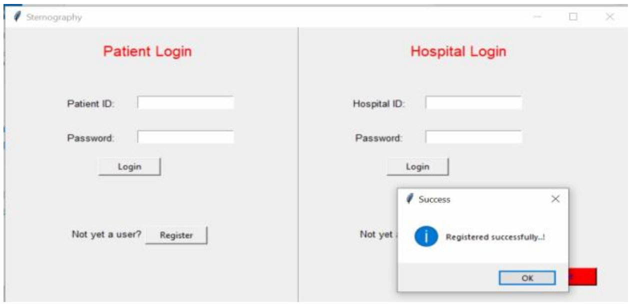
Gender Female

Blood group: A+

Password: *******

Fig. 2. Patient registration page

Once the registration is done by the patient. The dialogue box as represented in the fig 6.3 will appear with the statement "Registered successfully….!"



Registered successfully..!

Fig. 3. Registered successfully

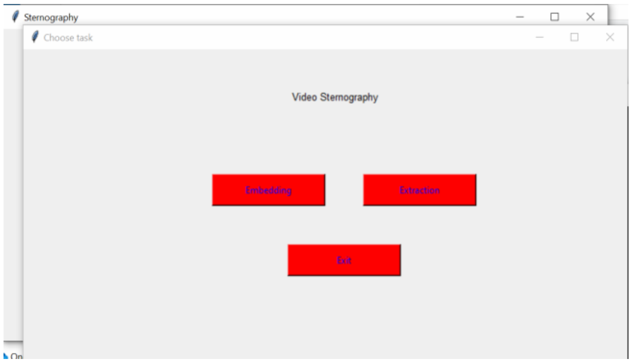
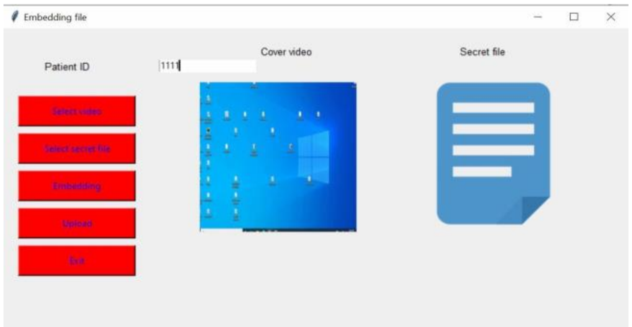


Fig. 4. Menu of functionalities

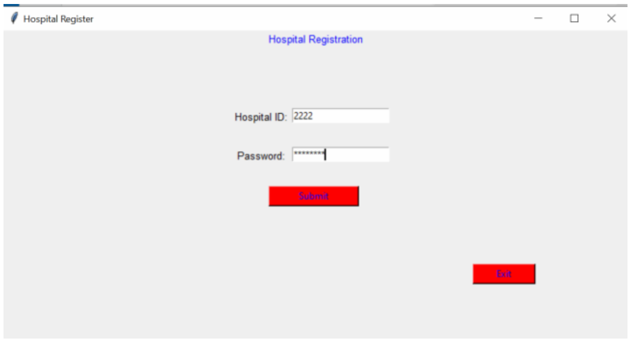


Patient ID 1111

Fig. 5. Embedding of secret file into the cover video

Table 1

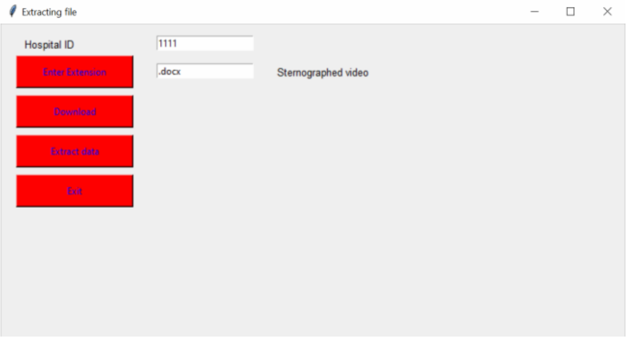
Test Case ID	Test Case Description	Input Data	Expected Output	Actual Output	Status
1	Patient Registration	Name Patient ID Gender Blood Group Password	Registered Successfully	Registered Successfully	Pass
2	Patient Login	Patient ID Password	Patient Login Successful	Patient Login Successful	Pass
3	Embedding	Cover Video Secret file	File is steganographed successfully	File is steganographed successfully	Pass
4	Uploading	Steganography Video	File is uploaded successfully!	File is uploaded successfully!	Pass
5	Hospital Registration	Hospital ID password	Registered Successfully	Registered Successfully	Pass
6	Hospital Login	Hospital ID password	Hospital Login successful	Hospital Login successful	Pass
7	Downloading the steganography video	Patient ID Extension of file	Successfully downloaded	Successfully downloaded	Pass
8	Extract data	Steganography video	File extracted successfully	File extracted successfully	Pass



Hospital ID: 2222

Password: ********

Fig. 6. Hospital registration page

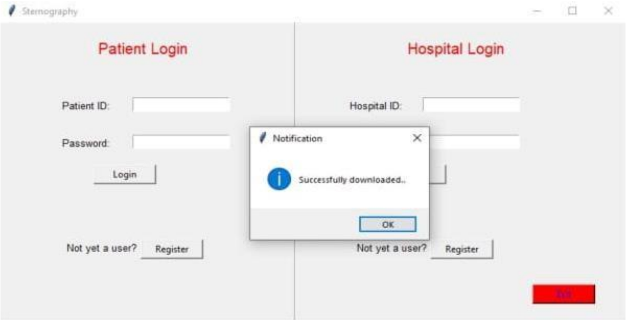


Hospital ID 1111

.docx

Sternographed video

Fig. 7. Hospital ID and the extension of the document



Successfully downloaded..

Fig. 8. File is successfully extracted and downloaded

4. Conclusion and Future Enhancement

A. Conclusion

The project presented focuses on the data security, reliability and integrity of the confidential data transmitted between patients and the hospital, thereby making the E- healthcare system more efficient. Hospital data of any type such as text document, image, video, audio, etc. Any of such data can be hidden in the cover media, which is a video. The confidential data is protected by three level security using AES encryption + high level steganography + firebase. This project uses the idea of using video as the cover media, which can be a good substitute channel to hide data, since it has many exceptional features such as high capacity and good imperceptibility. The project allows both the hospital administration and the patients use the system by the registering and logging in individually. Project facilitates both Embedding and extracting of the data on both the sides using highly secured algorithmic techniques and therefore can be a great alternative over the naïve techniques of transmission of confidential data.

B. Future Enhancement

The project has a lot of scope for the enhancement and further developments.

- The proposed system can be enhanced in terms of capacity and robustness for better efficiency and effectiveness.
- The noise contained in the extracted data and embedded media can be removed to obtain more precise results. Other different and more efficient techniques for steganography can be performed.
- Reduction of processing time is a factor to be worked on.
- Future work can be performed on the functionality of the GUI, which is slightly limited and can be improved.

References

[1] Balu, Sidharth & Babu C, Nelson & Kandasamy, Amudha, “Secure and efficient data transmission by video steganography in medical imaging system,” in *Cluster Computing*, vol. 22, 2019.