ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Improved Data Security Using Two Stage Steganography

Anmol D Kulkarni[1], Esti bansal[1], Rasika R Jadhav[1], Hole Rajashree B[1], Laxmi Madhuri[2]

Student, Dept. of Computer Engineering, Dr. D. Y. Patil School of Engineering Lohagaon, Pune, SavitribaiPhule Pune University, Pune, India[1]

Professor, Dept. of Computer Engineering, Dr. D. Y. Patil School of Engineering Lohagaon, Pune, SavitribaiPhule Pune University, Pune, India[2]

ABSTRACT: Security of data is an important issue. The data needs to be protected from unauthorized users to prevent undesired actions. Steganography is one of the techniques to protect data. It provides an efficient way of communication between sender and receiver without any loss in the data and originality of the cover object. This paper focus on enhancing the security of data by implementing a two stage process, where the data is hidden inside an image and then the image is hidden into a video. In the first stage improved least significant bit (LSB) method is used and in the second stage DCT algorithm is used. While embedding the data or image the visual quality of the cover image remains unchanged such that the negligible changes are not detected. The next focus is to reduce the size of the final video. This is achieved by compressing the video before transmission. Then the video is transmitted to the receiver where the receiver will extract the secret data.

KEYWORDS: Steganography, least significant bit, DCT, compressing

I. Introduction

Since these days with the rise in communication technologies the data can be transferred easily from one place to another, thus data security becomes a crucial issue. With the advent of new tools hackers can hack the data and misuse it. Hence there is a need to improve the existing techniques of hiding the data. Steganography is a method of hiding information by embedding message within another message that is to be kept secret. It hides the existence of the message. Steganography is carried out by substituting bits of useless or unused data in files (such as text, audio, video, graphics) with bits of secret information. This secret information can be cipher text, plaintext, images or even videos. Many times steganography is used in cases where encryption cannot be done. Or, steganography is used to reinforce encryption. The secret file may be encrypted before applying steganography or a file having secret data hidden into it may be encrypted at a later stage to provide security. Steganography provides an efficient way of communication between sender and receiver without any loss in the data and originality of the cover object. This technique protects the data from unauthorized or undesired viewing. Steganography not only hides the information but also keeps the presence of message secret whereas other techniques only hides the information, so there are chances that the information hidden may get noticed [1].

Many steganographic methods have been proposed in therecent years. But these techniques often suffer from issues like lack in security, may cause the quality of a cover file to degrade and also allow less data to be hidden.

So to overcome these issues and to enhance the security of data and improve the process of information hiding a two stage process is to be used. In this paper a two stage process is used in which the data is hidden inside an image and then the image is hidden into a video. In the first stage improved least significant bit (LSB) method is used to hide the secret data into image and in the second stage DCT algorithm is used to hide the obtained stego image into a video [10]. While hiding large amount of data the size of the video is increased which takes more time for transmission. Thus, the focus is to reduce the size of the final video. This is achieved by compressing the video before transmission. Then at the other end the receiver will extract the secret data by applying the same process in a reverse order.

DOI: 10.15680/IJIRCCE.2016. 0404228

II. Related work

An algorithm based on color histogram was proposed for video steganography [2]. The video is divided into frames and the histogram value of each frame is calculated. The secret data is hidden into the frames by dividing each pixel in two parts; the bits embedded in the right part are counted and mentioned in the left part.

An algorithm was proposed which was based on the principle of linear block code [4]. The algorithm made use of a sequence of nine uncompressed video sequences to be used as cover data. The secret message was a binary image. Even the secret message was encoded using Hamming code (7, 4) to make the message more secure before embedding.

An algorithm consisting a combination of steganography and cryptography was proposed with high capacity of embedding data [7]. Firstly, this process encrypts the message by a method called Transposition Cipher method. Then by using LSB insertion method the encrypted message is embedded inside an image. This algorithm claims to fulfill the requirements like capacity, security and robustness but it increases the size of the message to a great extent.

A new method was proposed to improve quality of image. In this technique identical bits are searched between the secret message and image pixel values [8]. Using this technique the secret message is hidden inside the image. The results were obtained by analyzing the ratio between the values of the pixel color and the values of the message. This technique is efficient in improving the quality of the image with 83% of accuracy ratio.

Another algorithm was proposed to maintain data integrity during steganography. The message is encrypted and then the encrypted bits are embedded by using RSA algorithm [9]. The first least significant bit is replaced using LSB method and the last four significant bits are replaced using Modulus 4 bit technique in the image pixels. MD5 hash algorithm is used to provide data integrity. Use of this algorithm satisfies the user that the integrity of the received message is intact.

III. Proposed System

The existing system suffer from issues like less data hiding capacity, less security and degrade the quality of cover image. To overcome these issues we propose a two stage process:

1. The text data is hidden into an image by performing Image steganography, then the stego image obtained in this stage is passed to the second stage.
2. The stego image is hidden into one of the selected frame of the video using steganography algorithm.

To send text message of small size large size video has to be transmitted which becomes a drawback. To overcome this drawback we will use compression technique to compress the video before transmission.

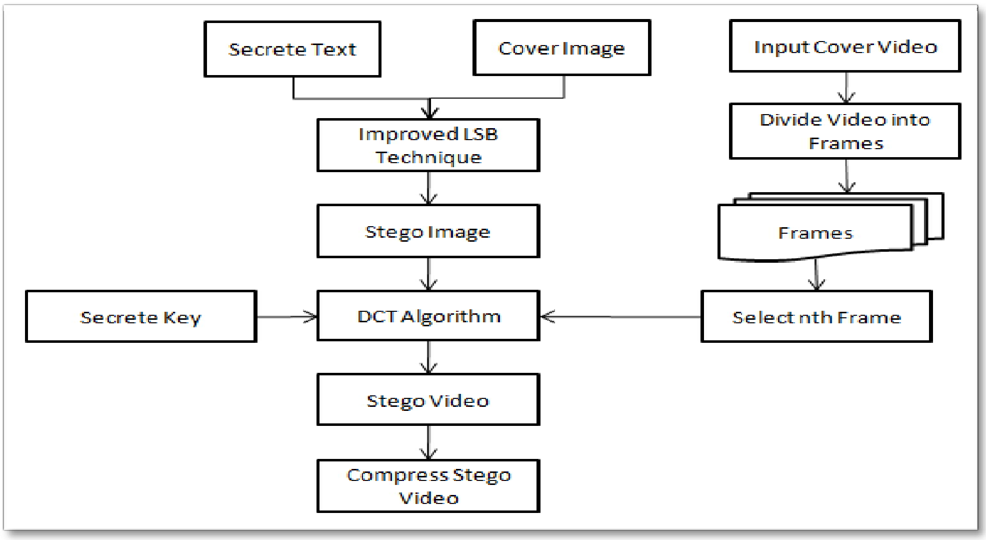

Fig. 1: Embedding process

STEPS USED FOR EMBEDDING(as shown in Fig. 1):

Step 1: Enter the secret text to be hidden.
Step 2: Select an image of any format (jpg, jpeg, gif etc) as a cover image.
Step 3: Divide the cover image into Red, Blue and Green plane.
Step 4: Substitute the LSBs of RGB with the bits of secret text in the order 2, 2, 4.
Step 5: From step 4 a stego image will be obtained.
Step 6: Select a video to be taken as a cover video.
Step 7: Divide the video into frames.
Step 8: Select Nth frame to hide the stego image.
Step 9: Select a key which is used in hiding the stego image into a frame using DCT algorithm.
Step 10: After this a stego video is obtained.
Step 11: Compress the stego video.
Step 12: Compressed stego video ready for transmission.

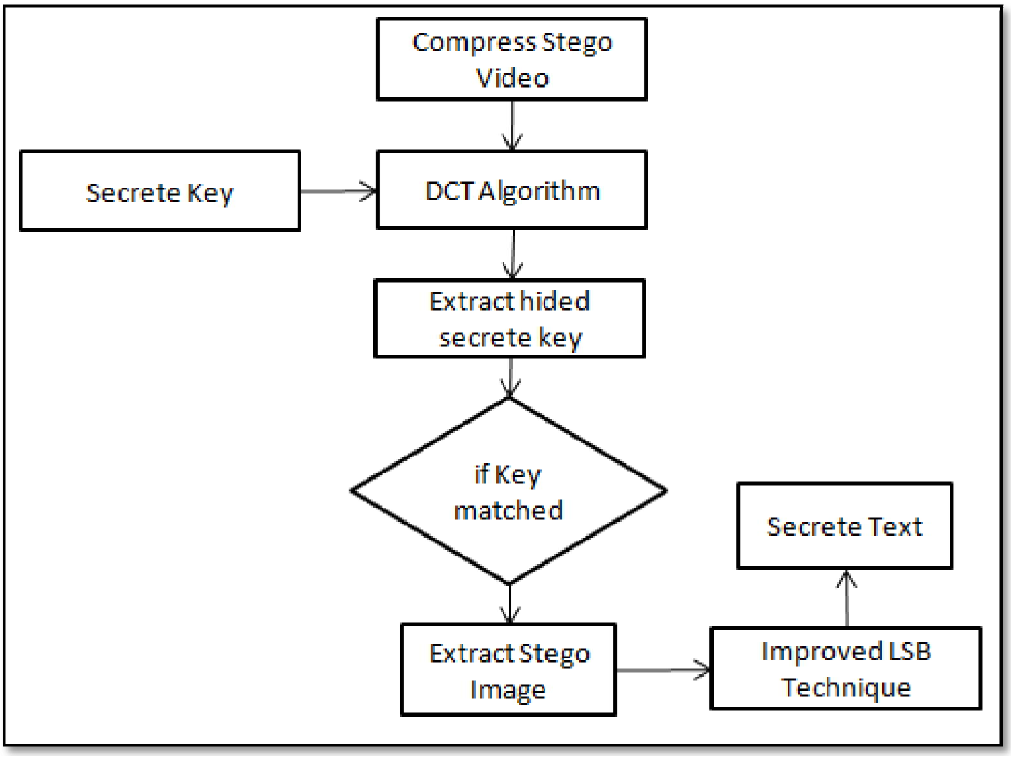

Fig. 2: Extraction process

STEPS USED FOR EXTRACTION(as shown in Fig. 2):

Step 1: Extract the stego video from the compressed video.
Step 2: Enter the key and if it matches go to step 3.
Step 3: Apply reverse DCT algorithm on the stego video to obtain stego image.
Step 4: Apply reverse improved LSB algorithm to extract the secret text.

IV. RESULTS

In this, results of final steps of the proposed methods are highlighted. Implementation is done on JAVA. Experimental results of intermediate steps show the efficiency of the proposed approach. As the following histogram shows that the image does not get tampered during extraction process.

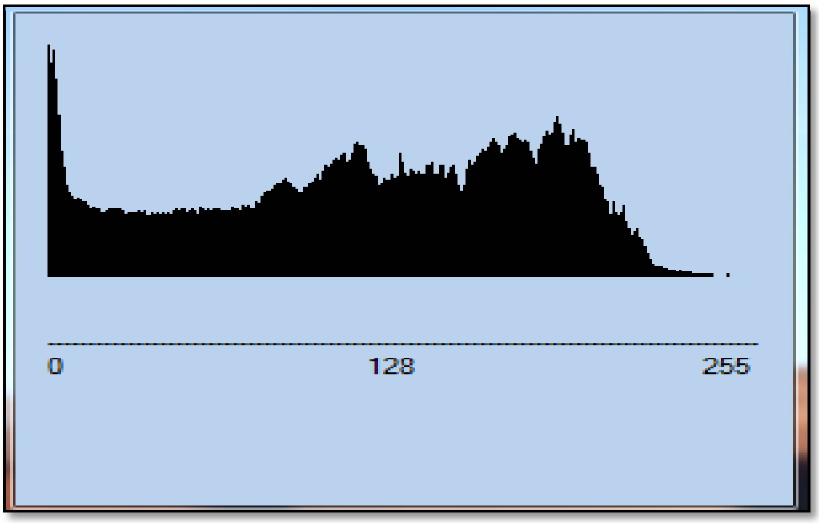

Fig. 3Histogram of stego image

Fig. 3 Depicts the histogram of stego image that is image obtained after secret message has been embedded. Generally histogram is used to show the difference between two images. Both the histogram has x axis with range of 0 to 255 that is histogram is calculated on grey colored images. For calculating histograms we have designed the program that converts images into grey scale and calculates histogram on grey scaled images. Total colors in histogram are 256 so the range is 0 to 255. As both histogramsdepicted by Fig. 3 and Fig. 4 are nearly similar which concludes that the image does not get tampered during extraction process. Hence the quality of image remains intact.

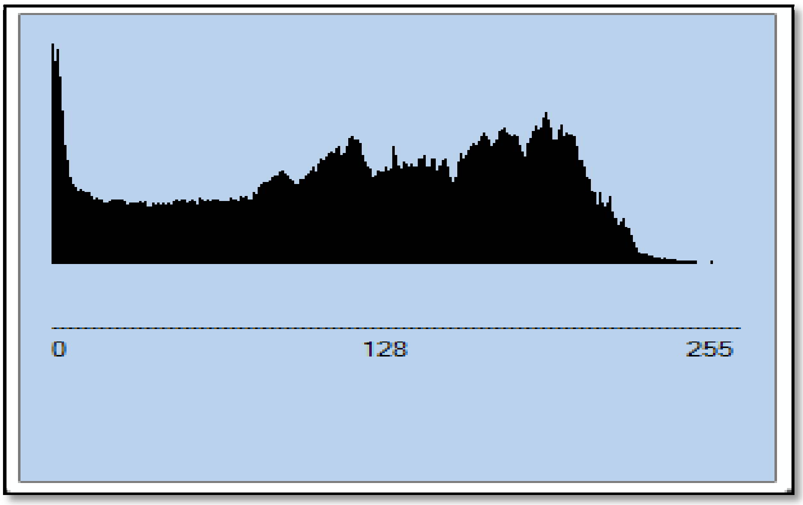

Fig. 4 Histogram of stego image after extraction

DOI: 10.15680/IJIRCCE.2016. 0404228

V. CONCLUSION AND FUTURE WORK

In this paper we have presented a new system for the combination of Steganography which could be proven as a highly secured method for data communication in near future. The proposed High secured system using steganography is tested by taking message and hiding it in image, this image then embbeded in selected input video. The results that are obtained from these experiments are recorded. The Proposed algorithm provides more security in comparison to simple LSB algorithm.

.

REFERENCES

[1] Amritpal Singh, Harpal Singh, “An Improved LSB based Image Steganography Technique for RGB Images”, IEEE *International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, DOI: 10.1109/ICECCT.2015.7226122, 2015

[2] S. Deepa1, R. Umarani, **“**A Prototype for Secure Information using Video Steganography”,*International Journal of Advanced Research in Computer and Communication Engineering*,Vol. 4, Issue 8, pp 442-444, August 2015..

[3] Mrudul Dixit, Nikita Bhide, SanikaKhankhoje, RajashwiniUkarande, “Video Steganography”, *International Conference on Pervasive Computing(ICPC)*, DOI: 10.1109/PERVASIVE.2015.7087159, 2015.

[4]Ramadhan J. Mstafa , Khaled M. Elleithy, “A Highly Secure Video Steganography using Hamming Code (7, 4)”, *IEEE Long Island Systems, Applications and Technology Conference(LISAT),* DOI: 10.1109/LISAT.2014.6845191, 2014

[5] Pooja Yadav, Nishchol Mishra, Sanjeev Sharma, “A Secure Video Steganography with Encryption Based on LSB Technique”, *IEEE International Conference on Computational Intelligence and Computing Research,*, DOI: 10.1109/ICCIC.2013.6724212, 2013.

[6] D. NithyaKalyani, Dr. K. Mahesh, “Safe Information Hiding Using Video Steganography”, *International Journal of Computer Science and Mobile Computing (IJCSMC),* Vol. 4, Issue. 7, pp. 502-512, July 2015,

[7] Shamim Ahmed Laskar, “High Capacity Data Hiding using LSB Steganography and Encryption”, International Journal of Database Management Systems (IJDMS), Vol. 4, No. 6, December 2012

[8] Attallah M. Al-Shatnawi, Al-albayt University, Mafraq, Jordan “A New Method in Image Steganography with Improved Image Quality”, Applied Mathematical Sciences (AMS), Vol. 6, 2012, no. 79, 3907-3915

[9] Deepali, “Steganography with Data Integrity”, International Journal of Computational Engineering Research (IJCER), Vol. 2, Issue 7, Issn 2250-3005, November 2012

[10] Anmol D Kulkarni, EstiBansl, Rasika R Jadhav, Hole Rajashree B, “Improved data security using video steganography”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 10, October 2015