IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Hospital Database System Using Image Steganography

Prof. Diksha Bhave[1], Swanand S. Desai[2], Rahul N. Mahale [3], Ritesh L. Mhatre[4]

[1234]Department of Computer Engineering,

[1234]Shivajirao S. Jondhale College of Engineering, Thane, Maharashtra, India

Abstract **–** Steganography is the process of concealing secret messages in color covering images, steganography hides the existence of the message within the color image so that it cannot be seen by natural eyes. Steganography is a crucial process that can be utilized in multiple life applications. This paper will introduce some methods used for data steganography. These methods will be implemented and results based on the experiment will be gained. A great method of steganography will be utilized, it will be shown how this method will bring efficiency, capacity, security, and covering image quality. To give more security for the biomedical reports for the patient privacy for the patient highly confidently patient image reports can be placed in databases digitally. If unknown persons like hospital staff, relatives, and third parties like intruders trying to see the report it has in the form of a hidden state in another image. The patient detail like Patient Name, Age, Gender, referred by a doctor, referred to, Date, Medicine Names have been converted into any form of steganography. Then, encrypt those images by using the proposed steganography algorithm and placed them in the database**.**

I. INTRODUCTION

In the present time, as everything is turning into digital, sending data or private information is rapidly increasing. At the same time, threats of data hacking or leaking are also increasing. This threat has imposed people to share their data confidentiality. Possible reason for data hackers to hack or leak the information is that they can read and understand the data. Intruders may reveal the information to others, alter it to misrepresent an individual or organization, or use it to launch an attack. One alternative to this problem is, through the use of steganography. Steganography is a method of hiding information in digital media. In opposite to cryptography, it is not to keep others unaware about concealed information but it is to keep others from thinking that the information is even available. Steganography has become more important as more people join the World Wide Web revolution. Steganography is the art of concealing information in ways that avoids the detection of hidden messages. Steganography includes an array of secret communication methods that conceal the message from being seen or discovered. Because of advances in Information and Communications Technology, most of information is kept electronically. Ultimately, the security of information has become a fundamental issue. Along with cryptography steganography can be used to conceal data securely. Apart from concealing data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video and images. The increasing opportunities of modern communications require the specific means of security specially on computer network. As the digital data sharing had raised, network security becomes an issue. Therefore, the confidentiality and data integrity are necessary to keep it safe against illegal access and use. This has impacted in tremendous growth of the field of information concealing. Information hiding is an emerging research area, which comprises applications such as copyright protection for digital media, virtual lockers, etc. Steganography conceals the secrete message inside the host data set. In today's world all the hospitals are transforming from papers to the e record, it comprises data of patients and assists in the further treatment. The diagnosis by the doctor is determined by the data in these digital images. If someone corrupts this data, then the whole treatment will be affected. Due to the non-availability of patient's history of treatment, diagnosis, etc. at one place across departments or doctors or hospitals, the treatment is delayed or affected. Thus, to avoid such problem, steganography resolves the issue fundamentally. This methodology will ensure the safety of data and thus ensuring timely and effective treatment. As it offers to have all information at one place, it will result in quick treatment and timely treatment. This Paper primarily focused on the data security while sharing the information digitally. Also, this conceals the patient report and treatment in the scanned images. This paper also introduces the application of mixed perspective to the steganography in medical field.

II. PROBLEM DEFINITION

There are problems with traditional systems. In the current scenario information is very difficult to acquire and to find specific information. Like to find out about the patient's history, the user has to pass through different registers. The information generated by virus transactions consumes time and effort to be saved at the right place. vital modifications to data like patient details or doses of vaccines are difficult to make as paperwork is involved. Preparation of accurate and prompt patient reports becomes a challenging job as information is difficult to collect from the viral register. Calculation which are done manually can have error and consumes too much time. This can cause differences, mistakes and discrepancy. For example, calculation of patients' bills based on different treatments given.

.

III. LITERATURE REVIEW

Steganography and its current usage

The tremendous innovations in the field of network communications during the past years have generated a need for safe image transmission over the Internet. Internet is an open network and is not so safe for the transmission of confidential data. To meet this challenge, steganographic techniques need to be applied (Savitri G, K.L. Sudha 2014). Image steganography is very interesting and important technique which attracts many researchers to perform research on it to find and suggest new and better solution to make important information more secure (Azmat U, Mohsin I, 2018). There are two types in in this, which have been used by researcher till now, and we get ample information about this in detail. Cryptography is method of saving and transferring data in specific form so that only those who have been given access can read and use it. because of generated cipher text, one can explain message has been encrypted. And attacker try to regain secret message by having a chain of attack on cipher text. And if attacker couldn't succeed, then might be possible that during attack encrypted secret message will be destroying. Steganography is an art of covering secret and confidential information within a carrier which could be an image file.

In steganography, there are various forms like image steganography, audio steganography video steganography, etc. Amongst this, all are best and gives good results but image is simple to handle and not very complex. As because Image Steganography does not take more space in a system and its compression is lossless. Such loss is not very high. On the contrary, audio and video are little lossy. In image steganography, image is used as a cover object to hide data behind it. In image steganography, the message is hidden behind cover object by changing the bits. The bits are changed by using a very famous and most useful technique called Least Significant bit (LSB). In LSB, the redundant bits image is replaced by bits of data. In this way message is hidden behind image cover object and this image can be normally send from one point to another point using any sharing device.

This system works better when the file is longer than the message file and image is Gray scale. (PAWAN S. and others, 2018). This technique provides an invisible form of communication since an image file which has the secret information embedded within it is delivered to receiver instead of secret information itself. It hides the existence of secret message, only the sender and receiver can suspect the existence of secret information. (Azmat U, Mohsin I, 2018).

Current usage

Currently this technique is used in various areas to ensure secrecy of the information. Apps have developed this technique in various areas. This encodes secret message into an image like that quality of cover image will not compromised and secret message is protected in cover image by assigning password on it and encoded image can be shifted to any communication medium i.e., the Gmail, WhatsApp, etc. there are other data hiding methods for various reasons and applications. These methods are cumulatively called as 'information hiding' techniques. Steganography, cryptography; watermarking and fingerprinting are techniques which are connected to each other as well. Steganography also named 'Covered Writing' conceals structure of concealed secret data to conceal object as against cryptography hides the data to restrict the attacker from comprehending the information. Steganography is utilized where cryptography cannot be allowed or utilized.

Steganography and cryptography are complementary to each other. These can be utilized in together offer higher level of safety. Watermarking is the method of embedding watermark signal into multimedia data to create watermarked data to save legitimacy of creator of digital object. It specifically highlights on the comprehensiveness of embedded message without hiding. As we cannot have increasing capacity and robustness simultaneously. Therefore, watermarking can be utilized for copyright safety and overall security. In fingerprinting, separate marks are embedded in the copies of the object that are offered to clients like concealed sequential figures which makes the intellectual property owner to recognize individuals who breach their license agreement and

provide the property to external parties. Steganography offers an ultimate assurance of recognition that no other security tool can assure. The basic objective of steganography techniques is to optimize embedding rate and reducing the detect capacity of the resulting Stego-images (PAWAN S. and others, 2018).

As per current research there are following method which have been used in image steganography:

LSB method: The LSB technique of data steganography reserves 8 pixels from the concealing image to hold one character from the secret message, every binary bit from message character is to be added in the minimum important bit of the related pixel of the concealing image

LSB2 method LSB2 method of data steganography likes LSB method, but it reserves 4 pixels from the concealing image to possess one character from the secret message, by this LSB2 method improves the ability twice. The utmost ability will be same to the given image size divided by 4.

PVD method Pixel value differencing (PVD) method uses 2 pixels from the covering image to conceal a set of bits from the secret message to be concealed in image. This method of data concealing begins with an initialization phase, in which we divide the pixels range value (0:255) into non-overlapping partitions (partitions are named lookup table, each partition has a lower and upper values, and each partition is related with number of bits from the message to be concealed)

Limitations in current usage

Most of applications are developed to only conceal text message into an image which must be less. But image must be less in size, not exceeding than few words. These applications don't conceal the image in cover image.

New in the field of Medical data transfer

Thousands of papers which are based on steganography are available today. Individual papers discuss with various algorithm to increase the security in transmission. In present time, as everything converting into digital form and thus there is an increased risk of data hacking. So, to resolve this problem, different processes have been discovered but they all could not resolve this problem completely. To remove the threat of data, Steganography can resolve this problem.

Steganography is the only method which can resolve this problem completely. However, this technique has not been explored much in the field of medical where data transfer is very frequent and data security becomes utmost important. However, there is hardly research papers which describe usage of image steganography in the field of medical.

IV. ALGORITHM

AES Encryption: -

Embedding Algorithm: -

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

Extracting Algorithm: -

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

V. METHODOLOGY

Methodology is classified into four major components namely User login, Encode, Decode and Database Connectivity.

A. User Login: -

In this, a user can login to the system using this Username and Password which would be assigned earlier only. While login it will assure whether the username and password matched or not. Only after the username and password match with each other the user will be able to utilize. Otherwise, the user has to crosscheck the correctness of password and username.

B. Encode: -

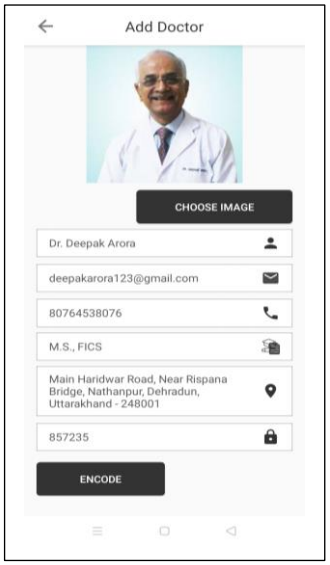
In this, the text in an image will be encoded by the sender. This will generate an array of integers which will possess the whole message in the structure of bit format. A message is composed up of characters. Every character is of the size of one byte which is 8 bits. Every byte here is divided into 4 parts of 2 bits, and saved in the two-bit message array. Hence, the size of a two-bit message is 4 times the length of the original message. It encodes 2 bits of message in 1 pixel while performing this. Basically, 4 pixels carrying 8 bits of encoded bits. In cumulative carry one character.

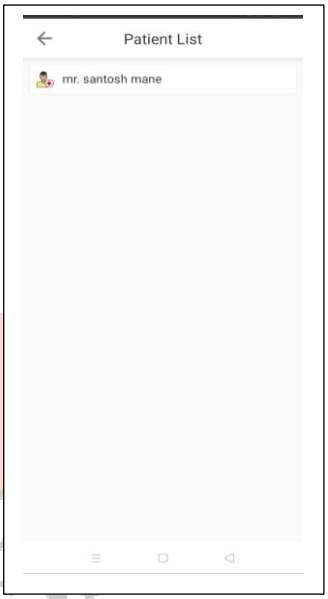
C. Decode: -

In this, the text from an image is decoded by the receiver. Take a RGB value at particular position and then extract 2 Least Significant Bits (LSB) from encoded data. Add the data in a queue for later processing. As, it acquires 8 bits of data, mixes it and prepares a byte and saves it as a character.

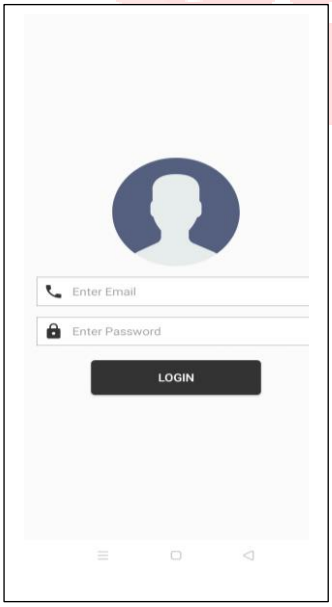
D. Database Connectivity: -

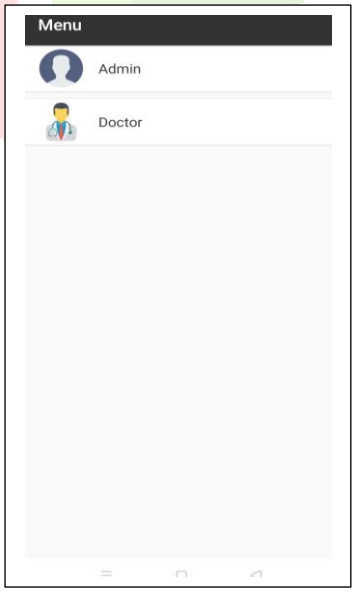
It connects to MySQL database; it saves Usernames and password in MySQL server. In login, the user enters the given username and password. Later the database will verify if it has any match in the database. After matching with each other it will offer access otherwise not.

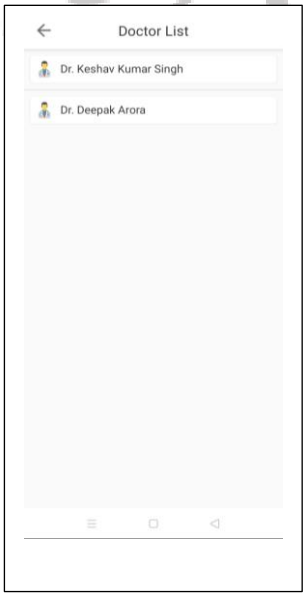


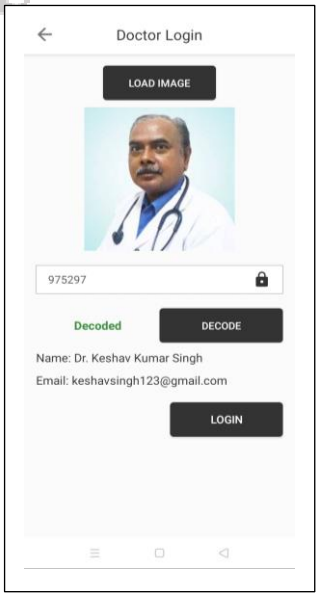


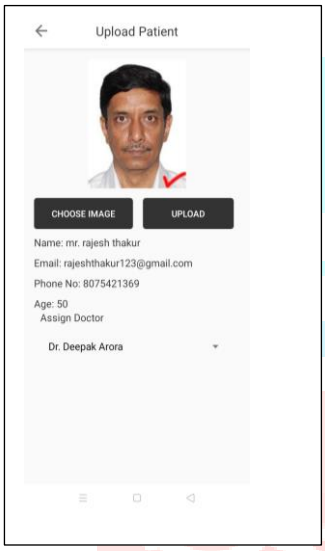
VI. RESULTS











VII. APPLICATION

This application can be used in hospitals, clinics to secure patients or hospital data. Steganography can be used in different areas of application like Defense, Software Development related data sharing, E banking, Online transaction - Confidential communication and confidential data saving. Protection of data alteration., in military applications to transfer highly confidential documents between international Governments.

VIII. CONCLUSION

In the current scenario where the health services sector is expanding. Easy and secure digital transfer of patient's details will transform the system. It will make the transfer of patients from one doctor to another within the same hospital or from one hospital to another quick as complete details will be instantly transferred without losing the confidentiality. This will ensure financial as well as health security of that patient.

As our project cover every minute details of patients like demographic details, illness history, current diagnosis, treatment, doctors who were operating the patient, their educational background, thus this can result in more efficient and time saving treatment to the patient in case of transfer. Also, as the detailed record will be available it will also work as ready reference. Thus, this project makes the health service efficient and effective to some extent.

ACKNOWLEDGMENT

We sincerely wish to thank our Project guide Prof. Diksha Bhave for her endless guidance, support to make our project a success. Our project guide made us confident to keep going in this journey with her expert guidance, inspiration and trust which helped us to successfully accomplish our project Hospital Database System Using Steganography and to keenly work on it in the right direction.

REFERENCES

[1] Savithri G, K L Sudha ,"Android Application for Secret Image Transmission and Reception Using Chaotic Steganography", International Journal of Innovative research in Computer and Communication engineering, 2014

[2] Rajashree Ghare, Pruthvi Bansode, sagar Bombale, Bilkis Chandargi, "LSB Steganography Using Android Phone", International Journal of Computer Sciences and Engineering, 2016

[3] Pawan Sharma, Srishant shetty, Om Kadam, Prof. Ritu Sharma, "Android Based Image Steganography", International Research Journal of Engineering and Technology, 2018

[4] Azmat Ullah, Mohsin Ijaz "Stego App Android based Image Steganography Application using LSB Algorithm", International Journal f, 2016

[5] "Using Color Image as a Stego-Media to Hide Short Secret MessagesRushadi Abu Zneit, Jam,il Al-Azeh; Ziad Alqadi, Belal Ayyoubu, Ahmad Sharadqh", International Journal of Computer Science and Mobile Computing, 2019