



Video Steganography by Hiding Secret Image behind Multiple Least Significant Bit of Color Components

Navdeep Ghotra*

Computer Science & Engineering
HEC, Jagadhri, India

Aashdeep Singh

Computer Science & Engineering
HEC, Jagadhri, India

Kamal Gupta

Computer Science & Engineering
GNI, Mullana, India

Abstract: Steganography is an excellent means of conversing covertly if there are guarantees on the integrity of the channel of communication[1]. The Different encryption format can be agreed by the two persons in such a way that no one can find the information from the video. In Video Steganography data encrypted behind the least significant bits of video frame. 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 remove this problem occurred in video Steganography various types of approaches has been studied and MLSB is taken as most appropriate approach for embedding of data. Size of embedded data can be reduced by performing compression to stego video file.

Keywords: Steganography, Cryptography, MLSB.

I. INTRODUCTION

1.1 Steganography: The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. Steganography is one such pro-security advancement in which mystery information is inserted in a spread. There are many different protocols and embedding techniques that enable us to hide data in a given object. However, all of the protocols and techniques must satisfy a number of requirements so that steganography can be applied correctly the following is a list of main requirements that steganography techniques must satisfy:

1.2 Types of Steganography

- **Text Steganography:** Text steganography can be accomplished by changing the content arranging, or by modifying certain qualities of textual elements (e.g., characters). The objective in the configuration of coding techniques is to create modifications that are dependably decodable (even in the vicinity of clamor) yet generally confused to the perused. These criteria, dependable unraveling and minimum visible change, are to some degree clashing; thus lies the test in planning report stamping methods.
- **Image Steganography:** Concealing data inside pictures is a prominent procedure these days. A picture with a mystery message inside can undoubtedly be spread over the World Wide Web or in newsgroups.
- **Audio Steganography:** In audio steganography, mystery message is embedded into digitized sound signal which result slight adjusting of double arrangement of the relating audio record. There are a few routines are accessible for sound steganography. We are going to have a short presentation on some of them.
- **Video Steganography** : Despite the fact that BMP records are ideal for steganography utilization, they find themselves able to convey just little documents. So there is an issue, how to get sufficiently many documents to conceal our message, and what to do to peruse them in a right request? Great way out is to shroud data in a feature document, on the grounds that as we know, AVI records are made out of bitmaps, consolidated into one piece, which are played in right request and with fitting time crevice.
- **Protocol steganography::** The term protocol steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used.

1.3 Image Steganography Classifications

Generally image steganography is categorized in following aspects and the best steganography measures.

- **High Capacity:** Maximum size of information can be embedded into image.
- **Perceptual Transparency:** After hiding process into cover image, perceptual quality will be degraded into stego-image as compare to cover-image.
- **Robustness:** After embedding, data should stay intact if stego-image goes into some transformation such as cropping, scaling, filtering and addition of noise.
- **Temper Resistance:** It should be difficult to alter the message once it has been embedded into stego-image.

- **Computation Complexity:** How much expensive it is computationally for embedding and extracting a hidden message?

1.4 Steganography Techniques

- **Spatial Domain Techniques:** There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible for human eyes. Spatial domain techniques are broadly classified into:

1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding method (EBE)
4. Random pixel embedding method (RPE)
5. Mapping pixel to hidden data method
6. Labeling or connectivity method
7. Pixel intensity based method
8. Texture based method
9. Histogram shifting methods

Advantages of spatial domain LSB technique are:

1. There is less chance for degradation of the original image.
2. More information can be stored in an image.

- **Transform Domain Technique:** This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Most of the strong steganography systems today operate within the transform domain. Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and loss format conversions. Transform domain techniques are broadly classified into:

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).
4. Lossless or reversible method (DCT)
5. Embedding in coefficient bits

- **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. Message may be scrambled or packed before stowing away. A pseudo random number generator may be utilized to spread the mystery message over the spread in an irregular way. This is a simple strategy yet is defenseless against debasement because of little changes in bearer.
- **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. In this way it is hard to evacuate the message totally without altogether devastating the spread. It is an exceptionally strong method that discovers application in military correspondence.
- **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. This strategy is not utilized as a part of numerous applications on the grounds that the decoder must have entry to the first cover.
- **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. This technique is difficult to apply because a good test must be found that allows for proper distinction between modified and unmodified cover blocks.
- **Protection of Data Alteration:** We exploit the delicacy of the inserted information in this application zone. Getup. 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. In the event that manufactured, modified, or altered, it is effectively located by the extraction program Protection of Data Alteration.

II. RELATED WORK

Tiwari et al. [1] “Color Guided Color Image Steganography” Author want to propose that most of the data hiding methods in image steganography used a technique utilizing the Least Significant Bits (LSB) of the pixels, i.e. the LSB of each pixel is replaced to hide bits of the secret message. This, normally, produce changes in the cover media but with no significant effect. All the LSBs of pixels of cover image can be used for hiding the secret bits. The hidden information can easily be uncovered using many known statistical steganalysis techniques, such as the X2 that can detect the concealed data inside the image with its original size.

Marwaha et al. [2] “Pixel Indicator High Capacity Technique for RGB Image Based Steganography” in this paper author want to say that the multimedia steganocryptic system, the message will first be encrypted using public key encryption algorithm, and then this encrypted data will be hidden into an image file thus accomplishing both data encoding and hiding. The multimedia data will be used to provide the cover for the information. Each color in the multimedia data when considered as an element in an arrangement of 3D matrix with R, G and B as axis can be used to write a cipher (encoded message) on a 3D space. The method which we will use to map the data is a block or a grid cipher. This cipher will contain the data which will be mapped in a 3-D matrix form where the x-axis can be for R (red), y-axis can be for G (green) and z-axis can be for B (blue). Embedding data into an image often changes the color frequencies in a predictable way and also gives redundancy in formats like bmp.

Gutub et al. [3] “Pixel Indicator Technique for RGB Image Steganography” in sequence, if the first indicator selection is the Red channel in the pixel, the Green is channel 1 and the Blue is the channel 2 i.e. the sequence is RGB. In the second pixel if we select, Green as the indicator, then Red is channel 1 and Blue is channel 2 i.e. the sequence is GRB. If in third pixel Blue is the indicator, then Red is channel 1 and Green is channel 2. The sequence of the algorithm is given below. The first 8 bytes at the beginning of the image are used to store the size of the hidden message, which is also used to define the beginning of the indicator channel sequence. These 8 bytes consumes all LSBs of the RGB channels, assuming it is enough to store the size of the hidden bits. To choose the first indicator channel, the size stored in the first 8 bytes is used. The indicator choice is assumed as the first level, followed by the data hiding channels as second level.

Bailey and Curran [4] “Visual cryptographic steganography in images” Author described an image based multi-bit steganography technique to increase capacity hiding secrets in number of bits, i.e. Stego-1bit, Stego-2bits, Stego-3bits and Stego-4bits. Stego-1bit is the simplest of this, where it inserts the secret message data into one LSB (lower order bit) of the image pixels, which is undetectable. Hide and Seek is an example of this technique. Note that if this bit insertion is performed into the higher order bit (most significant bit), the value of the pixel will show a great detectable change spoiling its security. It is known that insertion of hidden bits into lowest order LSB in all color RGB channels of the image pixels is unnoticeable. In the Stego-2bits method two bits of lower order LSB in RGB image steganography is used; Stego-2bits doubled the capacity of message hiding with negligible security reduction.

Amirtharajan et al. [5] “An evaluation of image based steganography methods” Author use one component case: here we have 3 ways to determine the bits * 3 ways to decide the component R, G or B. this results in 9 cases. Using two component case: here we have 3 ways to determine the bits * 3 ways to decide the component RG, RG or GB. This results in 9 cases. Using three component case: here we have 3 ways to determine the bits * one way to decide the component which is RGB. This results in 3 cases. The average capacity ratio is around 1/7 or 14% of the original cover media size. The secret data is scattered throughout the whole image. Also, extracting the secret data without the knowledge of seeds is almost impossible.

The capacity of the triple technique is higher than the previous techniques. By using this algorithm, the ratio between the number of bits used inside a pixel to hide part of the secret message; and the number of bits in the pixels itself, which is defined as the capacity factor can be in the range from 1/24 to 9/24 if we use a maximum of 3 bits. Moreover, if we extend the algorithm to hide 4 and even 5 bits the factor can be increased up to 15/24 which is above half of the pixel bits, but the down side is the additional noise introduced as the number of bits used to hide the secret data increase.

III. PROBLEM FORMULATION

Steganography is an excellent means of conversing covertly if there are guarantees on the integrity of the channel of communication[1]. It is not even necessary for the two parties to agree to a specific hiding format. 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. The Different encryption format can be agreed by the two persons in such a way that no one can find the information from the video. Each technique can be implemented easily, but if someone tries to find out the tricks after knowing that someone using the stego-video file, then there are good chances of finding out the hidden information.

In order to avoid this, the some hybrid system is used, in such a way that even though someone finds out the one technique, it is used only on few frames and other frames contains different kind of steganography and hence total secrete message is not delivered. Due to these embedding the video Steganography get dispersed using different types. In Video Steganography data encrypted behind the least significant bits of video frame. 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. 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. Size of embedded data can be reduced by performing compression to stego video file.

IV. METHODOLOGY

In the first step of embedding the data we firstly select the secret image and then convert that secret image in the format of single vector.

That single vector contains the no of bits that has to be embedded in the video file. In this step video data is loaded and that video data has to be used for the purpose of hiding the secret data into the cover video if the size of the frame of a video is lesser than size of the secret message then another video has to be selected.

In this step video data is divided into number of frames and on the basis of these frames this data has to be divided in the different color regions.

These regions used for the extraction of multiple least significant bits of the color components. These bits used for the secret data information to be embedded. After embedding the data different frames of the video file have to be merged to restore the video data. This recovered video contains secret information embedded in it which has to be used.

V. RESULTS

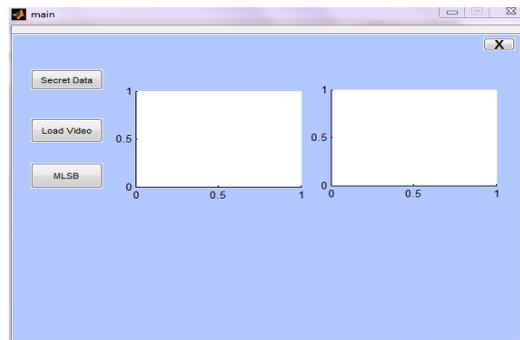


Figure 5.1: GUI

This graphical user interface is representing the process of steganography Buttons and axes are used to display images and perform functions. In the above GUI three buttons and two axes are displayed .Secret data button will upload the secret data on first axis. Load video will upload the video on the second axis. MLSB button will perform the MLSB Operation on image and video as well. MLSB will take the MLSB most least significant bits of the image and embed these into the video.

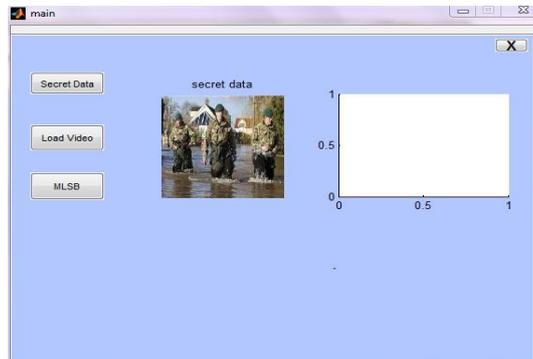


Figure 5.2: Upload Secret Data

Secret data button has uploaded the secret data on first a

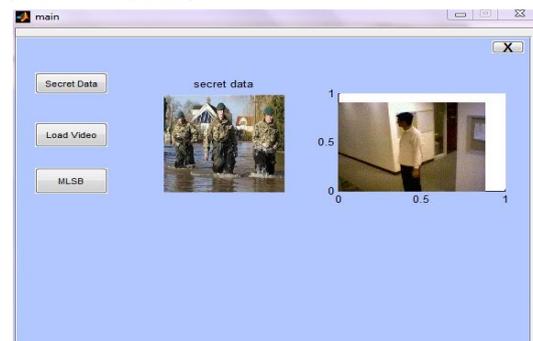


Figure 5.3: Video is uploaded

Video is uploaded on the second axis.

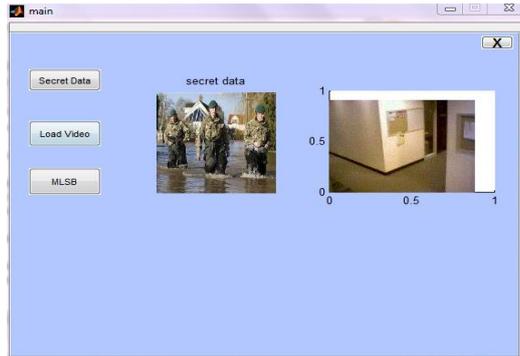


Figure 5.4: Apply MLSB operation

MLSB button has performed the MLSB Operation on image and video as well. MLSB will take the MLSB most Least significant bits of the image and embed these into the video. Now the video is called stego video.

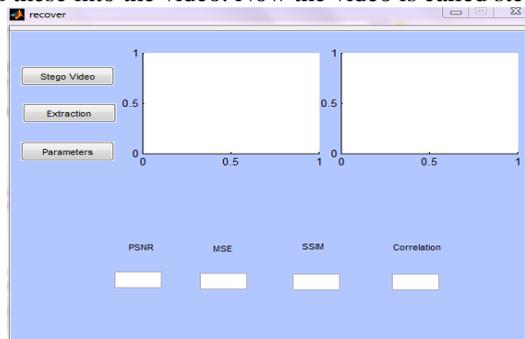


Figure 5.5: Apply Extraction Process

This is another GUI here the extraction process is started stego video button will upload the stego video on the first axis. Extraction will mine the secret image from the video. Parameters like PSNR, MSE, SSM and correlation are calculated from the whole process.

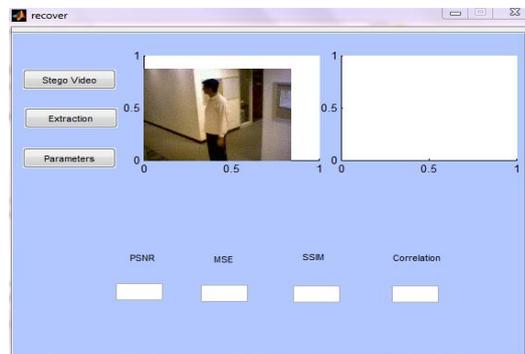


Figure 5.6: Upload Stego Video

Stego video is uploaded on the first axis.

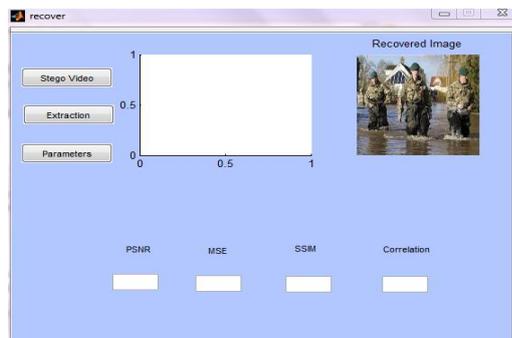


Figure 5.7: Recovered Image

Extraction will mine the secret image from the video. Now the image is named as recovered image.

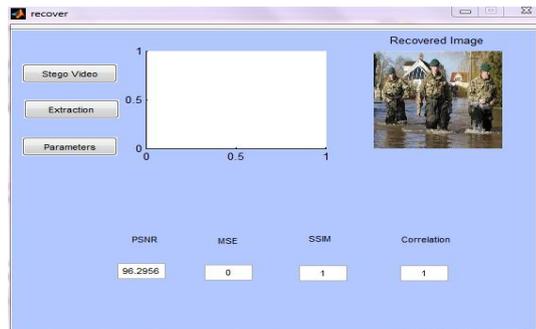


Figure 5.8: Parameteres Analysis

Parameters like PSNR, MSE, SSM and correlation are calculated from the whole process. Their values are displayed in the respective fields.

VI. CONCLUSION

Steganography is characterized as the craft of hiding data, information or messages in a picture. In this Video Steganography is used. This is used by MLSB. 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. In Video Steganography data encrypted behind the least significant bits of video frame. 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. 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 remove this problem occurred in video Steganography various types of approaches has been studied and MLSB is taken as most appropriate approach for embedding of data. Size of embedded data can be reduced by performing compression to stego video file.

REFERENCES

- [1] Behera, S.K. "Colour Guided Colour Image Steganography", Universal Journal of Computer Science and Engineering Technology, Vol. 1, No. 1, pp. 16-23, IEEE, 2010.
- [2] Gutub, A. "Pixel Indicator High Capacity Technique for RGB Image Based Steganography", WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, U.A.E., pp. 154-159, IEEE, 2008.
- [3] Gutub, A. "Pixel Indicator Technique for RGB Image Steganography", Journal of Emerging Technologies in Web Intelligence, Vol. 2, No.1, pp. 193-198, IEEE, 2010.
- [4] Marwaha, P. "Visual cryptographic steganography in images", Second International conference on Computing, Communication and Networking Technologies, pp. 34-39, IEEE, 2010.
- [5] Bailey, K. "An evaluation of image based steganography methods", Journal of Multimedia Tools and Applications, Vol. 30, No. 1, pp. 55-88, IEEE, 2006.
- [6] Mahata, S.K. "A Novel Approach of Steganography using Hill Cipher", International Conference on Computing, Communication and Sensor Network (CCSN), pp 0975-888, IEEE, 2012.
- [7] Chapman, M. Davida G, and Rennhard M. "A Practical and Effective Approach to Large Scale Automated Linguistic Steganography" found online at <http://www.nicetext.com/doc/isc01.pdf>.
- [8] Mehboob, B. "A steganography implementation", Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium, ISSN 978-1-4244-2427-6, pp 1 – 5, IEEE, 2008.
- [9] Saravanan, V. "Security issues in computer networks and steganography", Intelligent Systems and Control (ISCO), 2013 7th International Conference, ISSN 978-1-4673-4359-6, pp 363 – 366, IEEE, 2013.
- [10] Moon, S.K. "Data Security Using Data Hiding" Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference, ISSN 0-7695-3050-8, pp 247 – 251, IEEE, 2007.