



## An Approach for Video Steganography Using Multiple Least Significant Bits

Jaspreet Kaur, Naveen Kumari

Punjabi University Regional Centre for Information Technology and Management  
Punjab, India

*Abstract- Video steganography comprises of the hiding the secret information behind the cover object. Using this frames have been used for the hiding the secret information. This paper includes the various approaches that have been used for hiding the secret information behind different cover object and the purposed work that represent the hiding the information behind the cover video using the multiple least significant bits. In this Proposed System most of the tools are checking for information hided by LSB, DCT, Frequency Domain Analysis etc and finds whether the video has hidden or secret data or not. In this Proposed System LSB and Random Byte Hiding techniques are implemented and MATLAB based implementation is done to simulate the results*

*Keywords— Steganography, LSB, ISB, Frequency Domain Analysis ,DCT, Random Byte Hiding*

### I. INTRODUCTION

#### 1.1 Steganography

Steganography is the workmanship and exploration of imperceptible correspondence. This is refined through concealing data in other data, hence concealing the presence of the conveyed data. The word steganography is gotten from the Greek words "stegos" signifying "spread" and "grafia" signifying "written work characterizing it as "secured composition". In picture steganography the data is shrouded solely in pictures. The idea and practice of hiding information has a long history. In *Histories* the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message. In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

#### 1.2 Different kind of Steganography:

**1.2.1 Text steganography:** Concealing data in content is the most imperative technique for steganography. The system was to conceal a mystery message in each nth letter of each expression of an instant message. In the wake of blasting of Internet and diverse kind of computerized record positions it has diminished in significance. Content steganography utilizing advanced documents is not utilized regularly in light of the fact that the content records have a little measure of excess information [9].

**1.2.2 Image steganography:** Pictures are utilized as the well known spread items for steganography. A message is inserted in an advanced picture through an implanting calculation, utilizing the mystery key. The subsequent stego picture is Send to the recipient. On the other side, it is prepared by the extraction calculation utilizing the same key. Amid the transmission of steno picture unauthenticated persons can just notice the transmission of a picture yet can't figure the presence of the shrouded message.

**1.2.3 Audio stenography:** Audio stenography is covering, which misuses the properties of the human ear to shroud data unnoticeably. A perceptible, sound can be indiscernible in the vicinity of another louder capable of being heard sound .This property permits to choose the direct in which to shroud data [8].

**1.2.4 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 Applications of Steganography

1. Steganography can be an answer which makes it conceivable to send news and data without being edited and without the apprehension of the messages being blocked and followed back to us.
2. It is likewise conceivable to just utilize steganography to store data on an area. For instance, a few data sources like our private saving money data, some military insider facts, can be put away in a spread source. When we are obliged to

unhide the mystery data in our spread source, we can without much of a stretch uncovers our managing account information and it will be difficult to demonstrate the presence of the military privileged insights inside [3].

3. Steganography can likewise be utilized to execute watermarking. Despite the fact that the idea of watermarking is not so much steganography, there are a few steganography procedures that are being utilized to store watermarks in information. The fundamental contrast is on goal, while the motivation behind steganography is concealing data, watermarking is only developing the spread source with additional data. Since individuals won't acknowledge perceptible changes in pictures, sound or feature documents in view of a watermark, Steganography techniques can be utilized to conceal this.

4. E-business takes into account an intriguing utilization of steganography. In current e-trade exchanges, most clients are secured by a username and secret word, with no genuine technique for confirming that the client is the real card holder. Biometric unique mark checking, joined with special session IDs inserted into the finger impression pictures by means of steganography, take into account an exceptionally secure alternative to open ecommerce exchange confirmation.

5. Paired with existing specialized techniques, steganography can be utilized to do shrouded trades. Governments are keen on two sorts of shrouded correspondences: those that bolster national security and those that don't. Computerized steganography gives boundless potential to both sorts. Organizations may have comparable concerns Regarding prized formulas or new item data.

## II. LITERATURE REVIEW

**Tiwari et al. [1]** "Color Guided Color Image Steganography" Author want to propose that the vast majority of the information concealing routines in picture steganography utilized a system using the Least Significant Bits (LSB) of the pixels, i.e. the LSB of every pixel is supplanted to conceal bits of the mystery message. This, ordinarily, deliver changes in the spread media however with no huge impact. All the LSBs of pixels of spread picture can be utilized for concealing the mystery bits. The shrouded data can undoubtedly be revealed utilizing numerous known measurable steganalysis procedures, for example, the X2 that can distinguish the disguised information inside the picture with its unique size

**Marwaha et al. [2]** "Pixel Indicator High Capacity Technique for RGB Image Based Steganography" in this paper author want to say that the sight and sound steganocryptic framework, the message will first be scrambled utilizing open key encryption calculation, and after that this scrambled information will be covered up into a picture record accordingly finishing both information encoding and stowing away. The media information will be utilized to give the spread to the data. Every shading in the sight and sound information when considered as a component in a plan of 3D network with R, G and B as pivot can be utilized to compose a figure (encoded message) on a 3D space.

**Gutub et al. [3]** "Pixel Indicator Technique for RGB Image Steganography" in arrangement, if the first pointer determination is the Red directs in the pixel, the Green is channel 1 and the Blue is the channel 2 i.e. the succession is RGB. In the second pixel on the off chance that we select, Green as the marker, then Red is channel 1 and Blue is channel 2 i.e. the arrangement is GRB. On the off chance that in third pixel Blue is the pointer, then Red is channel 1 and Green is channel 2. The succession of the calculation is given underneath. The initial 8 bytes toward the start of the picture are utilized to store the measure of the concealed message, which is additionally used to characterize the start of the pointer channel arrangement. These 8 bytes expends all LSBs of the RGB channels, expecting it is sufficient to store the span of the shrouded bits. To pick the first marker channel, the size put away in the initial 8 bytes is utilized. The marker decision is accepted as the first level, trailed by the information concealing channels as second level. Each of the six conceivable determinations are acquired from the length of message (N), which will control the grouping.

**Bailey and Curran [4]** "Visual cryptographic steganography in images" Author described an picture based multi-bit steganography method to expand limit concealing privileged insights in number of bits, i.e. Stego-1bit, Stego-2bits, Stego-3bits and Stego-4bits. Stego-1bit is the most straightforward of this, where it embeds the mystery message information into one LSB (lower request bit) of the picture pixels, which is imperceptible. Find the stowaway is a case of this method. Note that if this bit insertion is performed into the higher request bit (most huge bit), the estimation of the pixel will demonstrate an awesome distinguishable change ruining its security. It is realized that insertion of concealed bits into most reduced request LSB in all shading RGB channels of the picture pixels is unnoticeable. In the Stego-2bits technique two bits of lower request LSB in RGB picture steganography is utilized; Stego-2bits multiplied the limit of message covering up with irrelevant security decrease.

**Amirtharajan et al. [5]** "An evaluation of image based steganography methods" Author use one part case: here we have 3 approaches to focus the bits \* 3 approaches to choose the segment R, G or B. this outcomes in 9 cases. Utilizing two part case: here we have 3 approaches to focus the bits \* 3 approaches to choose the segment RG, RG or GB. This outcome in 9 cases Utilizing three segment case: here we have 3 approaches to focus the bits \* one approach to choose the segment which is RGB. This outcome in 3 cases. The normal limit proportion is around 1/7 or 14% of the first cover media size. The mystery information is scattered all through the entire picture. Additionally, extricating the mystery information without the learning of seeds is verging on incomprehensible. The limit of the triple procedure is higher than the past systems. By utilizing this calculation, the proportion between the quantity of bits utilized inside a pixel to conceal piece of the mystery message; and the quantity of bits in the pixels itself, which is characterized as the limit component can be in the extent from 1/24 to 9/24 in the event that we utilize a greatest of 3 bits. Besides, in the event that we extend the calculation to conceal 4 and even 5 bits the variable can be expanded up to 15/24 which is above a large portion of the pixel bits, however the drawback is the extra commotion presented as the quantity of bits used to shroud the mystery information increment.

### III. PROPOSED WORK

In the Purposed work video data has been used as cover object for hiding the secret information. Frames from the video have been extracted by using the video reader function. These frames have been collected for extraction of three different color regions that red, green and blue. These true colors have been used for hiding the secret information. The multiple least significant bits have been computed from three different color regions. Secret information that has to be embedded behind the cover object has been converted into the binary format and the XOR operation has been used for embedding the information behind the cover object. These frames have been recombined after embedding of secret information behind the cover object. The frame that has been recombined that provides stego video that can be transmitted to the receiver side for extraction of secret information.

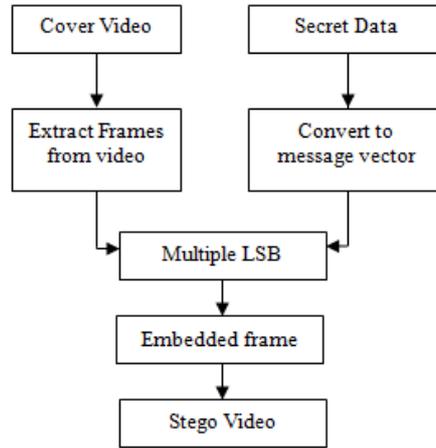


Fig 3.1 Flow for embedding secret information

This figure represents the flow for embedding the secret information behind different frames of video file.

Algorithm flows for purposed work to hide the secret data behind the multiple least significant bits of the video frames have been explained below:

Read Cover video and identify the frame size (R ×C)

1. Divide the cover video into frames and compute frame size and number of frames.
2. Read the secret data and reshape the secret message into vector form.
3. Extract the frames from the video and compute multiple least significant bits available.
4. Embedded the vector message to the nits of the video frames using XOR operation.
5. Repeat the step 4 and 5 until all the bits of the message has been embedded
6. Integrate the frames at a particular frame speed to reconstruct the video.

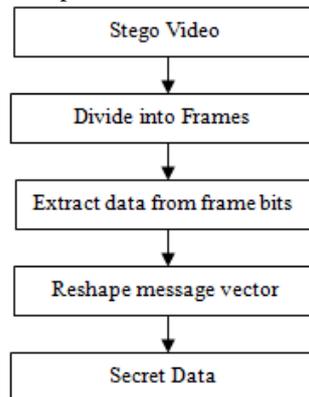


Fig 3.2 Flow for Extraction of secret information

This figure represents the flow for extraction of the secret message from the video frames.

Algorithm flow for extraction of the data has been represented as described below

1. Read stego video.
2. Extract the frame from the video.
3. Separate the data from the frames by multiple least significant bits.
4. Repeat step 3 until all the data has been extracted.
5. Reshape the message to form secret message.

### IV. RESULTS AND DISCUSSIONS

In the purposed work the video files that are in AVI format have been used for steganography. These files have been read by using the function and size of the frames, number of frames and duration has been computed. The images have been used for hiding behind the frames of the video.

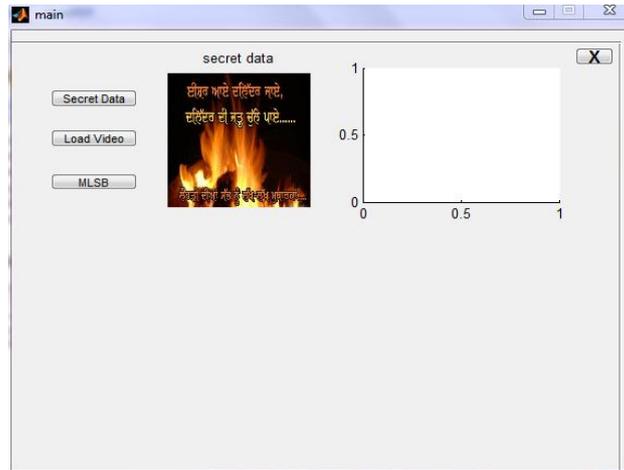


Fig 4.1 Input of Secret Information

This figure represents the secret information has been loaded from the user that has to be hiding behind the cover object. The input secret information is RGB in the format. The image can be of PNG, JPEG and BMP format.



Fig 4.2 Cover Video for embedding

This figure represents the cover video that has been selected for secret information to be hide behind the cover object. In this the three color region from the video has been extracted and the least significant bits from all these regions have been computed. The secret information has been hide behind these bits using XOR operation.

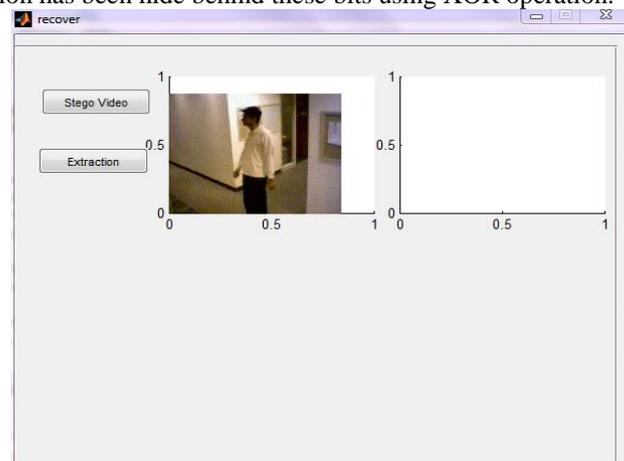


Fig 4.3 Loading of stego video at receiver end

This figure represents the stego video that has been developed after the processes of embedding of secret information behind the cover object. This video has been loaded at receiver end for extraction of the secret data that has been embedded behind this.

This information has been extracted by using the three sub regions of the pixels that have been computed on the basis of least significant bits

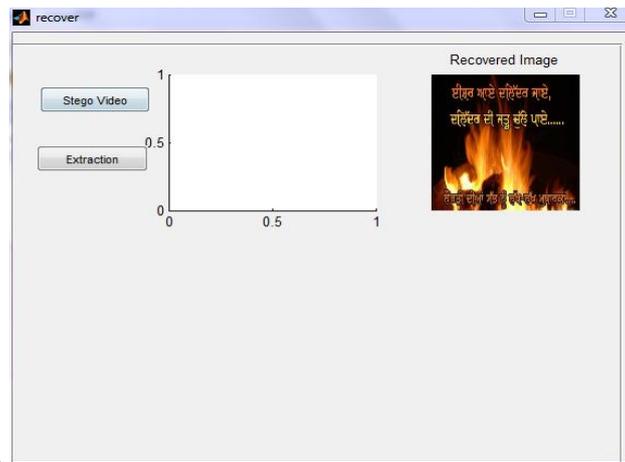


Fig 4.4 Secret Data after extraction from video

This figure represents the data that has been extracted from the video that has been hiding by the user for secure transmission the data. Data can be further goes for checking of integrity.

Table 5.1 parameters values for video steganography

Video	PSNR (dB)	MSE
Video1	55.95	0.156
Video2	50.36	0.169
Video3	60.12	0.25
Video4	58.25	0.14
Video5	65.21	0.1

This table represents the value of PSNR, MSE for video steganography. The values of these parameters have been computed for performance evaluation of the purposed work

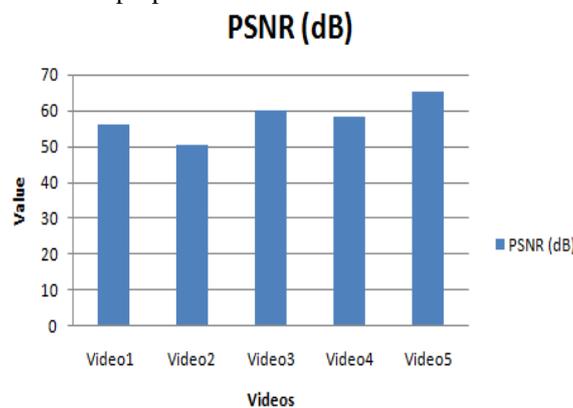


Fig 5.5 PSNR for video steganography

This graph represents the values of the PSNR for different videos that have been used for video steganography

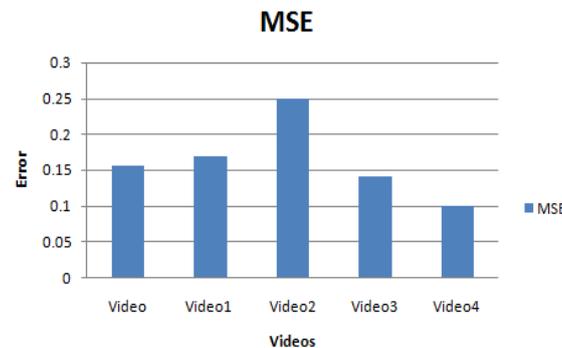


Fig 5.6 MSE for video steganography

This graph represents the values of the mean square error for different videos that have been used for video steganography

## V. CONCLUSION

Video steganography is the process for hiding the secret information behind the different pixels of the cover object. The frames of the video have been extracted. After extraction the secret information has been converted into the vector form that has been used for hiding the information. In this the least significant bits have been computed from all the regions of the video frames. The data has been embedded behind these significant bits using the embedding approach. After this all the frames have been reconstructed at a frame speed so that video can be reformed and transmit to the receiver. This approach used for video steganography provides much better results because the data can be hidden in large quantity and the attacker cannot extract data easily because he has no information about the frame in which data has been embedded.

## REFERENCES

- [1] Behera, S.K. "Color Guided Color 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.