EAI Endorsed Transactions
on Cloud Systems
Research Article EAI.EU

Video Steganography using MATLAB

Paramesh.G[1,*], Pavithra.K.V[2] , Ranjitha.N[3,] Swetha.S[4] and T.Anushalalitha[5]

[1]Alumni.Dept.of TCE,BMSCE
[2] Alumni.Dept.of TCE,BMSCE
[3]Alumni.Dept.of TCE,BMSCE
[4] Alumni.Dept.of TCE,BMSCE
[5] Assistant Professor, BMS college of Engineering,Bangalore-19

Abstract

This paper discusses a Video Steganographic scheme that can provide approvable security with high computing speed, by embedding data in video frames. The technique of embedding data in a video file by using LSB before which the secret information is encrypted using symmetric XOR operation, thereby providing two layers of security. Data Hiding and Extraction procedure are experimented successfully. All experiments are done using Matlab 2010a simulation software. This method proves to be more efficient than other methods with the amount of data that can be embedded in it, showing a PSNR of above 30 dB.

Keywords: video steganography; LSB substitution

Received on 14 October 2017, accepted on 26 November 2017, published on 20 December 2017

doi: 10.4108/_____

1. Introduction

Video Steganography is a technique to hide any kind of files in any extension into a carrying video file. An input content such as video is encoded to hide plural-bit auxiliary data therein. The process generates an intermediate signal that is a function of the plural bit auxiliary data and data related to human perception attributes of the content signal. This intermediate signal is then summed with the content signal to effect encoding. The encoding is desirably robust against various forms of content degradation such as lossy compression/decompression, scaling, re-sampling, analog to digital conversion and back again etc., so that auxiliary data can be detected back from the content not withstanding such corruption.

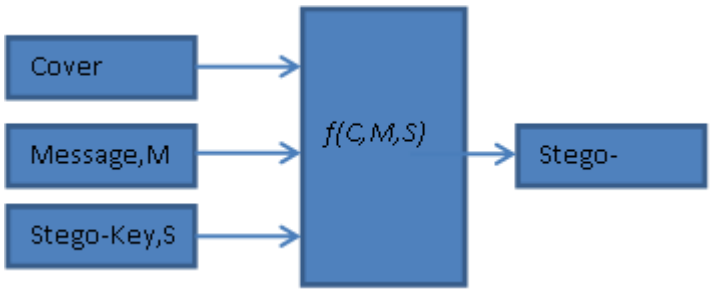

Figure 1. Basic Model of Steganography

*Corresponding author. Email:author@emailaddress.com

2. Video Steganography

Message is the data that the sender wishes to remain it confidential. It can be plain text, cipher text, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Password is known as stego-key, which ensures that only recipient who knows the corresponding decoding key will be able to extract the message from a cover-object. The cover-object with the secretly embedded message is then called the stego-object.

Yadav.P.et.al[1] proposed a technique in which each frame of secret video is broken down into individual components, then converted into 8 binary values, and encrypted using XOR with secret key, encrypted keys will be hidden in the LSB of each frames using sequential encoding of cover video. Balaji.R et.al [2] created an index for the secret information, placed in the frame of the video. Mozo,A.J.et.al. [3] got promising results for the uncompressed FLV embedded with data and uncompromised integrity of hidden data when modified FLVs were transferred through internet. Kelash.H.M.et.al[4] proposed an algorithm based on color histograms for embedding data into video clips directly.

1.2 Problem Definition

The aim of this paper is to arrive at a method for embedding information into video files without affecting its original perception and also not giving any hint to the intruder.

The objectives are three fold.

i. Hiding the secret information in an AVI video file format

ii. Encryption to increase security

iii. Decryption and message recovery.

A. Steganography Vs Cryptography

In Cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. Steganography, in contrast, hides the secret message inside a cover image, so it cannot be seen.

It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography.

A steganographic algorithm for compressed video is introduced in this paper. In a GOP, control information is embedded in I frame, and in P frames, and B frames, the data are repeatedly embedded in motion vectors of macro-blocks, for the purpose of resisting video processing. Because digital video consists of series of frames and greater signal space, video steganography will get large capacity compared to image.

Video Steganography can be done in several ways based on the following.

i. Non-uniform rectangular partition

ii. Tri-way Pixel value Differencing

iii. Adaptive scheme for compressed video steganography

iv. LSB substitution using differential polynomial equations

v. Vector quantization of DCT

vi. Integer Wavelet Transform

vii. Dynamic cover generation

B. Methodology

The methodology used is Least significant bit (LSB) for video steganography, bits of the message are directly embedded into LSB plane of the cover image, in a deterministic sequence. Modulating the LSB does not lead to human perceptible difference, as th change in amplitude is small.

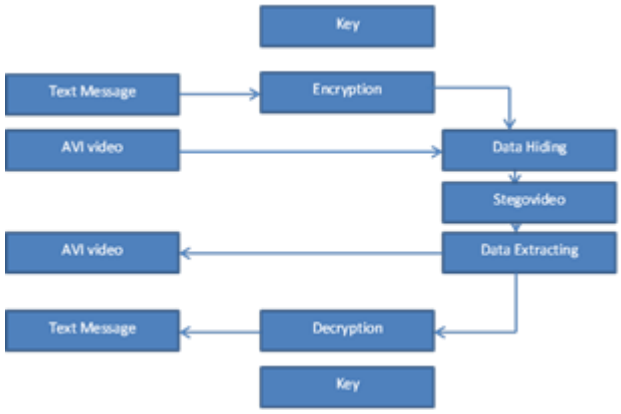

Figure 2.Block Diagram

The text message is the secret data which is to be encrypted and hidden inside the video. Befor hiding the information, it is encrypted using symmetric encryption. Stego video is the video obtained after putting back the embedded frame in a video using LSB substitution technique

2.1. LSB SUBSTITUTION TECHNIQUE

This is the simplest of approaches. The binary representation of the hidden data is taken and used to overwrite the LSB of each byte within the cover image. If a 24-bit color is used, the amount of change will be minimal and indiscernible to the human eye.

The following example illustrates the method.

There are three adjacent pixels`(nine bytes) with the following RGB encoding:

Figure 3 .A sample raster data for three pixels

If the9 bits of data 100000001 are to be hidden, these 9 bits are overlayed over the LSB of the 9 bytes above.

RGB Images

Three colors RGB of intensity varying from fully OFF to fully ON form the color component. Zero intensity of each component gives the darkest color and full intensity gives white. When the intensities of all components are same, it forms grey, darker or lighter depending upon the intensity. When the intensities are different, the result is a colorized hue, more or less saturated depending on the difference of the strongest and the weakest of the intensities of the primary colors employed.

The algorithm here is a combination of cryptography and steganography, but in a robust way as to reinforce each other. The subjects of the algorithm are text information and video, where the text is encrypted and embedded into the video.

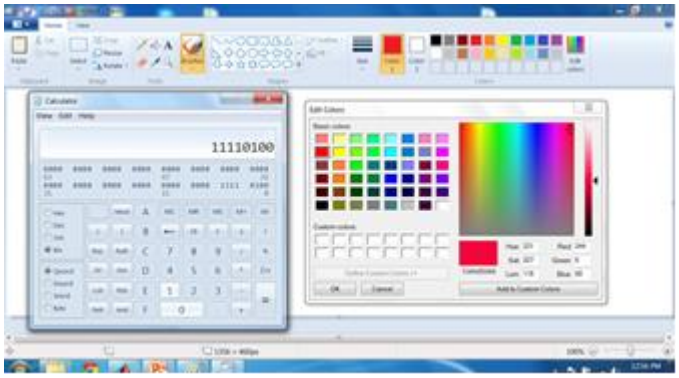

Figure 4. Original color intensity

The above figure shows the color intensity in the specified position, which are as follows:

Red-244
Green-6

Blue-60As the following order RGBBGRRG is used, red channel is used initially. The pixel value is then converted into corresponding binary value.

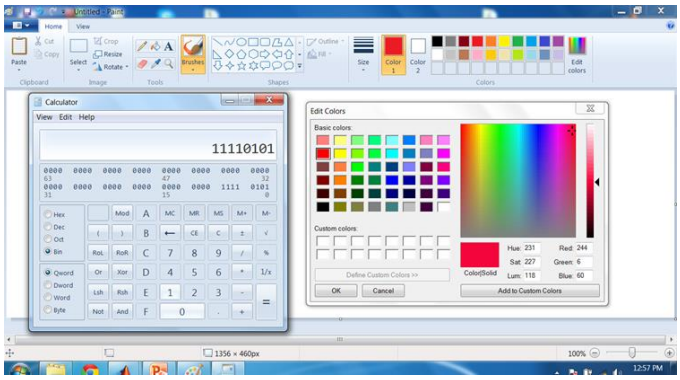

Figure 5. Altered color intensity

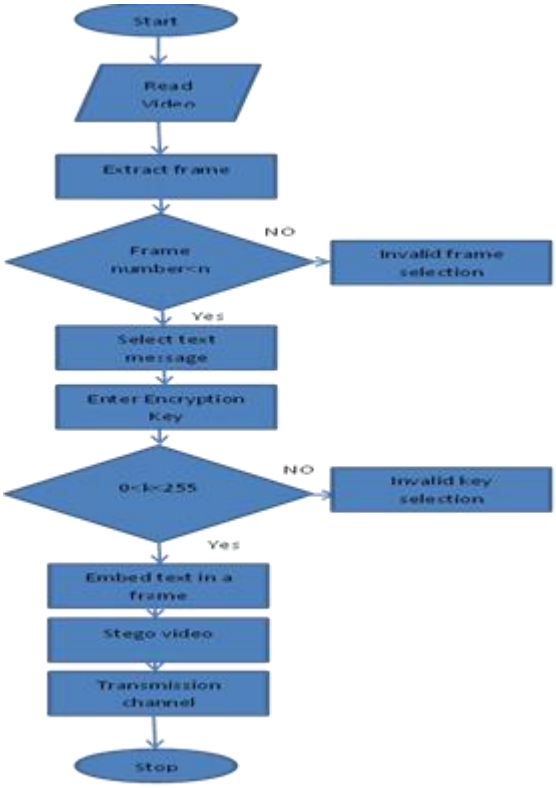

Figure 6. Flow chart for Encoding

The above figure shows the 1 LSB bit manipulation of the pixel value. After replacing the LSB bit, the intensity of the color will not change to a greater extent.

Since only one bit manipulation is achieved, there will not be much variations in the intensity of the frame, so that intruder will not be in a position to make out that the frame is modified. Encryption is performed before hiding the secret information which ensures two layers of security. Hence the attacker would be forced to believe that the file is a AVI video file. But for the intended recipient who receives the file shall have the knowledge of decoding the information by which he will be able to decrypt it faithfully.

A. Encoding

i. The raw video in which the text has to be embedded is read, thereby separating the frames from the video.
ii. The user defined frame is selected which should be within the range of the video.
iii. The text is taken and encrypted using encryption key.
iv. Here, the symmetric XOR operation is done for the encryption of the text information. The 8-bit key can take any value fron 0-255 for the encryption.
v. The encrypted data bits are replaced in the LSB of each channel pixel value of the selected frame using a RGBBGRRG order. It is done fron left to right through the target image.
vi. This process is repeated for all the data points.
vii. The text embedded frame is replaced back into the original raw video.This regenerated video is called StegoVideo.This finished file is dubbed as an AVI video file.

B. Decoding

i. At the receiver end, the stegovideo looks like the ususal video.
ii. The receiver will have the knowledge of the frame and encryption key used in the encoding, only if he is the authorized person.
iii. Thus, the encrypted data is obtained by performing the reverse of the LSB operation.
iv. Since it is the symmetric encryption, by using the same key, XOR operation is done to retrieve the original secret information.
v. To achieve this, the sender and the receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

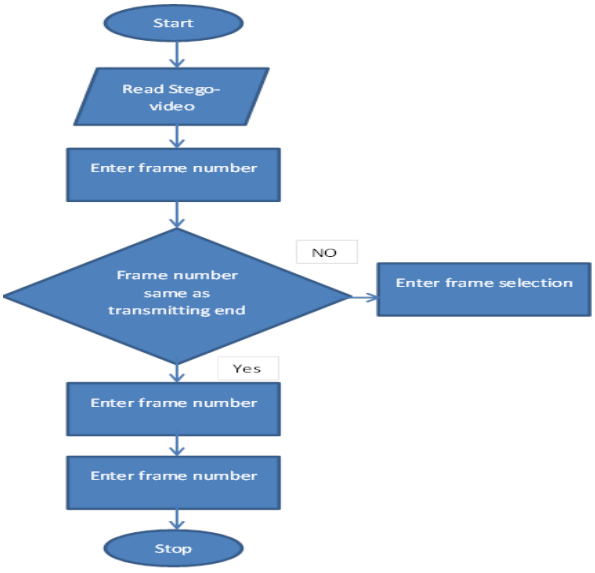

Figure 7. Flow chart for Decoding

C. Software used

- A very large (and growing) database of built-in algorithms for image processing and computer vision applications.
- MATLAB allows you to test algorithms immediately without recompilation. You cantype something at the command line or execute a section in the editor and immediately see the results, greatly facilitating algorithm development.
- The MATLAB Desktop environment, which allows you to work interactively with your data, helps you to keep track of files and variables, and simplifies common programming/debugging tasks. The ability to read in a wide variety of both common and domain-specific image formats.
- The ability to call external libraries, such as OpenCV. Clearly written documentation with many examples, as well as online resources such as web seminars ("webinars").
- The ability to auto-generate C code, using MATLAB Coder, for a large (and growing) subset of image processing and mathematical functions, which you could then use in other environments, such as embedded systems or as a component in other software.

A. *P*erformance Analysis

These automated quality assessment techniques are based on mathematical and computational algorithms to measure the accuracy of the perceived image. Most of the recent objective quality assessment techniques are based on computing the quality of the image with the original image. Here we compare the accuracy of the cover image with the stegoimage using two techniques,ie.,Mean Square Error(MSE) and Peak Signal to Noise Ratio(PSNR).

$$MSE = \frac{\sum_{M,N}[C(m,n)-S(m,n)]^2}{M \times N}$$

Where M and N are the rows and columns of the cover image respectively, C and S are the cover and stegoimage respectively.

$$PSNR = 10 \log_{10} \frac{R^2}{MSE}$$

Where R is the dynamic range of pixel values(R=255 for gray scale images).PSNR gives the value infinity under one condition only; that is when the cover image is compared to itself.

Otherwise if the PSNR result is greater than 30 dB , then the human visual system would not be able to differentiate between the cover image and the stegoimage progressively. A
PSNR value of less than 30 dB would indicate a human ability to notice the quality degradation.

By using the above equations and getting the number of pixels at each level from the histogram of the cover and stegoimage as shown , we have

$$PSNR \approx 78.4038$$

As we see the PSNR value is greater than 30 db which indicate that human visual system cannot differentiate between cover image and stegoimage.

Figure. 8 Input Video

STEPS:

- The input is an AVI (AUDIO VIDEO INTERLEAVE) format
- The duration of the video is 10 secs.

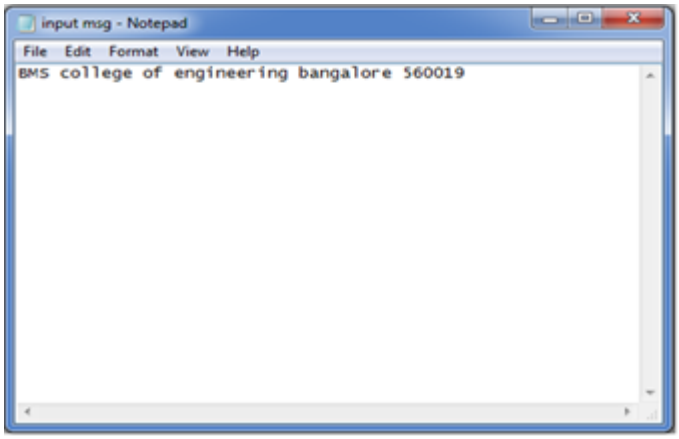

Figure. 9 Input Message

- The input is in the ".txt format"
- The input message can be alphabet, number and special character.

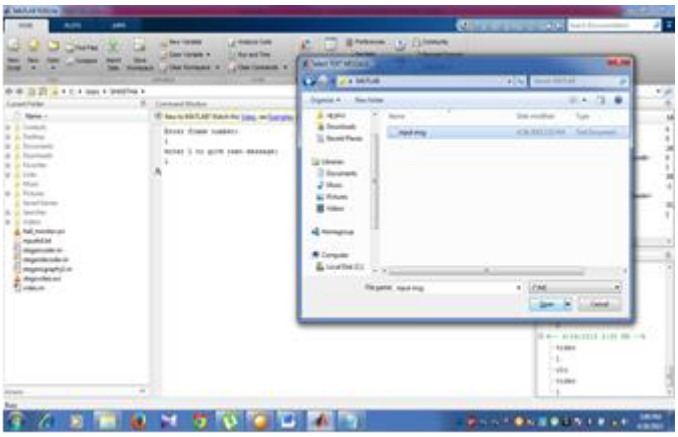

Figure. 10 Selecting Text file

Steps to start the encoding process

- Select the frame from the video.
- Frame number must be within the range of video.
- If the entered frame number is beyond the range it will display invalid frame number.
- Select the text information (.*txt file format) to be embedded in the frame.

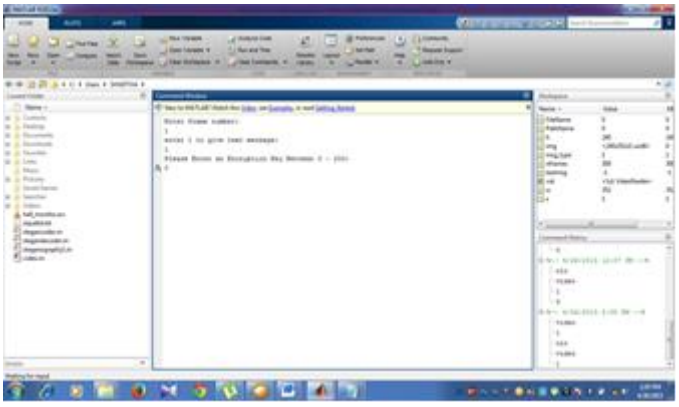

Figure. 11 Encryption Key

Symmentric encryption is used.

- Same key must be used in both encryption and decryption.
  - Enter the encryption key in the range 0-255.
  - The text is encrypted using the key.

Steps to start decoding process:

- Stegovideo is choosen.
- The text is extracted and decrypted from the frame using the key.
- Same frame number must be entered as used in encryption process.
- Also decryption key must be same as encryption key.
- We must give the name of the folder where result will be store as ".txt" format.
- The recovered text is saved in the specified folder.

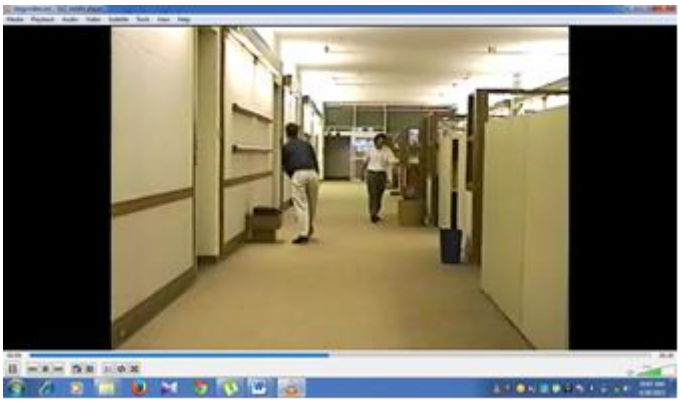

Figure. 12 Stego Video

The text selected is embedded in the specified frame .

- The modified frame is replaced in the original video.
- The above figure shows the obtained stego video which is saved in a folder.
- The duration of the stegovideo will be 20sec.
- The stegovideo will be slower than original video.

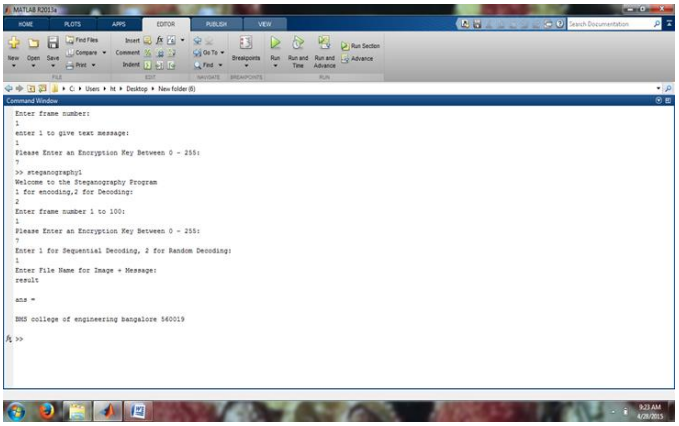

Figure. 13 Recovering Text

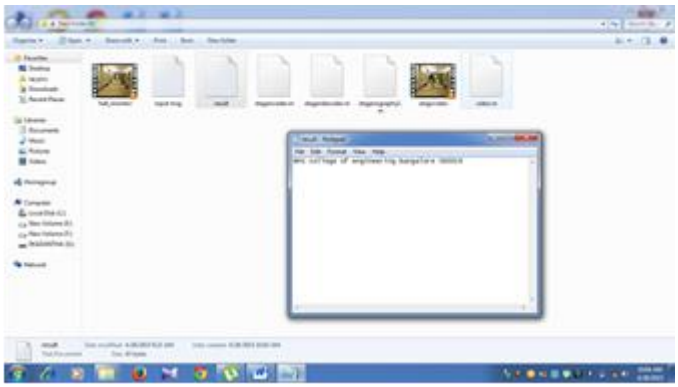

Figure. 14 Recovered text file is saved as,".txt"in a specified folder

CONCLUSION

With the growth in digital media, data security has become a major concern. Mere steganography is not a good solution to secrecy nor is mere encryption but a combination of both provide a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place.

In this project we have presented two levels of security for communicating secret information. Video steganography proves to be more efficient than other steganographic methods with the amount of data that can be embedded in it. The text is encrypted prior embedding in the video thus increasing the security of information. Since the text is embedded by modifying only the least significant bit, no much change in the intensity of the image is noticeable. The calculated PSNR obtained above 30 dB verifies this.

For an intruder to steganalyse and decrypt the information he/she must have the knowledge of various parameters, which include the frame in which the information or data is hidden and the encryption key.

The future work mainly focuses on audio-video steganography with chaotic algorithm and reversible data hiding mechanism. Through reversible data hiding method the exact image and data can be retrieved along with the cover video and audio. The audio and video quality can also be preserved. The reversible data hiding method is mainly based on interpolation and error prediction mechanism.

Acknowledgments

The work reported in this paper is supported by the college through the TECHNICAL EDUCATION QUALITY IMPROVEMENT PROGRAMME [TEQIP-II] of the MHRD, Government of India.

References

[1] Yadav, P.; Mishra, N.; Sharma, S., "A secure video steganography
with encryption based on LSB technique," Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on , vol., no., pp.1,5, 26-28 Dec. 2013.

[2] Balaji, R. "Secure data transmission using video Steganography" IEEE International Conference on Electro/Information Technology (EIT), 2011, pp. 1 – 5.

[3]Cryptography and Network security-Principles and Practice: William Stallings, ThirdEdition. Fundamentals of image processing by Rafeal C. Gonzalez and Richard E. Woods,second edition. Pearson edition inc.

[4]Mozo AJ., and Obien M.E., C.J. Rigor, "Video Steganography using Flash Video (FLV)" I2MTC 2009 - International Instrumentation and Measurement Technology Conference Singapore, 5-7 May 2009.

[5]Kelash, H.M., Abdel Wahab, O.F., Elshakankiry, O.A., and El-sayed, H.S., Hiding data in video sequences using steganography algorithms, in Proceedings of International Conference on CT Convergence (ICTC), 2013, DOI-10.1109/ICTC.2013.6675372, pp:353-358.