A COMPARATIVE STUDY OF LSB BASED VIDEO STEGANOGRAPHY TECHNIQUES

[1]IVIN AL-SALIHI, [2]SEMA KOC KAYHAN

University of Gaziantep, Gaziantep, Turkey.

Abstract- This study presents, a brief analysing of two different approaches for data embedding and extracting embedded data in a video files having an admirable quality. In these two approaches data encryption process are rebased on least significant bit (LSB) technique. The first method, improved LSB image steganography technique uses Bit-Inverse in 24 Bit colour image, and the second LSB image steganography approach uses RGB colour components and image patterns are compressed using weighted principal component. The performance and comparison of these two techniques are measured using Peak-to-Signal Noise Ratio (PSNR) and Mean Square Error (MSE) metrics. Our proposed approach tries to improve payload capacity of image steganography and provide more security to the stego video through using the RGB pixel component.

Keywords- Video steganography, LSB Insertion, MSE, PSNR.

I. INTRODUCTION

Steganography hides private or confidential data within a carrier in invisible manner. It is driving from the Greek word steganos, meaning covered or secret and graphy (writing or drawing) [1]. Cover medium is an object that contains data privately. This can be any type of files such as image, video, or an audio. Any stego algorithm eliminates the unneeded bits in the cover media and adds the secret information into the space. More unneeded bits can be generated and then hidden due to the higher quality of video or sound. Military, industrial and intellectual property rights (IPR) are applications of Steganography. Lossless steganography is a technique that sends and receives messages securely which was based historically on hiding information in image type files[2]. However, recent work suggests applying steganographic techniques to video files similarly[3,4]. In order to prevent the attack of hacker of video files that are exit in the hiding information. The advantage of video files over image files in hiding information can be due to the fact that video files are more secure against the attack of hacker and that is because of the complexity of its structure. video steganography has various benefits to society that was applied to many fields including; digital watermarking, feature tagging, smart card to embed personal detail of person (verification purposes), biometrics (hiding fingerprints detail and voice for recognition), secret communication in military base, and by computer forensics (detecting fake video files and cybercriminals) [5].

Embedding and extraction process are the two phases that are video steganography based on. In the embedding phase, secret data are hidden inside the video utilizing a range of embedding algorithms. This procedure can be conducted by the sender side. On the other hand, extraction phase is conducted by the receiver side and only authorized users are capable to extract secret message using Stego key. These users have to be known to the sender and receiver in order to increase the security of hidden data from hackers. This is the reverse process of embedding phase.

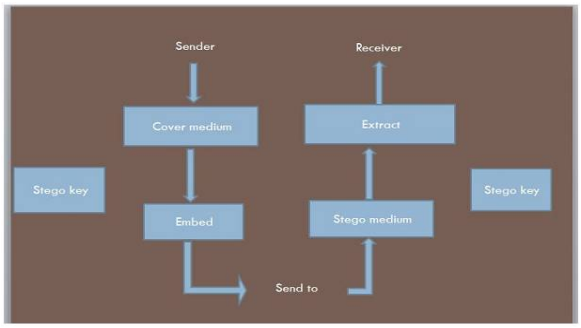


Figure 1: steganography mechanism.

In video steganography technique least significant bit is commonly used to hide data in video cover files due to its simplicity. In this technique from video particular frames selected in which text will embedded or hided in that frames by using bit of each of the Red, Green and Blue color components can be used. The RGB component consist of 24 bits values for each pixel. It is very suitable as it contains a lot of information which can be very helpful in hiding the secret information with a bit change in the frame resolution in a way that does not affect the video quality and protect the message from hackers. This technique brings simplicity in LSB insertion technique in addition reduces the attacks from third party. In the present paper two approaches[6][7] for video steganography are implemented with the assistance of MATLAB, and to assess the quality of video sequences PSNR and MSE error parameters for both approaches are utilized.

II. LEAST SIGNIFICANT BIT (LSB)

Least Significant Bit is the oldest and simplest technique that have been used for steganography.

Secret information is hidden into least significant bits of a byte representing an intensity value of a pixel [8]. The criterion of using only LSB or last two, three or four LSBs are based on the amount of data to be hidden and the importance of the secret data and also the type of cover video and frequency of the pixels used in a video. Therefore, best LSB steganography algorithm can be designed on the basis of the above parameters of a cover video and secret information that have to be hidden. The stego-video is the result after the secret message is embedding. The binary code below represents the process of message embedding in cover video.

Cover video Pixels:
00110011 11101001 01101010 10101001
11011000 10001101 10001100 01101101

Secret Message:
1 0 0 0 1 1 1 0

Result (Stego-video):
00110011 11101000 01101010 10101000
11011001 10001101 10001101 01101100

For RGB, a technique from [9] alternates the least significant bits of each pixel of Red, Green or Blue with the secret message bits. The result of the LSBs alternation causes minor changes in the RGB colors and therefore, it is difficult to be noticed by the human eye.

III. PROPOSED APPROACH

This proposed approach presents video steganography for data embedding and extracting embedded data in video files by using LSB (least significant bit) insertion technique. The technique implements two approaches for embedding data [6][7].The following sections illustrates these two techniques in details.

The Proposed Steganography Algorithm

The proposed algorithm for hiding secret message in an input video (AVI format) is implemented as follows:

- ✓ Read Input Image (host video) and Secret message file.
- ✓ Extract the video to frames.
- ✓ Select the frame for embedded code.
- ✓ Decomposition of input video into red, green and blue color component frames.
- ✓ Conversion of secret message into binary form.
- ✓ Sequencing each character (binary form) of message in single column matrix (array).
- ✓ Get the length of the binary array (character) or no. of bits to be embedded in Host video.
- ✓ Generate the random locations in host video equal in no. of bits to be embedded.
- ✓ Generate the two LSBs of first location pixel from red component frame and XOR with first bit of frame to be embedded.
- ✓ If the XOR result is ‘00’ or ‘11’, then exchange the red component pixel with bits to be embedded.

If XOR (RLSB, MB) = 10.
OR
If XOR (RLSB, MB) = 11.
Then, RLSB = MB
Where, MB = Message Bit.

- ✓ If the XOR result is ‘01’, then exchange the green component pixel with bits to be embedded.

If XOR (RLSB, MB) = 01.
Then, GLSB = MB.
Where, MB = Message Bit.

- ✓ If the XOR result is ‘10’, then exchange the blue component pixel with bits to be embedded.

If XOR (RLSB, MB) = 00.
Then, BLSB = MB.
Where, MB = Message Bit.

- ✓ Concatenate the R-, G- and B-component frames to get stego video.

Stego video = CAT (3, R, G, B.)

Evaluate the performance indices mean square error, peak signal to noise ratio values.
For Code Extraction, the inserted code can be extracted by taking the stego video as input video as well as extract frames from video. Similarly, it is spitted into its R-, G- and B-color constituents. The stego coordinates and xor value can be gained from the key file. These values are used to obtain the R-, G- and B-constituents color information to recover the Least Significant Bit (LSB) in order to change the binary sequence into ASCII code. The outcome of this process, is the message that was embedded using Least Significant Bit.

IV. THE PROPOSED BIT INVERSION TECHNIQUE

Least significant bit (LSB) inversion method is a process that inverses the bit of each pixel within the cover-video based on the values of the secret video. This standard LSB method can be completed when all secret messages’ bits are embedded or hidden in the cover-video. The proposed inversion technique based on the comparison between the cover-video (i.e., 2nd last and 3rd last bit) and the bits from the stego video, which can be obtained from applying the standard LSB method.

The step-by-step process of the proposed method is as follows:

- ✓ Calculate the pattern occurrences of these two bits on the cover-video, which are either 00, 10,

10, or 11. Classify the cover video according to these four patterns.

- ✓ Apply the standard LSB method to obtain the stego-video.
- ✓ From the stego-video, once again, calculate the pattern occurrences in the 2nd last and 3rd last bit of the stego-video. From these patterns, we use them as a guide for the inversion steps.
- ✓ Compare between each pattern from cover video with the same pattern in the stego-video.
- ✓ Inverse the LSB bits if the number of pixels that have been changed is greater than the number of pixel that has not change.
- ✓ Store the status of the patterns that inverse its pixel in specific location.

In order to recover the secret message from the stego-video, we need to save these patterns for which the corresponding LSB bit is inverted. Since we have checked all possible combinations of the 2nd and the 3rd bit of all pixels, we may need to store maximum of 4 patterns information in the stego video. Secret message that are exhibited in the stego-video can be recovered by storing these patterns for which the corresponding LSB bit is inverted. Therefore, in de-steganography, the information that guides us to the pixels patterns that has been inversed is to firstly read from the stego-video to be able to identify the inversed and non inversed patterns. After that, the stego-video is classified according to the four patterns and then re-inversing the bits to extract the massage bits.

V. SIMULATION AND RESULTS

The simulation results and performance of the proposed schemes are explained where the carrier object was the AVI format video in this simulation. The experimental platform was programmed in MATLAB version 7.9.0 R2009b. Since the steganography algorithm is meant for video sequence. Therefore, three different videos were examined for each approach[6,7]. The experiment was investigated by the code word of 696 bits. The videos that are used in this experiment were as: (baby.avi; size:14.6MB), (watermelon.avi; size: 48.2MB), (basketball.avi; size: 1.6MB) and the results are summarized in the blow figures (Figure 2 & 3). As shown the figures, a fair performance was observed by applying the code word.



Figure (2): Host (a1, b2 and c3) and Stego (a2, b2 and c2) videos based on Proposed steganography algorithm method



Figure (3): Host (a1, b2 and c3) and Stego (a2, b2 and c2) videos based on bit inversion algoithm method

VI. PEAK SIGNAL-TO-NOISE RATIO (PSNR)

In steganography technique, PSNR is the standard measurement that tests the quality of the stego video. PSNR defines a ratio that lies between the maximum possible power of a signal and the power of corrupting noise which can affect the fidelity of its representation [10]. In this case, the signal is corresponding to the cover-video, whereas the error that is introduced by the bits of the secret message represents the noise. The high quality of the stego-video can be evaluated by the higher value of PSNR. To demonstrate that, consider a cover video K of size M × M and the stego-video L of size N × N. Then, each cover-video K and stego-video L will have pixel values of (x, y) from 0 to M-1, and 0 to N-1 respectively [11]. The mean square error (MSE) which measures the average of the squares of the errors is calculated first. The results are then used to calculate the PSNR.

$$PSNR = 10 \log_{10} \frac{MAX^2}{MSE} \text{ (db)}$$

Where,

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (\alpha_{i,j} - \beta_{i,j})^2$$

Here, $\alpha_{i,j}$ is the pixel of the cover video where the coordinate is (i, j), and $\beta_{i,j}$ is the pixel of the stego-video where the coordinate is (i, j). M and N represent the size of the video. A large PSNR value points out that the variation between cover video and stego video is significantly considered unnoticed to the human being eye. Table 1 and 2, show the PSNR values for all cover video applied by both each approaches.

Table 1: PSNR and MSE of the first method

Proposed steganography algorithm		
Cover Video	MSE	PSNR
Baby.avi	0.0034426	72.7619
Watermelon.avi	0.0033834	72.8372
Basktball.avi	0.0034327	72.7744

Table2: PSNR and MSE of the second method

Bit inversion algorithm		
Cover Video	MSE	PSNR
Baby.avi	0.0034130	72.7994
Watermelon.avi	0.0037582	71.66344
Basktball.avi	0.0033933	72.8246

CONCLUSIONS

Two techniques have been implemented in the present study for embedding data in video files, using least significant bit (LSB) technique. These techniques, for hiding a particular text message in a video, hide it securely with minimum mean square error and as a result gives maximum PSNR. This will assist the transmittance of the data securely by embedding it in a video file and without disclosing to the unintended receiver and any alternation in secret message. In addition, this will increase the payload capacity with minimal distortions in the host video. Therefore, these techniques have good quality of invisibility and detect ability for the host video. Worth to mention that the goal of the techniques are not just to increase the capacity of the message but making it difficult to any unauthorized party to determine the presence of a secret message.

REFERENCES

[1] E. Cole and R.D. Krutz, "Hiding in Plain Sight: Steganography and the Art of Covert Communication", Wiley Publishing, Inc., ISBN 0-471-44449-9, 2003.

[2] Katzenbeisser and Fabien A. P. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House Books, ISBN 1-58053-035-4, 1999.

[3] D. Stanescu, M. Stratulat, B. Ciubotaru, D. Chiciudean, R. Cioarga and M. Micea, "Embedding Data in Video Stream using Steganography", 4th International Symposium on Applied Computational Intelligence and Informatics, SACI-2001, pp. 241-244, IEEE, 2007.

[4] Feng Pan, Li Xiang, Xiao-Yuan Yang and Yao Guo, "Video Steganography using Motion Vector And Linear Block Codes", IEEE 978-1-4244-6055-7/10/, pp. 592-595, 2010.

[5] Ramandeep Kaur, Pooja, "XOR Encryption Based Video Steganography", International Journal of Science and Research (IJSR), Vol.4, Issue 11, November 2015.

[6] Pooja Jain and Navdeep Kanwal, "Image Steganography in RGB Color Components using Improved LSB Technique Image Pattern Compression using Weighted Principal Components Algorithm", Indian Journal of Science and Technology, 9(45), 2016.

[7] Mohammed Abdul Majeed and Rossilawati Sulaiman, "An improved LSB image steganography technique using bit-inverse in 24 bit colour image", Journal of Theoretical and Applied Information Technology, 80(2), 2015, p.342-348.

[8] Sanjiv Manchanda, Mayank Dave and S. B. Singh, "Customized and Secure Image Steganography Through Random Numbers Logic". In Signal Processing: An International Journal, Volume 1: Issue (1).

[9] Chan, C.-K. and L.-M. Cheng, "Hiding data in images by simple LSB substitution. Pattern recognition", 37(3), 2014, p. 469-474.

[10] Rawat, D. and V. Bhandari, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image". International Journal of Computer Applications (0975–8887), 64(20), 2013.

[11] Wang, c.-m., et al., "A high quality steganographic method with pixel-value differencing and modulus function", Journal of systems and software, 81(1), 2008, p.150-158.

★★★