ISSN: 2277 – 9043
International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE)
Volume 4, Issue 8, August 2015

Steganography Over Video Files Using Multiple Least Significant Bits

Jaspreet Kaur, Naveen Kumari

***Abstract*-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[4]. 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. 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 techniques like DCT[1] and hence total secrete message is not delivered. Due to these embedding the video Steganography get dispersed using different types[9]. LSB & MLSB approach is used for embedding of data.**

***Index terms*:- DCT,LSB,MLSB ,Video Steganography.**

I. INTRODUCTION

1.1 Steganography: Steganography hides the secretive message however not the way that two gatherings are corresponding with one another. The steganography handle for the most part includes setting a shrouded message in some vehicle medium, called the transporter. The mystery message is inserted in the transporter to structure the steganography medium. The utilization of a steganography key may be utilized for encryption of the concealed message and/or for randomization in the steganography plan.

1.2 Types of Steganography:

1.2.1 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.

1.2.2 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. The utilization of steganography in newsgroups has been inquired about by German steganographic master Niels Provos, who made a filtering bunch which distinguishes the vicinity of concealed messages inside pictures that were posted on the net[9].

1.2.3 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

1.2.4 Video Steganography: Despite the fact that BMP records are ideal for steganographic 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. Remembering that we should simply to get out is record single edges and spares them as BMP records. In the event that we'll utilize calculation for concealing information as a part of computerized pictures, we can conceal our message in bitmap got along these lines, and afterward spare it into new AVI record. We'll break down just uncompressed AVI record, on the grounds that if any pressure is executed documents lose its information.[1]

AVI documents are made out of few streams. Fundamental document stream is a feature stream and sound stream, which can be record of any augmentation, for instance WAVE. In view of presence of those streams, it is conceivable to conceal information in record's casings as well as in said sound stream. Because of this we can consolidate chances of concealing information in advanced pictures and in sound records.

1.3 Steganography Techniques[3]

1.3.1 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 .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[3].

Manuscript received Sep , 2015.
Jaspreet Kaur, Punjabi University Regional Center for Information Technology and Management Ludhiana,9779506350
Mrs.Naveen Kumari (Assistant Professor) Punjabi University Regional Center for Information Technology and Management Mohali.

1.3.2 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. 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[3].

1.3.3 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[3].

1.3.4 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. This strategy is not utilized as a part of numerous applications on the grounds that the decoder must have entry to the first cover[3].

1.3.5 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. This technique is difficult to apply because a good test must be found that allows for proper distinction between modified and unmodified cover blocks[3].

2. LITERATURE SURVEY

Ashish & T. Bhole et al [1] Author presented that Steganography was an art of hiding the secret information inside digitally covered information. In this paper, the hidden message was text and it was implemented over video file. The traditional well known method uses image as cover which had the limitation of embedding dimension. So, cover should be a video to overcome the limitation of embedding dimension. the use of a video based steganography was common and numbers of steganalysis tools were available to check whether the video was stego-video or not. Most of the tools were checking for information hided by LSB, DCT, Frequency Domain Analysis etc and finds whether the video had hidden or secret data or not. LSB and Random Byte Hiding techniques were implemented and MATLAB based implementation is done to simulate the results.

Jinsuk Baek et al [2] Author proposed that in this paper it utilized some simple observed relationships between the binary representation of a pixel, the gray code representation, and the utilization of a simple Exclusive-OR operation based upon N images available to the sender and the receiver, called the cover images. It presented the algorithms for embedding the secret data in the altered, last image, N+1, called the stego image; as well as extracting this data on the receiving side. It presented some experimental images utilizing two cover images, and one stego image and show that the procedure that proposed had a high PSNR value, and an almost identical histogram when compared to the before stego image. In this paper it also discussed the robustness of this algorithm under attack methods such as steganalysis.

Moon & S.K et al [3] Author explained that in this it used the least significant bit (4LSB) substitution method. By using this proposed algorithm, everyone can hide our file of any format in an image and audio file. After that send the image via e-mail attachment or post it on the web site and anyone with knowledge that it contains secret information, and who is in possession of the encryption password, will be able to open the file, extract the secret information and decrypt it.

Saravanan et al [4] Author discussed that this paper reduces the detectable distortion in a joint photographic experts group (JPEG) file during data hiding process, by introducing new region selection rule. The new region selection rule considers three factors, i.e., the horizontal difference (HD), vertical difference (VD) and region size (RS). The JPEG image will be split into number of blocks and each pixel in it will be examined to calculate the variations. Depends upon the variation, the amount of secret information will be hide in an image. This proposed method of information hiding will help to solve the security issues in computer networks. The experimental result says that, the proposed system hides approximately 45% of secret information in addition, comparing existing methods without increasing detectable distortion.

Gutub et al [5] Author proposed that the first 8 bytes at the beginning of the image were used to store the size of the hidden message, which was also used to define the beginning of the indicator channel sequence. These 8 bytes consumes all LSBs of the RGB channels, assuming it was enough to store the size of the hidden bits. To choose the first indicator channel, the size stored in the first 8 bytes was used. The indicator choice was assumed as the first level, followed by the data hiding channels as second level. All six possible selections were obtained from the length of message (N), which will control the sequence, i.e. if N was even; the indicator channel was R, leaving an option of RGB or RBG based on the parity bit of N. Similarly, if N was a prime number, Chanel B was considered as the indicator leaving R and G for data hiding. If N value was neither even nor prime, "else" row was chosen, selecting the indicator to be G and the channels R and B were for secret data holding.

3. METHODOLOGY

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

4. ALGORITHM USED

MLSB: Multiple Least Significant Bit (MLSB) embedding is a simple strategy to implement steganography. Like all steganography methods, it embeds the data into the cover so that it cannot be detected by a casual observer. The technique works by replacing some of the information in a given pixel with information from the data in the image. While it is possible to embed data into an image on any bit-plane, MLSB embedding is performed on the least significant bit(s). This minimizes the variation in colors that the embedding creates. Embedding into the second bit-plane can change the color value by 2. If embedding is performed on the least significant two pixels, the result is that a color in the cover can be any of four colors after embedding. Steganography avoids introducing as much variation as possible, to minimize the likelihood of detection. MLSB embedding always lose some information from the cover image. This is an effect of embedding directly into a pixel. To do this we must discard some of the cover's information and replace it with information from the data to hide. MLSB algorithms have a choice about how they embed that data to hide. They can embed lossless, preserving all information about the data, or the data may be generalized so that it takes up less space.

DCT (Direct Cosine Transform): A discrete cosine transform (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from loss compression of audio to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical for compression, since it turns out (as described below) that fewer cosine functions are needed to approximate a typical signal, whereas for differential equations the cosines express a particular choice of boundary conditions. DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and/or output data are shifted by half a sample. There are eight standard DCT variants, of which four are common.

5. RESULT & DISCUSSION

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

Table 5.1 represents the value of PSNR,MSE for video steganography. The values of these parameters have been computed for performance evaluation of proposed work. The values of these parameters are computed by formulas of PSNR and MSE.

Table 5.2 Table representing PSNR values of previous and proposed work

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

Table 5.2 represents PSNR values of previous and proposed work. On comparing the results of previous approach used and proposed approach we conclude that the PSNR in proposed approach gives better results than the previous one by using Multiple Least Significant Bits.In the previous work , the techniques which is used for this is Least Significant bits.But in the proposed work we can used Multiple Least Significant Bits for video steganography

The Multiple Least Significant bits approach gives the better results than the Least Significant Bits .

Table 5.3 Table representing MSE values of previous and proposed work

Video	MSE (Proposed)	MSE (Previous)
Video1	0.156	0.45
Video2	0.169	0.356
Video3	0.25	0.78
Video4	0.14	0.65
Video5	0.1	0.9

Table 5.3 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.

5. CONCLUSION

Video steganography is the process for hiding the secret information behind the different pixels of the cover object. 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. Main problem arises due to embedding behind least significant bits of video frames stegnalysis can be one easily on these frames to retrieved data. This does not provide security to secret dat. 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 steno video file. This approach used for video steganography provides much better results because the data can be hidden in large quantity and the attacker cannot extract easily data because he has no information about the frame in which data has been embedded.

REFERENCES

[1] Ashish T. Bhole, Rachna Patel , "Steganography over Video File using Random Byte Hiding and LSB Technique" *International Conference on Computational Intelligence and Computing Research, IEEE*, pp 1-6, 2012.

[2] Jinsuk Baek, Fisher, P.S. , Hongyang Chao "Secret sharing approach based on steganography with gray digital images", *IEEE International Conference on Wireless Communications, Networking and Information Security*, pp. 325 – 329, 2010

[3] Moon, S.K, Kawitkar, R.S. "Data Security Using Data Hiding", *International Conference on Computational Intelligence and Multimedia Applications*, pp. 247 – 251, IEEE, 2007.

[4] Saravanan, Neeraja, A. "Security issues in computer networks and stegnography", *7th International Conference on Intelligent Systems and Control*, pp. 363 – 366, IEEE, 2013.

[5] Gutub, A. "Pixel Indicator Technique for RGB Image Steganography", *Journal of Emerging Technologies in Web Intelligence*, Vol. 2, pp. 193-198, IEEE, 2010.

[6] Samima, S, Roy,R. , Changder, S. "Secure key based image realization steganography" IEEE Second International Conference on Image Information Processing, pp. 377-382, 2013.

[7] Vineeta Singh, Priyanka Dahiya, Sanjay Singh "Smart Card Based Password Authentication and User Anonymity Scheme using ECC and Steganography" *International Conference on Advances in Computing, Communications and Informatics*, pp. 1614-1621, 2014.

[8] Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography" *3rd International Conference on Informatics, Electronics & Vision*, pp. 1-6, 2014.

[9] Bugár, G. , Broda, M. , Levický, D. "Data hiding in still images based on blind algorithm of steganography" IEEE *24th International Conference on Radio elektronika*, pp. 1-4, 2014.

[10] Akhtar, N, Khan, S., Johri, P. "An improved inverted LSB image steganography" *IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques*, pp. 749-755, 2014.