



Hiding of Secret Information behind Video Frames Using LSB & ISB

Jasvir Kaur¹, Neha Jain²

^{1,2}Computer Science Engineering, Punjab Technical University,
Jalandhar, Punjab, India

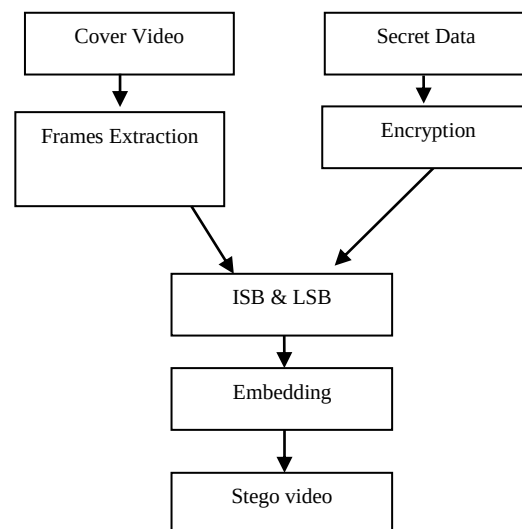
Abstract: Video Steganography is a method to conceal any sort of records into convey Video document. Different encryption format can be agreed by the two persons in such a way that no one can find the information from the video. Main problem arises because due to embedding behind least significant bits of video frames stagnalysis can be one easily on these frames to retrieved data. Second issue is that on embedding the data size of data gets increases which are not easy to transmit over the network. To overcome this problem occurred in video Steganography we will use ISB & LSB approaches.

Keywords: Video Steganography, ISB, LSB.

1. INTRODUCTION

A. Steganography: Steganography is characterized as the craft of hiding data, information or messages in a picture. Indeed the diverse record organizations can be utilized with the end goal of hiding the data like for instance the feature or sound and so forth. The object is to pass on the data with no respect or learning of others securely to the goal. The playing point of steganography is that the individuals who are outside the gathering even don't understand that a correspondence is being carried out.

Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.



In this figure

- In the first phase the cover video data has to be selected and from that particular data different numbers of frames have to be extracted. From particular frames the intermediate significant bits and least significant bits has to be captured. On the other side the secret data has to be encrypted by using encryption scheme and this data has to be converted into message vector. And each bit has to be embedded behind ISB and LSB detected using XOR operation.
- The encoder will encrypt the video by using secret key to hide information so that it should be shared secretly. Then decompression will be done. It converts the information so that the existence and nature of the information will be only known by the sender and intended recipient. The information will be hidden into a file and send to the receiver for decryption.

- On the receiver end different bits from the stego video have been extracted and the bits extracted in a message format and after this message are reshaped to construct the image vector. The least significant bits will be decrypted by the receiver to get the secret information.

B. Different kind of Stenography

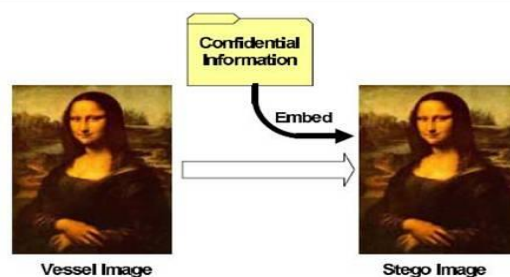
B.1 Text stenography: Hiding data in content is the most vital strategy for steganography. The method was to hide a mystery message in every nth letter of each expression of an instant message. In the wake of blasting of Internet and diverse kind of advanced document groups it has diminished in importance.

B.2 Audio stenography: Audio stenography is veiling, which misuses the properties of the human ear to shroud data unnoticeably. A perceptible, sound can be imperceptible in the vicinity of an alternate louder audible sound.

B.2.1 Audio Steganographic Methods: There have been numerous procedures for concealing data or messages in sound in such a way that the adjustments made to the sound record are perceptually indiscernible.

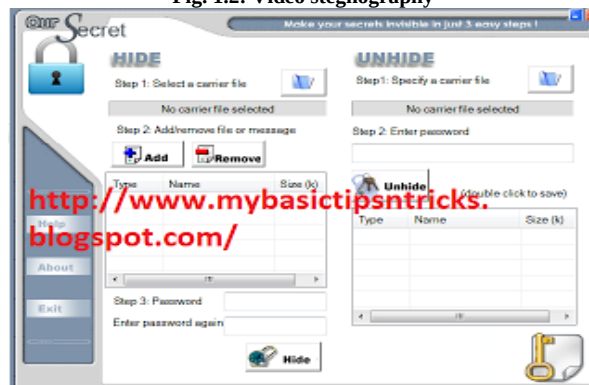
B.3 Image stenography: Pictures are utilized as the prominent spread items for steganography. A message is implanted in a computerized picture through an implanting calculation, utilizing the mystery key. The resulting stego picture is send to the receiver. On the other side, it is handled by the extraction calculation utilizing the same key.

Fig. 1.1: Image Steganography



B.4 Video Steganography: Video Steganography is a method to conceal any sort of records into convey Video document. The utilization of the feature based Steganography can be more qualified than other interactive media documents, on account of its size and memory prerequisites. The least significant bit (LSB) insertion is an essential methodology for implanting data in a transporter record. Least significant bit (LSB) insertion system works on LSB bit of the media document to conceal the data bit.

Fig. 1.2: Video steganography



In this extend, an information concealing plan will be produced to conceal the data in particular casings of the feature and in particular area of the edge by LSB substitution utilizing polynomial mathematical statement. Video Steganography is a system to hide any sort of records in any extension into a carrying Video file. This venture is the application created to insert any sort of data (File) in an alternate document, which is called transporter record.

C. Steganography Techniques

C.1 Substitution Technique: In the substitution technique, the repetitive parts are secured with a mystery message. This procedure incorporates the Least Significant Bit Substitution system, where we pick a subset of spread components and substitute the slightest huge bits of every component by the message bits.

C.2 Spread Spectrum Technique: This strategy utilizes the idea of spread range. The message is spread over a wide recurrence transfer speed. The sign to commotion proportion in every recurrence band is small to the point that it is hard to catch. Regardless of the fact that parts of message are expelled from a few groups, enough data is show in different groups to recuperate the data.

C.3 Transform Domain Technique: In the transfer domain technique; the secret message is embedded in the transform space (e.g. frequency domain) of the cover. An example of this method includes the Discrete Cosine Transform (DCT) domain. The cover image is split into 8*8 blocks and each block is used to encode one message bit. The blocks are chosen in a pseudorandom manner. The relative size of two predefined DCT coefficients is modulated using the message bit. The two coefficients are chosen from middle frequencies.

C.4 Distortion Techniques: The data is put away by distorting the sign. The encoder applies a succession of changes to the spread. This grouping compares to the mystery message. The decoder measures the contrasts between the first cover and the contorted spread to identify the grouping of alterations and therefore recuperate the mystery message.

C.5 Statistical Techniques: In the statistical techniques, the information is encoded by changing several properties of the cover. The cover is split into blocks and each block is used to hide one message bit. If the message bit is one, then the cover block is modified otherwise the cover block is not modified.

C.6 Protection of Data Alteration: We exploit the delicacy of the inserted information in this application zone. On the off chance that it is actualized, individuals can send their "computerized endorsement information" to wherever on the planet through Internet. Nobody can fashion, change, nor alter such authentication information.

D. Histogram: A histogram is a graphical representation of the distribution of numerical data. It is an estimate of the probability distribution of a continuous variable (quantitative variable) and was first introduced by Karl Pearson. To construct a histogram, the first step is to "bin" the range of values—that is, divide the entire range of values into a series of intervals—and then count how many values fall into each interval. The bins are usually specified as consecutive, non-overlapping intervals of a variable. The bins (intervals) must be adjacent, and are usually equal size. If the bins are of equal size, a rectangle is erected over the bin with height proportional to the frequency, the number of cases in each bin. In general, however, bins need not be of equal width; in that case, the erected rectangle has *area* proportional to the frequency of cases in the bin. The vertical axis is not frequency but *density*: the number of cases per unit of the variable on the horizontal axis.

E. Techniques Used

E.1 Least Significant Bit: Least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the *right-most bit*, due to the convention in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the *ones* (right-most) position. It is common to assign each bit a position number, ranging from zero to N-1, where N is the number of bits in the binary representation used. Normally, this is simply the exponent for the corresponding bit weight in base-2 (such as in $2^{31} \dots 2^0$). Although a few CPU manufacturers assign bit numbers the opposite way (which is not the same as different endianness), the term least significant bit itself remains unambiguous.

The advantages of LSB are it provides security & occupy minimum space.

E.2 Intermediate significant bit: A Intermediate Significant Bit ISB insertion algorithm is proposed for hiding the bit sequences of the cipher text into the time-frequency domain using wavelet transform of the image pixels, in order to improve the robustness of the Steganography system. Results demonstrate the effectiveness of wavelet Modified Intermediate Significant Bit WMISB while evaluating its performance using Peak Signal to Noise Ratio PSNR measure. Moreover, additional experiments are evaluated for noising, and image compression for cover images to compare their Peak Signal to Noise Ratio PSNR. Bit Error Rate BER, is a key parameter that is used in assessing systems that transmit digital data from one location to another.

II. RESULTS

Fig. 6.1 GUI of the proposed work



Fig. 6.1 represents the graphical user interface of the proposed work.

Fig. 6.2 Representation of selection of cover video

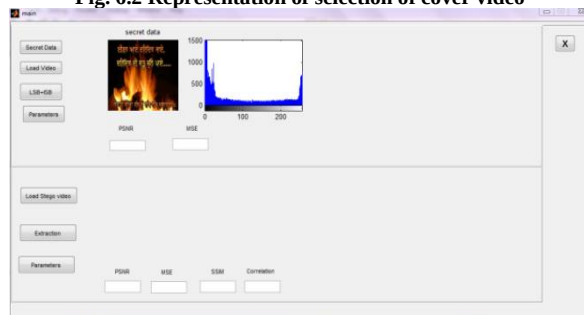


Fig 6.2 represents the first phase in which the cover video data has to be selected and from that particular data different numbers of frames have to be extracted.

Fig. 6.3 Representation of image into frames

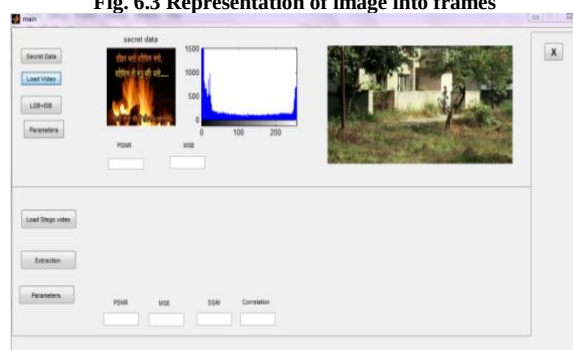


Fig 6.3 represents the image particular frames the intermediate significant bits and least significant bits has to be captured. On the other side the secret data has to be encrypted by using encryption scheme and this data has to be converted into message vector.

Fig. 6.4 Extraction of least and intermediate significant bits



Fig 6.4 represents the phase in which each bit has to be embedded behind ISB and LSB detected using XOR operation.

Fig 6.5 Representation of encryption of video

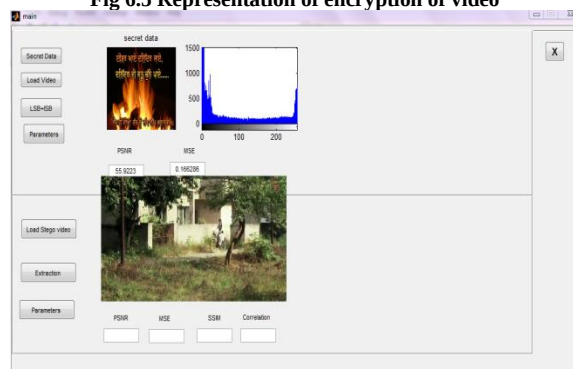


Fig 6.5 represents the encoder will encrypt the video by using secret key to hide information so that it should be shared secretly. Then decompression will be done.

Video	PSNR (Proposed)	PSNR (Previous)
Video1	58.96	45.98
Video2	60.39	46.65
Video3	65.68	53.68
Video4	59.26	44.62
Video5	55.69	42.63

Fig. 6.6 Represents video at the receiver side

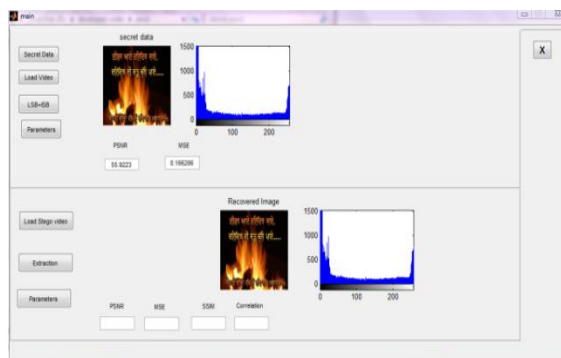


Fig 6.6 represents on the receiver end different bits from the stego video have been extracted and the bits extracted in a message format

Fig. 6.7 representing resulting parameters

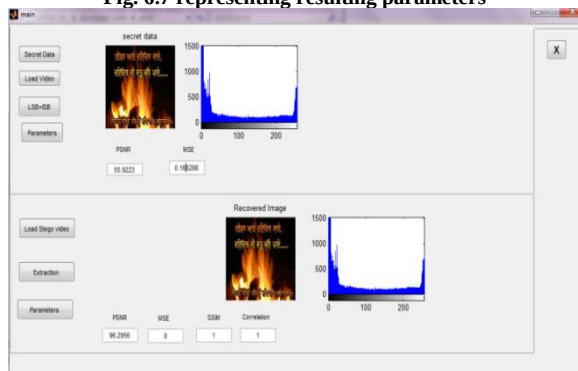


Fig 6.7 represents that the message are reshaped to construct the image vector. The least significant bits will be decrypted by the receiver to get the secret information.

Table 6.1 parameters values for video steganography

Video	PSNR (dB)	MSE
Video1	58.96	0.176
Video2	60.39	0.065
Video3	65.68	0.16
Video4	59.26	0.06
Video5	55.69	0.26

This table represents the value of PSNR, MSE for video steganography.

Table 6.2 represents PSNR values of previous and proposed work. On comparing the results of previous approach used and proposed approach we conclude that the PRSN in proposed approach gives better results than the previous one.

Table 6.3 Table representing MSE values of previous and proposed work

Video	MSE (Proposed)	MSE (Previous)
Video1	0.176	0.55
Video2	0.065	0.46
Video3	0.16	0.63
Video4	0.06	0.36
Video5	0.26	0.58

Table 6.3 represents MSE values of previous and proposed work. On comparing the results of previous approach used and proposed approach we conclude that the MSE in proposed approach is lesser as compared to the previous one.

III. CONCLUSION

Steganography is characterized as the craft of hiding data, information or messages in a picture. Steganography is an excellent means of conversing covertly if there are guarantees on the integrity of the channel of communication. If the video is seen by normal person, it is found that there is nothing but the normal video, but only the known persons can find out the decrypted message from the video. Main problem arises because due to embedding behind least significant bits of video frames steganalysis can be one easily on these frames to retrieved data. This does not provide security to secret data. Second issue is that on embedding the data size of data gets increases which are not easy to transmit over the network. To overcome these problem occurred in video Steganography various types of approaches has been studied and MLSB is taken as most appropriate approach for embedding of data. We got various types of parameters & on the basis of these parameters conclude that our system gives us better results.

Future Scope: In future we can hide video in the video frames & use encryption of one time password (OTP) approach for secure transmission of data.

ACKNOWLEDGMENTS

The author wishes to express her sincere gratitude and indebtedness to her Supervisor, *Prof. Neha Jain (Assoc. Prof., Department of computer science engineering)* for her valuable guidance, attention-grabbing views and obliging nature which led to the successful completion of this study. I lack words to express my cordial thanks to the members of Departmental Research Committee (DRC) for their useful comments and constructive suggestions during all the phases of the present study as well as critically going through the manuscript. Words fail the author to express her deep sense of gratitude towards his family members for their moral and financial support and encouragement without which the author would not have been able to bring out this thesis.

REFERENCES

- [1] Chengdu Hub "A Novel Video Steganography Based on Non-uniform Rectangular Partition" *14th International Conference on Computational Science and Engineering (CSE)*, 2011, pp. 57 – 61.
- [2] Bin Liu, "Secure Steganography in Compressed Video Bit streams" *Third International Conference on Availability, Reliability and Security*, 2008, pp. 1382 – 1387.
- [3] Balaji, R. "Secure data transmission using video Steganography" *IEEE International Conference on Electro/Information Technology (EIT)*, 2011, pp. 1 – 5.
- [4] Keren Wang, "Video Steganalysis Against Motion Vector-Based Steganography by Adding or Subtracting One Motion Vector Value" *IEEE Transactions on Information Forensics and Security*, 2014, pp. 741 – 751.
- [5] Tasdemir, K. "Video steganalysis of LSB based motion vector steganography", *IEEE Conf on Visual Information Processing (EUVIP)*, 2013, pp 260 – 264.
- [6] Dehkordi, A.B. "Robust LSB watermarking optimized for local structural similarity", *IEEE Conf. on Electrical Engineering (ICEE)*, 2011, pp 1
- [7] Islam, M.R. "An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography", *IEEE Conf. on Informatics, Electronics & Vision (ICIEV)*, 2014, pp 1 – 6
- [8] Yi-Chun Liao "Data hiding in video using adaptive LSB", *IEEE Conf. on Pervasive Computing (JCPC)*, 2009, pp 185 – 190
- [9] Pooja Yadav "A Secure Video Steganography with Encryption Based on LSB Technique" *2013 IEEE International Conference on Computational Intelligence and Computing Research*.
- [10] Mstafa, R.J., Elleithy, K.M. "A highly secure video steganography using Hamming code" *IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 2014, pp. 1 – 6.
- [11] ShengDun Hu "A Novel Video Steganography Based on Non-uniform Rectangular Partition" *14th International Conference on Computational Science and Engineering (CSE)*, 2011, pp. 57 – 61.
- [12] Bin Liu "Secure Steganography in Compressed Video Bitstreams" *Third International Conference on Availability, Reliability and Security*, 2008, pp. 1382 – 1387.