IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 6, PP 89-92

Secure Transfer of University Question Paper Using Image Steganography

Sanjeev Bhogan, Sai Kumawat, Ajay Chawla, Aditya Chaudhary,
Prof. Snigdha Bangal
(IT, Atharva College of Engineering/ Mumbai University, India)
(IT, Atharva College of Engineering/ Mumbai University, India)
(IT, Atharva College of Engineering/ Mumbai University, India
(IT, Atharva College of Engineering/ Mumbai University, India
(IT, Atharva College of Engineering/ Mumbai University, India)

Abstract: *This paper discusses on how the security of question paper delivery can be enhanced by image steganography. There are a lot of cases of university question paper leakage. Due to this, university has undergone various problems in order to tackle this event. The current system that the university uses for question paper transfer is based on face detection which is not very reliable and can be exploited. Moreover, this transfer process is not very secured and is a complex process, so we have developed our system to enhance the security of the transfer process.*

Keywords: *Face detection, Image Steganography, LSB embedding, Reliability, Question Paper*

I. Introduction

In recent years, Mumbai University has faced a problem regarding the security of question paper delivery to the colleges. To ensure the secure transfer of question paper to all the colleges, the University has implemented two methods in the past.

The University earlier used a simple method which comprised of a Licensed PDF Viewer. This PDF viewer software allowed the college authorities to view the question paper. No other PDF viewer was able to open the question paper file. The currently used method by the University is facial recognition. Four officials of a college are authorized to retrieve the question paper file from the dashboard of the University website. The IP address of the computer from where the question paper will be retrieved is authenticated with University. The facial recognition will only work if the authentication of IP is successful.

With the help of our system we are going to simplify the overall process and also making it more secured. The question paper file will be embedded into the image file such that there will be no visual changes in the output file. Now the sender and receiver only will know about the hidden question paper file into the steganograph image (output file). In this way, attackercannot detect the presence of the question paper and thus will not able to obtain it. Hence, the question paper will be transferred securely.

II. Literature Survey

This section shows various analysis and research made in the field of the Image Processing Technology. It also shows different methodologies being used by the existing system and the conclusion of this literature.

2.1 Steganography with LSB Encoding and DES Algorithm: In this paper, the author has implemented steganography using LSB embedding and DES algorithm. The secret data is embedded in an image file using LSB embedding technique. LSB embedding ensures that the original image does not get distorted from the original image. DES algorithm provides an additional layer of encryption to the password. In this way, the data stored will be more secured.

2.2 An Approach Towards Image, Audio and Video Steganography: In this paper the author proposes a methodology of image, audio and video steganography by converting the media type into a different form. In this paper they have devised the use of steganography in such a way that the video intended to be encoded is segmented into frames. Each frame of the video is considered to be a single RGB image. The frames are then converted into respective number of sound files. Later the steganographic files (sound files) are decrypted and combined in the original sequence to retrieve back the video using the reverse procedure. Again ordinary sound files containing speech and music were also tried to encode into a RGB image, which was later retrieved by running the decoding procedure.

We will be using both of the above mentioned techniques in our software. LSB embedding provides the 1st layer of security, and the embedded data is encrypted by DES algorithm which again a layer of encryption to the embedded data. Audio and Video steganography will also be used to make the process of transfer more challenging to crack. Therefore, we will be using both the techniques mentioned above.

2.3Licensed PDF Viewer: The university earlier used a Licensed PDF Viewer for viewing the question paper file. This PDF viewer software allowed the college authorities to view the question paper. No other PDF viewer was able to open the question paper file This PDF viewer software allowed the college authorities to view the question paper. No other PDF viewer was able to open the question paper file. The PDF Viewer used a license which allowed the installation of the software only on one computer of the college. The same license could not be used on any other computer. The major drawback of this method was if the authorized computer on which the software is installed crashes, then there is no other way that college can get retrieve the question paper securely.

2.4Facial Recognition: The currently used technique for securing the question paper transfer by the University is facial recognition. Four officials of a college are authorized to retrieve the question paper file from the dashboard of the University website. The IP address of the computer from where the question paper will be retrieved is authenticated with University. The facial recognition will only work if the authentication of IP is successful. But facial recognition is vulnerable and can be exploited. Varying lighting conditions, change in the facial appearance of the college officials may lead to failure of face recognition process and thus question paper retrieval will fail.

III. Methodologies Used

3.1LSB embedding: Least significant bit (LSB) insertion is a simple approach to embedding information in image file. The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human perceptible difference because the amplitude of the change is small. In this technique, the embedding capacity can be increased by using two or more least significant bits. At the same time, not only the risk of making the embedded message statistically detectable increase but also the image fidelity degrades. Hence a variable size LSB embedding schema is presented, in which the number of LSBs used for message embedding/extracting depends on the local characteristics of the pixel. The advantage of LSB- based method is easy to implement and high message pay-load.

3.2Encryption: The process of encrypting the password enhances the security of data. Moreover, it provides an additional challenge to the attacker. Thus, we have used DES algorithm to encrypt the password, so that the password can be made more secured. Data Encryption Standard algorithm is such a cryptographic key which is applied to a block of plain text to convert it into a cipher text and vice-versa. DES algorithm has a block size of 64 bits and key size of 58 bits. DES has small time of operation i.e. 16 rounds of operations. These characteristics make DES algorithm to be usable in a software. Without the password, one cannot extract the question paper hidden behind the image file.

IV. Flowcharts

1. Flowchart (File Embed Process)

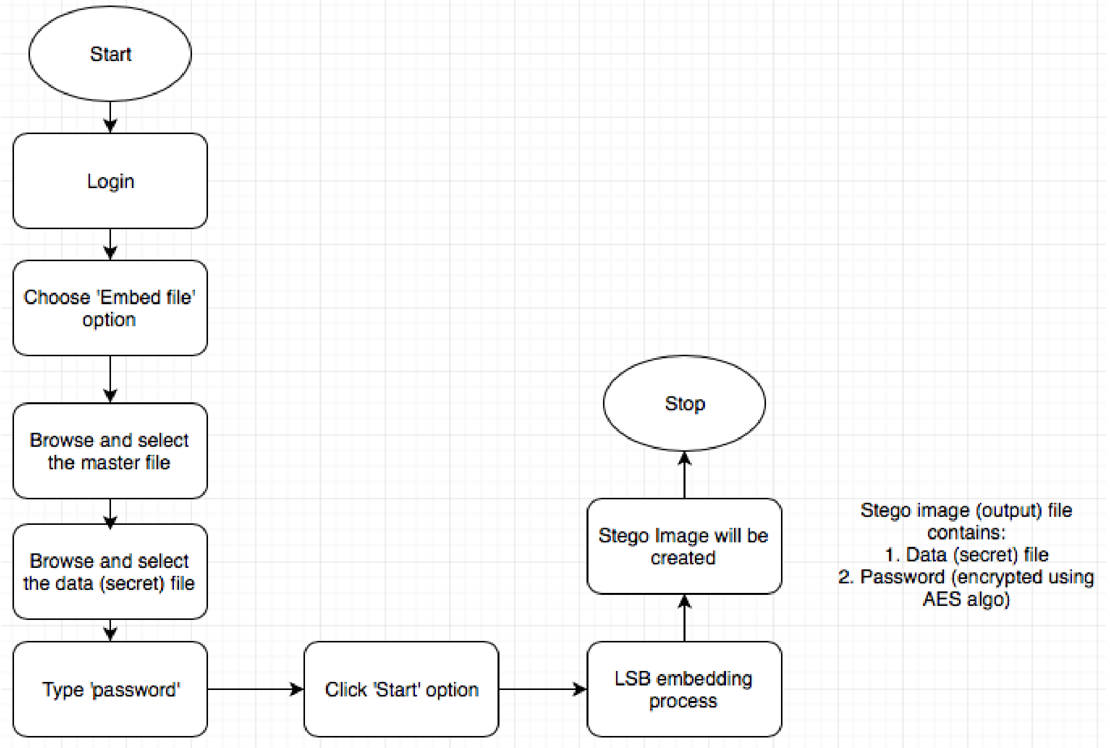
Start
Login
Choose 'Embed file' option
Browse and select the master file
Browse and select the data (secret) file
Type 'password'
Click 'Start' option
LSB embedding process
Stego Image will be created
Stop
Stego image (output) file contains:
1. Data (secret) file
2. Password (encrypted using AES algo)

Fig: File Embed Process

2. Flowchart (File Retrieve Process)

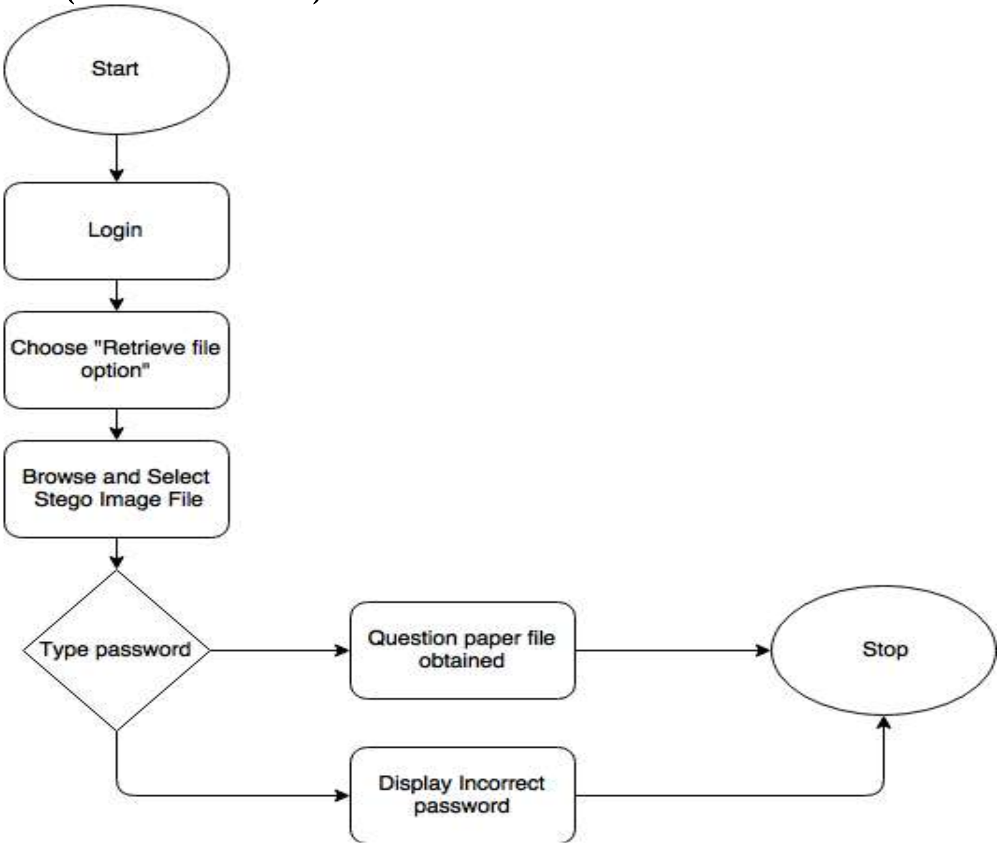
Start
Login
Choose "Retrieve file option"
Browse and Select Stego Image File
Type password
Question paper file obtained
Display Incorrect password
Stop

Fig: File Retrieve Process

V. Conclusion

The existing system uses the facial recognition technique which can be easily exploited and thus is not reliable. This system will be able to transfer the question paper (secret document) in a secured way so that the document cannot be intercepted by the attacker. It will be done by embedding the question paper and encrypting the password into the carrier image. The stego-image will appear similar to the original image so that theattacker cannot detect the presence of the secret document and thus confidentiality is ensured. Now, only the sender and receiver will be knowing that the stego-image contains the question paper. DES algorithm will be used to encrypt the password. This makes the process of the extraction of question paper from the stego-image more secured.

References

Journal Papers:

[1] A Combined Approach of Steganography with LSB Encoding technique and DES Algorithm, Prof. B.Karthikeyan, Prof. A.Deepak, *IEEE 2017*

[2] Research of Image Encryption Algorithm Based on S-DES, Linxain Zhi, *IEEE 2016*

[3] Lossless compression of high resolution disparity map images, Prof. Pekka Astola, Prof Ioan Tabus, *IEEE 2017*

[4] Effect of saturated pixels on security steganographic schemes for digital images, Prof. Vahid Sedighi and Prof. Jessica Fridrich, *IEEE 2017*

[5] An Approach Towards Image, Audio and Video Steganography, Prof. Kunal Hossain, Prof.Ranjan Parekh *IEEE 2016*

[6] Wu HT "Secure JPEG steganography by LSB matching and multi-brand embedding", *IEEE International conference on image processing, November 2014, Article number 6116235, Pages 2737-2740.*

[7] Gupta R "New proposed practice for secure image combining cryptography steganography and watermarking based on various parameters", International Conference on Contemporary Computing and Informatics , November 2014, *Article number 7019643, Pages 475-479 .*

[8] Baek J "(N, 1) secret sharing approach based on steganography with gray digital images", *IEEE International Conference on Wireless Communications, Networking and Information Security,2010, Article number 5541793,Pages 325-329.*

[9] Bajwa IS "A new perfect hashing based approach for secure steganograph", *6th International Conference on Digital Information Management" September 2011, Articlenumber6093325, Pages174-178.*

[10] Bouslimi D "Data hiding in encrypted images based on predefined watermark embedding before encryption process", MEDECOM, Plougastel Daoulas, France, *Volume 47, 1 September 2016, Pages 263-270.*

[11] Zhang W "Reversible data hiding in encrypted images by reversible image transformation", University of Science and Technology of China, Hefei, China, *Volume 18, Issue 8, August 2016, Article number 7470523, Pages 1469-1479.*

[12] Khodaei M "Adaptive Data Hiding, Using Pixel-Value- Differencing and LSB Substitution", Institute for Advanced Studies in Basic Sciences (IASBS), Zanjan, Iran, *14 August 2016, Pages 1-12.*

[13] Conci A "AES cryptography in color image steganography by genetic algorithms", 12th IEEE/ACS International Conference of Computer Systems and Applications, *Volume 2016-July, 7 July 2016, Article number 7507100*.

[14] Panda SS "A secure approach to spatial image Steganography" , VIT University, Vellore, India, Volume 8, Issue 2, June 2016, Pages 13384-13400.

[15] Nilizadeh A "A novel steganography method based on matrix pattern and LSB algorithms in RGB images" ,Dept. of Artificial Intelligence Engineering, University of Isfahan, Isfahan, Iran, *31 May 2016, Article number 7482107, Pages 154-159.*