I. J. Computer Network and Information Security, **2017, 9, 38-45**
Published Online September 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.09.05

Video Steganography: Secure Data Hiding Technique

Gat Pooja Rajkumar
M.Tech Student, Department of CSE, KLE Dr M S Sheshgiri College of Engineering & Technology,
Udyambag Belgavi, India
E-mail: poojagat9@gmail.com

Dr V. S. Malemath
Professor of CSE, KLE Dr. M S Sheshgiri College of Engineering & Technology
Udyambag Belgavi
E-mail: veeru_sm@yahoo.com

Received: 06 June 2017; Accepted: 01 August 2017; Published: 08 September 2017

***Abstract*—**Today, the security is getting the major attention due to the increased use of internet. As the use of internet is increased, the rate at which the data is exchanged per day is also increased. The data that is exchanged every day may become the victim of hackers. To deal with this problem one of the effective solution is the Steganography. The Steganography is a way to hide secret information behind an innocent cover file, such that the existence of information is not usually recognized. This paper uses the concept of video Steganography, where the data is hidden behind the frames of videos. This paper provides two level of security to the data i.e. Steganography and cryptography. First the data is encrypted using cryptography algorithm, next the encrypted data is embedded into frames of videos. The technique used to embed the data is LSB coding. It is the most common technique, but can hide large amount of data in most simplest and efficient way.

***Index Terms*—**Steganography, Cryptography, DES algorithm, LSB Coding.

I. INTRODUCTION

In today's world "Internet" is an important part of daily life. The rapid growth of internet makes the daily life much easier for human beings. Some examples which illustrate the use of internet are –the most used online shopping facility, online bill payment, online money transactions, booking online tickets, online recharge etc. The other part of facility which mostly affected the human lives is social networking sites like facebook, twitter, instagram, what's app etc. Due to this facility the peoples are sharing their important information, documents with the other person. People share their private and secret data with the other person through the internet. Transferring private data through internet may become a victim of hackers. So security is utmost important while sending the data through internet. The solution to this problem is "Cryptography" and "Steganography". The proposed system uses the combination of both Cryptography and Steganography for hiding the secret data behind the video clips. Therefore this system provides double security.

The secret data is first encrypted and then the encrypted data is hidden behind the frames of video. Cryptography is a technique which jumbles the secret information using encryption algorithms so that nobody can understand it. Using the key which is known only to sender and receiver the sender encrypts the data and sends it to the destination, where the receiver decrypts the data using the same key.

A. Steganography

Steganography is a sub-category of Anti-Forensic technique which is used to hide the secret information behind the cover medium. Steganography is a most commonly used technique to hide the data. The cover medium can be audio, video, image or text. In the proposed work video is used as cover medium to hide the secret data. In cryptography the any one can easily detect the existence of secret data behind jumbled word but in Steganography the existence of secret data is completely hidden behind innocent medium. No one can easily detect that secret information is hidden behind the video. Once the data is hidden behind the video we can see that there is change in the size of original video and encrypted video.

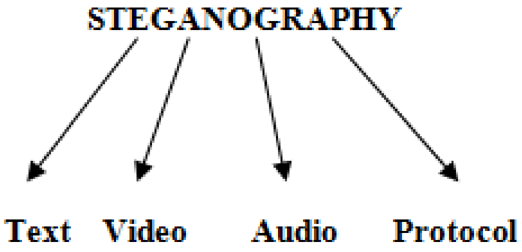


Fig.1. Types of Steganography

The figure shows the types of steganography. There are 5 types behind which we can hide our secret data. Hiding the data behind protocols means we can hide data behind the OSI layer. Hiding the data behind the video is same as hiding data behind the image. In proposed system video is used as cover media, where the video is divided into frames/images to hide the secret data. Next the secret information may be in text format or document is chosen to hide behind video. The proposed system uses the DES encryption algorithm to encrypt data. For embedding the encrypted data behind video the LSB technique is used. This outputs the stego media. It is the encrypted video behind which the data is hidden.

II. Literature Survey

The paper [1] implements the Audio-Steganography in which the data is hidden into another medium such as audio file. In Audio-Steganography we can hide the message in MP3 like sound files. The process of hiding the data behind the audio file is more complicated as compared to other steganography types or mediums. This paper deals with different types of audio steganographic methods with the advantages and disadvantages. First One is LSB coding, which is most commonly used and simplest technique but more efficient in providing security. Second is Phase coding which has disadvantage of low data transmission rate. Third one is spread spectrum in which the noise is introduced in the process of hiding data behind audio files.

The [2] paper introduces a new system called Steganography Imaging System (SIS).The two levels of security is provided in the proposed system. In this system cryptography is not used for first level of security instead Username and password is used to provide the login security. Here the secret key is used only to retrieve secret message from the image not for the encrypting purpose. In the proposed system, first the secret message is transferred to text file. Then the text file is compressed to zip file. At the next level the zip file is converted into binary codes to embed the message into image. The purpose of using zip file is that zip file is more secure than the normal text file.

Khosala et. al [3] paper is a combination of Video Steganography and Digital Watermarking which provides strong backbone for its security. This paper presents a new algorithm which is used for better security and transferring of data efficiently from source and destination. This paper uses the concept of Digital watermarking along with steganography. In digital watermarking the digital signal or pattern is inserted into digital content. This process can be used on any of the steganography types either audio, image or text. In this process first the secret data is converted into binary form. Then the LSB technique is applied to replace the least bit of cover image pixel with the binary bit. After applying LSB we get the stego image. Now the combined DWT and DCT technique is applied on stego image to get watermarked image. The watermarked image is then securely transferred to the destination.

This paper [4] deals with hiding the image as secret information behind the frames of video. Along with the LSB approach, the Masking-Filtering techniques are used to hide the secret image in frame. In this paper first the video is converted into frames and stored in the separate file. Only one frame is used to hide the input image. The Masking and Filtering techniques are generally used to conduct the analysis of the image. The Significant areas are selected to embed the secret image to provide more security. These two techniques are usually applied to only 24 bit and gray scale images. To embed the message into the video clips a key is used called the stego key.

[5] In this paper the first step is to encrypt the data. For encryption process of data, the most popular technique called the AES algorithm is used. Along with the AES algorithm pixel swapping technique is also used to embed message in video. In the pixel swapping technique randomly one frame is selected, after selecting the frame separate the Red, Green, Blue channel of that frame. Next for data hiding the particular channel is selected, in this case the paper makes use of blue channel. For every selected frame, the pixel positions of blue channel are swapped with the use of key. Encrypt the message using AES algorithm. Embed this encrypted message into the pixels to enhance the double level security. The concept of PSNR value calculation is used in this paper to compare the original and stego image. PSNR is Peak Signal-to-Noise Ratio. Both the PSNR values are compared, if we get the more value in the stego image, then we can say the proposed system is secured.

[6] the most common steganographic technique is Least Significant Bit (LSB).The above paper deals with the advanced LSB technique to hide data into images. In the common technique the least bits of the image is changed with the message bit but in this advanced technique it is suggested that the message bits are randomly inserted in the image. This advanced LSB technique is introduced in order to provide better security to system. In this advanced LSB technique the message bits are inserted into image, not only in the least bit of but also in the other bits in the random manner. In this process the message bit and the pixel bit randomly chosen is compared. If the message bit and pixel bit are identical then 1 is inserted into least significant bit otherwise 0 is inserted if the message bit is not identical with image bit. This paper compares the stego image and original image with the two techniques Mean-Squared Error (MSE) and Peak Signal-to-Noise Ratio. In the case of MSE measurement the value must be as less as possible. If it is 0 means that there is no change in original image and encrypted image.

III. Methodology

Initially the project is implemented with MATLAB tool of version 2015.The MATLAB tool is also used to design the user interface of this project. For the internal computation of the project two algorithms are used. One is the DES algorithm to encrypt the secret data and also for decryption at the receiver side. Second is the LSB

(Least Significant Bit) algorithm is used to hide the secret data behind the frames of videos. Next is the function “audioread” of MATLAB. This function is used to read the audio file separate from the video file.

A. *DES Algorithm*

The DES algorithm is Symmetric key algorithm, where only one private key is used to encrypt the data. The DES is most commonly used algorithm for encryption and decryption. The reason behind using the DES algorithm is that, it is faster and more efficient algorithm as compared to others. Because it takes less time to compute encryption, as it has 16 rounds of iterations. Each iteration performs different operations. The operations performed are the bit shuffling, non-linear substitutions (S-box) and exclusive-OR operation. Substitution and Permutation are the two important operations in the DES algorithm. Substitution maps the different value to each other and in permutation the bit positions are reordered so that we can get the permuted input. This techniques are used many number of times in each iterations. The DES encryption algorithm accepts 2 inputs-

1. Plain text to be encrypted.
2. Secret key.

The DES algorithm accepts the plain text of 64-bit block. The 54-bit block is taken as input and the 64-bit block of cipher text is produced as output. The second input to DES is the secret key. The same secret key is used at both the sender and receiver side. The key length is usually of 64-bit length. Every eighth bit of total key length is ignored, because it is used for the parity checking.

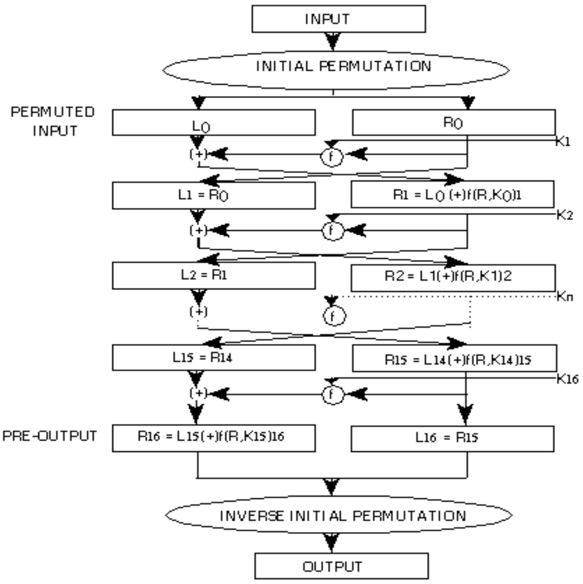


Fig.2. DES Algorithm

The process starts with the initial permutation; it simply rearranges the bits to form permuted input. After initial permutation the input is divided into 2 halves of 32 bits each. As seen in the figure the function f is performed in all the iterations.

$$L_i=R_{i-1} \tag{1}$$

$$R_i=L_{i-1} \quad f\bigoplus\{R_{i-1,}K_i\} \tag{2}$$

The function F is the fiestel function which performs the various functions.

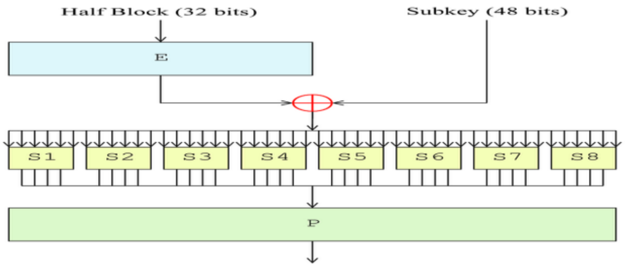


Fig.3. Fiestel Function (F)

As shown in above figure it first expands the right half of input from 32 to 48 bit similar to the length of key i.e. 48-bit.The XOR operation is performed between the key and right half of input. The output of XOR operation is 48-bit, which is input to s-boxes. The S-box takes input of 6-bits and provides 4-bit output. And total 32-bit is output from 8 S-boxes. This output is permuted using the P-box. This is the complete process of 1 round. After all rounds the left and right halves are not exchanged instead it is concatenated. And the result is the encrypted data. Along with the encryption process 48-bit key is also transformed. At each round different combinations of 48-bit sub keys are generated using circular shift. The decryption process is similar to encryption process, the only difference is that the key must be used in reverse order and instead of left shift it uses right shift to generate the sub keys.

There are many cryptography algorithms available for encryption and decryption. First the symmetric cryptography is used because it consists of only 1 secret key, so it is easy to implement. In other case i.e. asymmetric cryptography it consist two keys private and public key, so it is difficult and time consuming process to encrypt the data compared to symmetric. In symmetric, the reason of using the DES algorithms is, DES is less time consuming compared to AES.

B. *LSB Coding*

This paper work uses the most common technique for embedding the message into the frames. This technique is known as the LSB (Least Significant Bit). In the embedding process the least bits of the pixel of the frames are changed with the 1-bit of secret data. It is the simplest but faster technique to hide the data behind video. It is the common way to embed the data into video clips as well as it is more efficient for embedding. Using this technique, we can embed the secret data into the least bits of the pixels of frame. In this embedding process we can embed the 3-bits of message into the pixels. Each RGB component hides 1 bit of data. For this reason we have used Bitmap (BMP) image.

Example-

Following pixels are of 24-bit image –

(00101110 00001110 11001101)
(00011101 10101101 00001100)
(11101111 10100000 11000011)

Further take the character to hide it in the pixels of image given above. For example consider character ‘b’. This character is first converted into the ASCII value. The character ‘b’ has ASCII value 98. Now take the binary value of this ASCII value, so that we can embed the character into pixel. The binary value is 1100010.

(0010111**1** 0000111**1** 1100110**0**)
(0001110**0** 1010110**0** 0000110**1**)
(1110111**0** 10100000 11000011)

As shown in example only 1 bit change in each pixel is not recognizable.

The LSB coding is the common and simplest technique. The reason behind using this simple technique is that, though it is simple it provides fast embedding process and even the data is extracted at receiver side in proper way. It is easy to implement and provides the better security.

C. *Audioread Function*

audioread provides a single, unified MATLAB function for reading audio files in a range of different file formats, including wav, mp3, avi etc.

Syntax-

1. [y, Fs] = audioread(filename)

This syntax reads data from file named filename and returns the sample data y and a sample rate for that data Fs.

2. [y, Fs] = audioread(filename , samples)

Reads the selected range of audio samples in the file, where samples is a vector of the form [start, finish].

3. [y, Fs] = audioread(___, datatype)

Returns sampled data in the data range corresponding to the datatype of ‘native’ or ‘double’, and can include any of the input arguments in previous syntaxes.

IV. System Architecture

The System Architecture describes the overall procedure of the concept implemented in this paper. The Fig.4 shows the various algorithms and techniques used in this implementation.

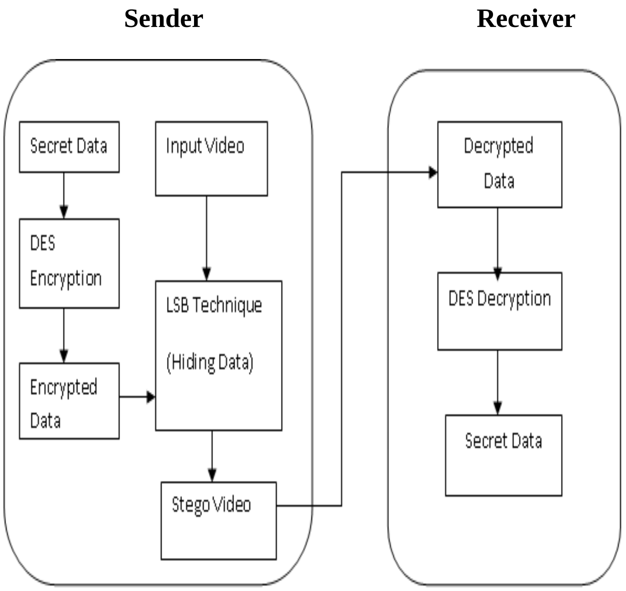


Fig.4. System Architecture

First the system accepts the input from user that is the cover file to hide the data behind. Cover file can be text, audio or video. Here the project is implemented with accepting video as cover file. Next the system gets the secret data from user to hide behind the frames. The system also accepts the document as secret data. The secret data can also be image, but processing the image and hiding behind image is critical process so this project is implemented with secret data as text.

The DES encryption is performed on the input secret data. The DES encryption contains 16 rounds process. The DES accepts the secret key as input from user, which can be of any length. It is like a password to provide security to the data. The same key must be known to the receiver to decrypt the data. After 16 rounds of process we get the encrypted data as output. At the next step the encrypted data and the cover video is provided as input to the embedding process. The LSB technique is used for embedding the secret data into the video. The “audioread” function is used to read the audio file. In the first frame of video the total bits of secret message is stored .And from the second frame, each frame contains 1 bit of message. Likewise the whole secret message is stored in the entire video. This process provides the output as stego video, which contains the encrypted data hidden behind frames.

At the receiver side the stego video is provided as input. Using the same LSB technique, we can retrieve the encrypted data from the video. As the first frame contains the number of bits the message has, so only that much amount of frames is processed to retrieve the data. The Output of this process is the encrypted data. The DES decryption is performed on the decrypted data to get the original secret data. It contains the same 16 rounds of iteration. The output produced is the original secret data.

In the existing system the data is hidden behind only one frame, the frame number is accepted as input from user. So the disadvantage of existing system is that, as the message is hidden behind only one frame, it may introduce some noise in the video. Where as in proposed system the 3-bits of message are hidden behind the 1 frame, likewise the whole message is embedded in the entire video. Only 1 bit of change behind a single frame does not affect to whole video. The advantage of proposed system is that, always the first frame hides the total number of bits the message contains. So that from first frame we can get the number of frames in which the message is hidden.

V. Experimental Result

The result of this paper is analyzed with different videos as input. This result provides the double security to any given input. First level security is provided through encrypting the secret information and second level security is provided through Steganography. The Steganography hides secret information behind the innocent cover media.

There are different algorithms for implementing the encryption of secret data. The one used in this paper is DES encryption algorithm. The reason behind using the DES algorithm is, it is the simplest and fastest algorithm for encryption of data. The secret data is encrypted using the 16 rounds of encryption techniques. These 16 rounds contain P-box, S-box, E-box of operations. Along with this 16 rounds of encryption the 16 round of key substitution is also performed, which provides 16 different subkeys at each step. These subkeys provide better security for encrypting data. Secret key is the important part of the encryption. Receiver decrypts the secret information using the same secret key provided by sender. A single bit change in the secret key may retrieve the wrong information. At the next level the encrypted data is hidden behind the cover media. The cover media may be audio, video, text, and protocol. This paper is implemented with the video as the cover media.

The result of this paper is that the sender can send his secret message to the receiver, by hiding the message behind the video. There are 3 inputs that we have to accept from user. First is the cover media that is video. The video can be of any size and format of video specified is ".mp4". if the video size is less we can get the fast results. The second input is the secret key, which is private and known only to sender and receiver. The key can be of any length, but smaller key length provides more accurate results. Third input is the secret data to hide. The secret data can be provided as text or select the text file as document to hide. The other options provided are encryption of secret data, after the encryption we can also view the encrypted data in the notepad which is saved in "tempoutput". Once the encryption is done, the data is hidden behind the video. And we can play the encrypted video as shown in the below figure. The encrypted video is saved as output video, so that at the receiver side we can select the same video. At decryption section first the hidden data is retrieved and then DES decryption is performed on the data and final original data is printed. This all options are designed in the user interface. The user interface is designed using the MATLAB tool. This is the design of paper work and the results of this work are shown below.

The user interface of this work is shown in below figure-

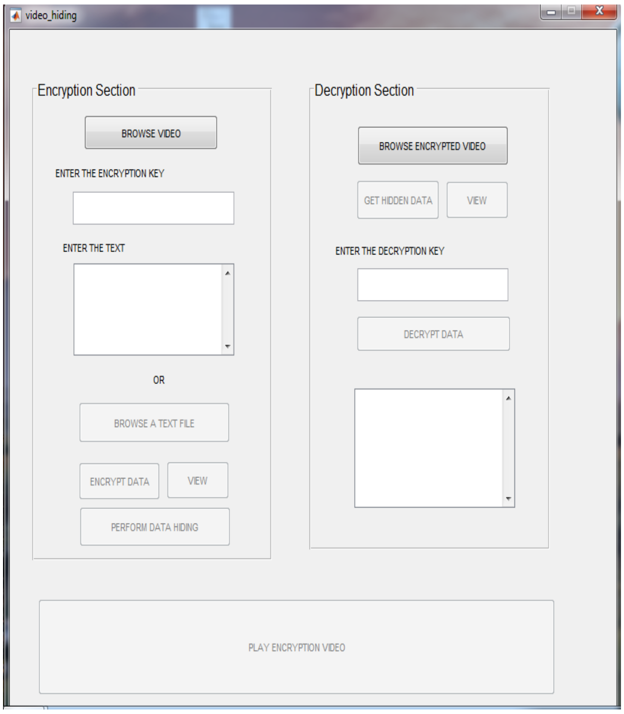
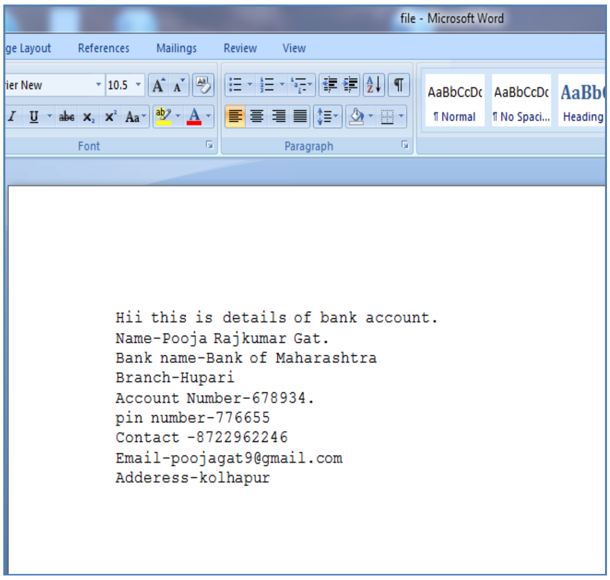


Fig.5. Front User Interface

As shown in the interface until the input video is not selected all the other buttons are disabled. After the video is selected, it accepts the secret key from user to encrypt the data and all other keys are enabled. One validation is provided at encryption side that is, if key is not provided it will display "Please provide encryption key".

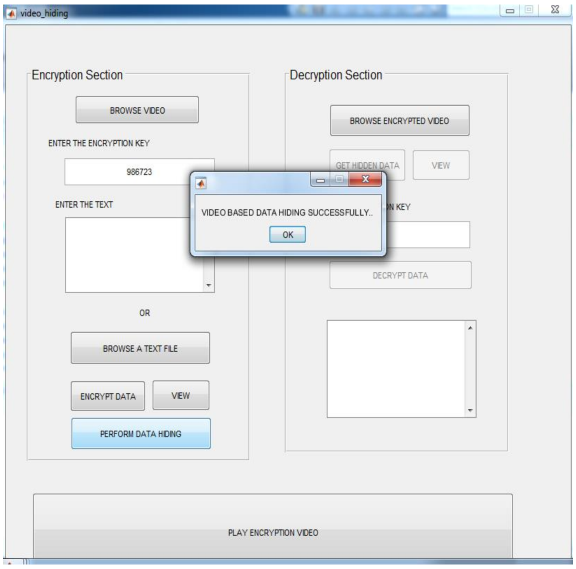
The below figure shows the result, where document is selected as secret data, which contains the bank details of customer. The document is named as "file.txt" as shown in figure-



```
Hii this is details of bank account.
Name-Pooja Rajkumar Gat.
Bank name-Bank of Maharashtra
Branch-Hupari
Account Number-678934.
pin number-776655
Contact -8722962246
Email-poojagat9@gmail.com
Adderess-kolhapur
```

Fig.6. Input Secret Document

For example the document which contains the bank details of the customer is to transfer across the internet to the receiver. The details of customer include name, account number, branch name, pin number, contact information etc. This data is important and may be hacked by the unauthorized user. So providing security is important in this case. The file is saved with the name “file.txt”. This file is hidden behind the video selected. All the above secret information is first encrypted. The secret key is also provided. The Fig. 7 shows the encryption side process, where first the video is selected. After selecting video secret key is entered. And third input i.e. document is selected to hide. The selected document is shown in Fig.6. After performing data hiding the message is displayed. Before displaying the message of success the whole procedure of embedding the secret information behind the video is carried out. The LSB Coding technique is used to implement the embedding process. As discussed above the LSB technique replace the least significant bit of the pixel. As we know video is collection of frames/images. This process first separates the audio and video segment. Next it calculates the number of frames in the videos. After it replace the least significant bits of the image pixels with the secret information bit. First frame always stores the total number of bits the secret information contains. After storing secret information the audio is divided across all the video. This whole process generates a new video called the encrypted video. This video now contains the secret data. After this process the message is displayed “VIDEO BASED DATA HIDING SUCCESSFULLY”. The sender can send the video to the receiver.

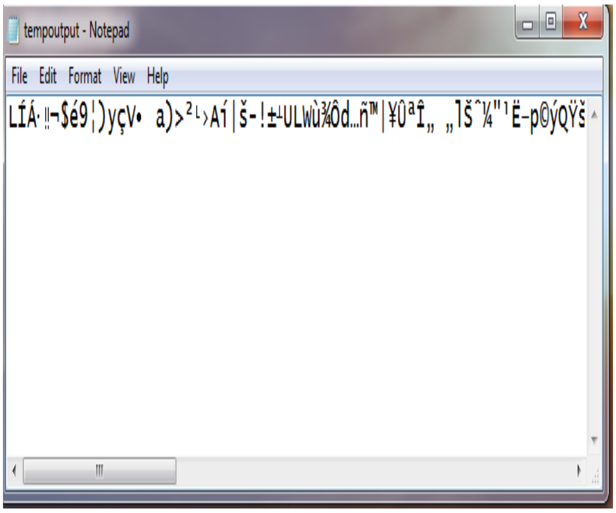


986723

VIDEO BASED DATA HIDING SUCCESSFULLY..

Fig.7. Encryption section

The data selected to hide is the customer bank details. This data is encrypted using DES algorithm. After the encryption process we can also view the encrypted data in notepad as shown in the fig.8. As shown in the figure the customer details are encrypted. This data is now hidden behind the video. In this DES encryption process first two bits are taken as input from the secret data. This two bit goes through all 16 rounds and produces encrypted data. In same this process is carried out for whole document and produce the encrypted data.



```
LÍÁ·‼¬$é9¦)yçV•  a)>²└›Aí|š-!±┴ULwù¾Ôd…ñ™|¥Ûªΐ„ „Ïš˜¼"¹Ë-p©ýQŸš
```

Fig.8. Encrypted data

After the data is hidden we can play the encrypted video. As we can see that there is no change in the encrypted video and the original video. It is impossible to detect that the text data is hidden behind the video. For hiding data behind the video we used the LSB technique. Behind each pixel of video 3 bit of secret data is hidden. For hiding data the Least Significant bits of pixels are modified with the secret information bits. One bit change in the pixel does not affect the quality of video. The one difference we can mention is that the size of video is changed. After hiding the data behind video the size of video is increased. The above video is encrypted video which contain the secret information of customer bank details. As shown in below fig-

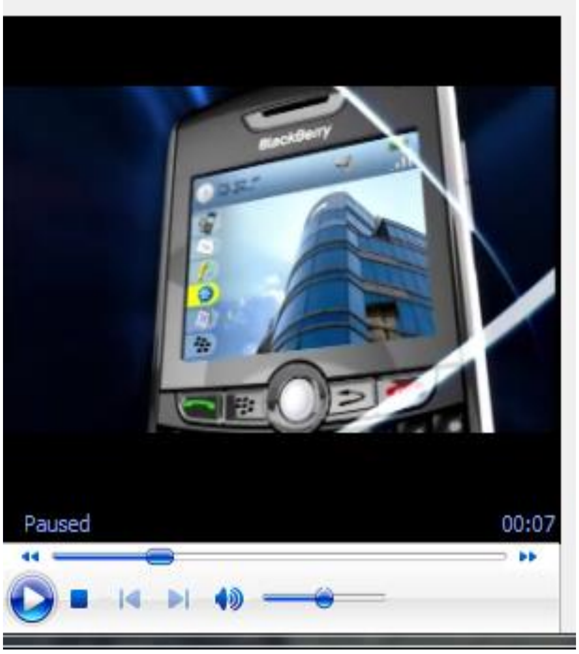
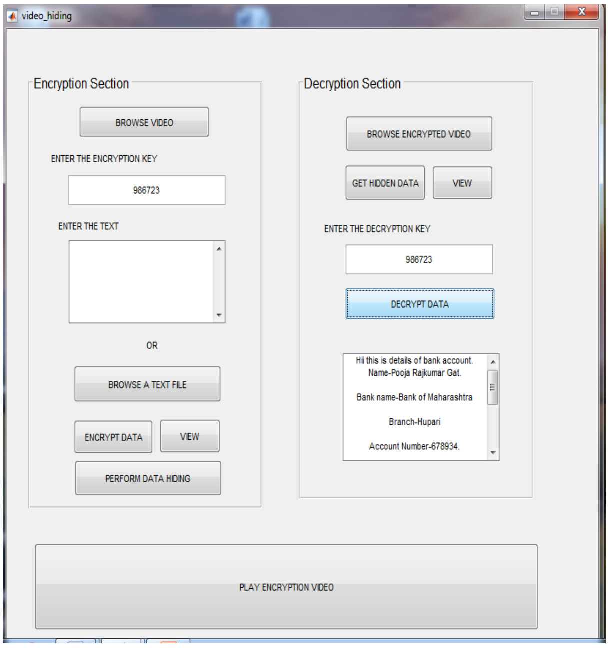


Fig.9. Encrypted Video

The encrypted video is input at the decryption side. At the decryption section first the hidden data is fetched. The same secret key is provided as provided at encryption. After clicking the “DECRYPT DATA” button we can get the original data back as shown in below fig-



ENTER THE ENCRYPTION KEY: 986723

ENTER THE TEXT

ENTER THE DECRYPTION KEY: 986723

Hii this is details of bank account.
Name-Pooja Rajkumar Gat.

Bank name-Bank of Maharashtra

Branch-Hupari

Account Number-678934.

Fig.10. Decryption side

The fig.10 shows the decryption side process. This process retrieves the hidden data from the video. It first retrieves the encrypted data from the video and next decrypts the data using the DES decryption algorithm. As we can see in the fig.10 the customer bank details is retrieved from the video. Encrypted video is input to this process.

The motivation behind the concept implemented in this paper is security. Security to the important data transmitted is major concern now days. As data transmission rate is increased, security must be provided to these data transmitted. With the use of the concept implemented in this paper we can provide a better security to the every important document. Sender can securely transfer the data to the receiver.

VI. Conclusion

The proposed video Steganography system provides two level of security, first with cryptography and second with Steganography. The proposed system results in hiding the encrypted information into the video clips. Each frame hides 3-bits of data. The proposed video Steganography is tested by taking different size of videos and different size of secret data. The proposed system shows that no noticeable noise is introduced in the encrypted video. It is similar to that of original video. The stego video is sent to the receiver, who knows the secret key. The existence of secret information is impossible to detect. Hence the data is transferred safely and securely to the destination. The DES algorithm used to encrypt data is simplest but efficient algorithm for encryption. Although it is simple and most common techniques are used, but it provides fast and efficient way to transfer data securely.

References

[1] Chhaya Varade, Danish Shaikh, Girish Gund, Vishal Kumar, Shahrukh Qureshi “A Technique for Data Hiding using Audio and Video Steganography”, International Journal of advanced Reseach in Computer Science and Software Engineering, Volume 6, Issue 2, February 2016.

[2] Rosziati Ibrahim and Teoh Suk Kuan “Steganography algorithm to hide secret message inside an image”, Computer Technology and Application 2 (2011) 102-108.

[3] Shivani Khosla, Paramjeet Kaur “Secure Data Hiding Technique using Video Steganography and Watermarking”, International Journal of Computer Applications (0975 – 8887) Volume 95– No.20, June 2014.

[4] K. Steffy Jenifer, G. Yogaraj, K. Rajalakshmi “LSB Approach for Video Steganography to Embed Images”, International Journal of Computer Science and Information Technologies, Vol. 5 (1), 2014, 319-322.

[5] Miss. Uma Sahu, Mr. Saurabh Mitra “A Secure Data Hiding Technique Using Video Steganography”, International Journal of Computer Science & Communication Networks, Vol 5(5), 348-357.

[6] Obaida Mohammad Awad Al-Hazaimeh “Hiding Data in Images Using New Random Technique”, International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012.

[7] Hsien-Chu Wu, Na-I Wu, Chwei-Shyong Tsai, Min-Shiang Hwang “An Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacements Methods”.

[8] K.Saranya, Dr.C.Suresh Gnanadhas, Minu George “Data Embedding Techniques in Steganography”, International Journal of Latest Trends in Engineering and Technology”, Volume.3 Issue2 November 2013.

[9] Amritpal Singh, Satinder Jeet Singh “An Overview of Image Steganography Techniques”, International Journal of Engineering and Computer Science, Volume 3, Issue7 July 2014.

[10] Syeda Musfia Nasreen, Gaurav Jalewal, Saurabh Sutradhar “A Study on Video Steganographic Techniques”, Internatinal Journal of Computational Engineering Research Volume 05, Issue 10, October 2015.

[11] Shikha, Vidhu Kiran Dutt “Text Steganography”, International Journal of Advanced Research in computer science and Software engineering, Volume 4, Issue 10,October 2014.

[12] D.Nithya Kalyani, Dr. K.Mahesh “Safe Information Hiding Using Video Steganography”, International Journal of Computer Science and Mobile Computing, Volume 4, Issue 7, July 2015.

[13] Satwant Singh, Proff. Lekha Bhambhu “Simple Steganography Technique for hiding Data into Image”, International Journal of Computer Science Trends and Technology, Volume 2, Issue 6, December 2014.

[14] Abhilasha Ramdas Bhagat, A. Prof. Ashish B Dhembhare “An Efficient and Secure Data Hiding Technique-Steganography”, International Journal of Innovative Reasearch in Computer and Communication Engineering, Volume 3, Issue 2, February 2015.

[15] Kaumal Kaushik, Suman “An Innovative Approach for Video Steganography”, International Journal of Computer

Network and Information Security, Volume 7, No 11, October 2015.

[16] Ali M. Meligy, Mohammed M. Nasef, Fatma T. Eid "An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Keys", IJCNIS Vol. 7, No. 7, June 2015.

Authors' Profiles

Pooja Rajkumar Gat completed Diploma degree in Computer Science and engineering from Dr. J.J. Magdum Polytechnic, Jaysingpur in 2011. Received B.E degree in Computer Science and engineering under Visvesvaraya Technological University of Belgaum in 2015. Currently pursuing her M.Tech degree in KLE Dr. M.S Sheshgiri College of engineering and technology Belgaum. Her research interests include Computer Network and Information Security.

Dr. Virendra. S. Malemath is Professor in Department of Computer Science & Engineering, KLE DR M S Sheshgiri College of Engineering & Technology, Belgaum. He did his Bachelors in Engineering in Electronics & Communication Engineering from Karnataka University, Dharwad in the year 1993, did his MS in Software Systems from BITS Pilani Rajasthan in 1998 and received his PhD in Computer Science from Gulbarga University, Gulbarga, India in 2009. His research interests are document image processing, pattern recognition and Network Security. He has published more than 70 articles in peer reviewed international journals and conferences.

How to cite this paper: Gat Pooja Rajkumar, V. S. Malemath,"Video Steganography: Secure Data Hiding Technique", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.9, pp.38-45, 2017.DOI: 10.5815/ijcnis.2017.09.05