International Journal of Science, Engineering and Technology
An Open Access Journal

Multimedia Data Hiding in Video Using Selective Bit Technique

[1]Harshitha H. P, [2]Navya R Kumar, [3]Sindhu N, [4]Uthpala S, [5]Darshan K R

Abstract

In our work the message/text file, audio, image or document is taken as an input from the user which needs to get embedded in the Video file. The Video file can be of the extensions .avi, .flv, .wmv or .rm. The message/text file, audio, image or document has to be selected to embed in the video file. The message digest is calculated using the MD5 algorithm and this is appended with the message/text file, audio, image or document. The appended message is then encrypted using the DES, Triple DES, RSA algorithm. The appended encrypted message is embedded in the video using the selective bit algorithm. The encoded message/text file, audio, image or document is transmitted. The password has to be given before transmitting. At the receivers side the watermarked Video file is taken as the input. The message in the text file, audio, image or document is extracted using those algorithms.

Keywords—Video Steganography, Selective Bit Algorithm, DES Algorithm, Triple DES Algorithm.

Introduction

Steganography is the technique of encrypting a file, message, image, or video within another file, message, image, or video. It is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word steganography is of Greek origin and means concealed writing. Generally, messages will appear to be something else: images, articles, shopping lists, or some other cover text and, classically, the hidden message may be in invisible ink between the visible lines of a private letter. The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Steganography includes the concealment of information within computer files.

Video steganography is a technique to hide any kind of files or information into digital video format. Video is used as carrier for hidden information. When information is hidden inside video the program or person hiding the information will usually use the DCT (Discrete Cosine Transform) method.DCT works by slightly changing the each of the images in the video, only so much though so it isn't noticeable by the human eye. To be more precise about how DCT works, DCT alters values of certain parts of the images, it usually rounds them up. For example if part of an image has a value of 6.667 it will round it up to 7. Steganography in Videos is similar to that of Steganography in Images, apart from information is hidden in each frame of video. The data to be hidden which is any multimedia file is taken as input from the user, which is encrypted and embedded in the video using Selective Bit algorithm. On the receiver's end if the password matches, the hidden file can be extracted from the video.

We propose a system where the user is enabled to secure his data by embedding it onto a video. The message digest is calculated using the MD5 algorithm and this is appended with the data file. Further the security is added by encrypting the data by a choice of three algorithms that is DES, triple DES and RSA algorithm. The embedding of data onto to the video is done using selective bit algorithm. At the receiver's end the message digest is recalculated to check for the authentication of the original message. The user can dynamically change the password which further enhances the security.

Literature Survey

Md.Rashedul Islam [1] proposes an efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography. In Steganography, the total message will be invisible into a cover media such as text, audio, video, and image in which attackers don't have any idea about the original message that the media contain and which algorithm use to embed or extract it. In this paper, the proposed technique has focused on Bitmap image as it is uncompressed and convenient than any other image format to implement LSB Steganography method. For better security AES cryptography technique has also been used in the proposed method before Steganography technique, AES cryptography will change the secret message into cipher text to ensure two layer security of the message.

In the proposed technique, a new Steganography technique is being developed to hide large data in Bitmap image using filtering based algorithm, which uses MSB bits for filtering purpose. This method uses the concept of status checking for insertion and retrieval of message. This method is an improvement of Least Significant Bit (LSB) method for hiding information in images.

Rig Das, et.al [2] proposes a novel steganography method for image based on Huffman Encoding. Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. This paper presents a novel technique for image steganography based on Huffman Encoding. Two 8 bit gray level image of size M X N and P X Q are used as cover image and secret image respectively. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of the Huffman encoded bit stream and Huffman Table are also embedded inside the cover image, so that the Stego-Image becomes standalone information to the receiver.

Ramaiya M.K, et.al [3] Improvisation of Security Aspect in Steganography Applying DES The unbelievable evolution of Internet technologies & its applications need very high level the security of data during transmission over the unsafe communication network. Image steganography is a technique for hiding information into a cover image. Least Significant-Bit (LSB) based approach is most common steganographic technique in spatial domain due to its easiness and hiding capacity. All of existing methods of steganography focus on the embedding strategy with less concern to the pre-processing, such as encryption of secrete image. The conventional algorithm does not provide the preprocessing required in image based steganography for better security, as they do not offer flexibility, robustness and high level of security. The proposed work presents a unique technique for Image steganography based on the Data Encryption Standard (DES) using 64 bit block size of plaintext & 56 bits of Secrete key. The preprocessing provide high level of security as extraction of image is not possible without the knowledge of mapping rules of S -Box and secrete key of the function.

Kumar, et.al [4] proposes Enhanced LSB technique for audio steganography. The idea of this paper is to invent a new strategy in Steganography to get the minimum effect in audio which is used to hide data into it. "Progress always involves risk" Fredrick Wilcox observed that technological progress of computer science and the Internet altered the way we lived, and will continue to cast our life. In this paper we have presented a Steganography method of embedding text data in an audio file. The basic approach behind this paper is to provide a good, well-organized method for hiding the data and sent to the destination in safer manner. In the proposed technique first the audio file is sampled and then appropriate bit is modified. In selected sample one bit is modified at least significant bit .The remaining bits may be used but it may be cause noise. We have attempted to provide an overview, theoretical framework about audio Steganography techniques and a novel approach to hide data in an audio using least significant bit (LSB).

Methodology

We use DES, triple DES and RSA algorithms for encrypting the data, and selective bit algorithm for embedding encrypting data onto the data file. And MD5 algorithm is used to authenticate the message.

Encryption Process

DES

The Data Encryption Standard was once a predominant symmetric-key algorithm for the encryption of electronic data. It was highly influential in the advancement of modern cryptography in the academic world.DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

1) Triple DES

In cryptography, Triple DES (3DES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. In cryptography, Triple DES (3DES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

2) RSA.

It is an asymmetric cryptographic algorithm. It is a block cipher in which the plaintext and cipher text are integers between 0 and n-1 for some n. A typical size for n is 1024 bits, or 309 decimal digits.

B. Embedding algorithm

Selective Bit Algorithm, The idea of this scheme is to encrypt different levels of selective parts of video stream by using the feature of video layered structures (e.g. encrypting all headers and I frames, encrypting all I frames and all I blocks in P and B frames). The basic selective encryption is based on the MPEG I-frame, P-frame, and B-frame structure. It encrypts the I-frame only because, conceptually P- and B- frame are useless without knowing the corresponding I-frame

C. *Authentication algorithm*

MD5 algorithm MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks. The message is padded so that its length is divisible by 512. The padding works as follows: first a single bit 1 is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits less than a multiple of 512. The remaining bits are filled up with a 64-bit integer representing the length of the original message in bits.

Implementation

A. Details of Language Used

The complete implementation of the design is in java language. Java is a programming language originally developed by James Gosling at Sun Microsystems (which is now a subsidiary of Oracle Corporation) and released in 1995 as a core component of Sun Microsystems Java platform.

We have majorly used the concepts of swings. Swing is a GUI widget toolkit for Java. Swing was developed to provide a more sophisticated set of GUI components than the earlier Abstract Window Toolkit (AWT). Swing provides a native look and feel that emulates the look and feel of several platforms, and also supports a pluggable look and feel that allows applications to have a look and feel unrelated to the underlying platform. It has more powerful and flexible components than AWT. In addition to familiar components such as buttons, check boxes and labels, Swing provides several advanced components such as tabbed panel, scroll panes, trees, tables, and lists. Unlike AWT components, Swing components are not implemented by platform-specific code. Instead, they are written entirely in Java and therefore are platform-independent.

B. Screenshots

Selection window which is shown in figure 2 consists of Hiding and Unhiding options both of which contain encryption algorithm buttons.

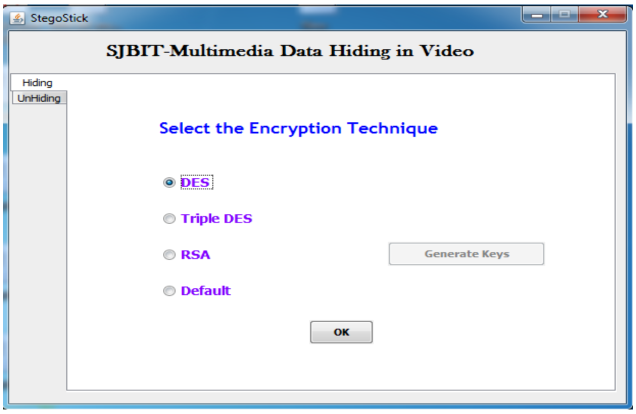

Figure 2: Snapshot for Selection of data encryption Algorithm

Figure 3 shows an interface of selecting the data files and cover file that is the video file that carries the secret message. Here the user also enters a dynamic password and the destination path where the embedded video file will be saved.

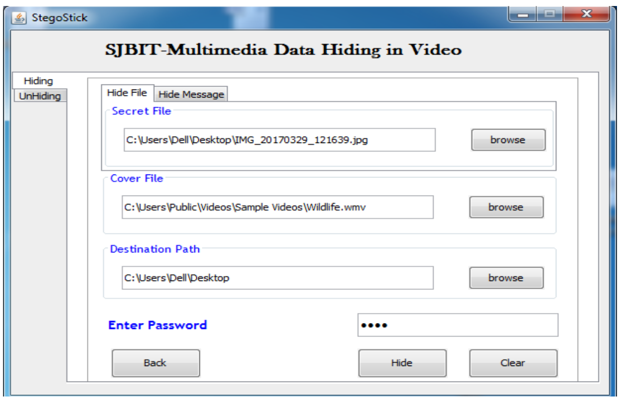

Figure 3.Selection of secret file and video file.

Figure 4- is a snapshot of the message dialog box that appears after successfully extracting the data hidden in the video file.

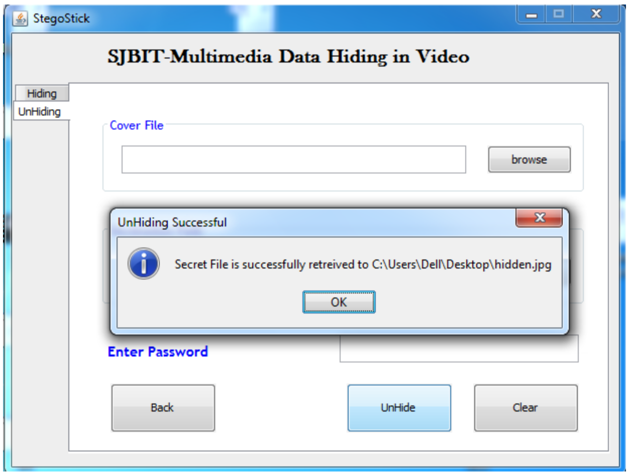

Figure 4.Dialog box after successful extraction of data files from video

Conclusion

In the proposed technique, we have introduced a concept of video steganography. We would like to emphasis that the goal of the technique is not to increase the capacity of the message but we tried to make it difficult for the unauthorized person to determine the presence of secret cipher. Moreover, we merge cryptography with it so that the security of the secret message is increased. So, the proposed technique fulfills the requirement of steganography technique.

Acknowledgement

We thank Dr. Mohan H.S,Professor & Head, Department of Information Science & Engineering, SJB Institute of Technology and our guide Prof. Darshan K.R for helping us with our work.

References

[1] Md.Rashedul Islam "An Efficient Filtering Based Approach Improvinvg LSB Image Steganography Using Status Bit along with AES Cryptography",IEEE -2014

[2] Das R,Tuithung T, "A novel steganography method for image based on Huffman Encoding", IEEE-2012

[3] Ramaiya M.K. Hemrajani N,Saxena A.K.,"Security Improvisation in Image Steganography using DES", IEEE-2012.

[4] Kumar, H, Anuradha ,"Enhanced LSB technique for Audio Steganography" ,IEEE July,2012

[5] Rajkumar L Biradar,"A Survey Paper on Steganography Techniques"- Vol-4,Issue 1 IJIRCCE-January2016

[6] Chhaya varade,Danish shaikh,Vishal kumar,Sharukh Qureshi-"A Rechnique for Data Hiding using Audio and Video Steganography"-IJARCSSE-2016

[7] ErsinEsen, A. AydinAlatan, "Robust Video Data Hiding Using Forbidden Zone Data Hiding And Selective Embedding ",IEEE ,VOL. 21, NO. 8, August 2015.

[8] K.Mohan, S.E.Neelakandan, "Secured Robust Video Data Hiding UsingN Symmetric Encryption Algorithms ", IJIRE ,VOL.6,December 2015.

[9] R. Ravi Kumar V., Kesav Kumar ,"Selective Embedding and Forbidden Zone Data Hiding for Strong Video Data Thrashing ",IJETT ,VOL. 4,September 2015.

[10] Mr.SudheerAdepu, Mr.P. Ashok ,Dr.C.V.GuruRao,"A Security Mechanism for Video Data hiding " ,IJCTT,VOL.4, August 2013.

[11] ResojuOmprakash and D. Jyothi,"Block Based Adaptive Videodata Hiding Technique", IJMSTH, 2012.

[12] W. Bender D. Gruhl,N. Morimoto,A. Lu,"Techniques for data hiding ", IBM Systems Journal, Vol.35, NOS 3 and 4, 2012.

[13] Mr. Mritha Ramalingam,"Stego Machine Video Steganography using Modified LSB Algorithm ", World Academy of Science, Engineering andTechnology,2011.

Author's details

[1,2,3,4]UG Students, 5Assistant Professor, Department of Information Science & Engineering, SJB Institute of Technology, Bengaluru, Karnataka, India

Email: harshithahp10@gmail.com