SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TNC TRANSACTIONS ON NETWORKS AND COMMUNICATIONS

VOLUME 4, ISSUE 6
ISSN: 2054 -7420

Multi-layers Video Steganography: A Novel Technique for Image Hiding

[1]Shadi A. Alhaj, [2]Ahmad M. Shaheen and [3]Talal M. Al-Kharoubi
[1]Information and Computer Science Dept., King Fahd University of Petroleum & Minerals, Saudi Arabia;
[2,3]Computer Engineering Dept., King Fahd University of Petroleum & Minerals, Saudi Arabia;
g201408500@kfupm.edu.sa; g201404320@kfupm.edu.sa; talalkh@kfupm.edu.sa

ABSTRACT

Steganography is hiding of a secret message within an ordinary message. Both secret and ordinary data can be of different type such as document, digital image or digital video. As videos are transmitted more frequently over the internet we imposed a large impact on video steganography. In this work, we are presenting a novel video steganography technique to hide greyscale image inside a colored video. Our proposed technique consists of five stages that take the 6 most significant bits from each pixel of the secret image and hide it in different layers in the cover video using the least significant 2 bits from each color in each pixel in the selected frame. We proposed a selection procedure of video frames to improve the technique security. The experimental results are promising.

Keywords: Video Steganography, data hiding, LSB, MSB, grayscale image.

1 Introduction

Recently, social media applications such as Instagram, Snapchat and other applications are being wildly used. These applications focus on images and videos as a main approach for digital communication. Also, images and videos have a pivotal role to transfer huge amount of data over the World Wide Web. "A picture is worth a thousand words" is an English idiom that describes the ability of images to carry abundant information. However, this poses a new challenge which is to secure confidential information embedded in images and videos. Therefore, numerous researches and applications have been developed to extract and analyze the embedded information inside an image or video. In addition, there are various techniques that use images and videos to hide secret information. Images and videos have an obvious advantage in hiding data due to the inability of the human eye to detect the infinitesimal differences between pixels. Images and videos are playing an important role in hiding data and information security.

Cryptography, Steganography and Watermark are three diverse techniques that are being used to secure information. These techniques are being extensively used in the digital world. Cryptography is a technique for securing communication and refers to hiding the content of the secret message by converting the message to an abstruse or unreadable format [1]. The digital watermark technique, which is capable of carrying secure information including authentication or authorization codes, has the main purpose of protecting the copyrights [2]. Another technique that can be used to hide secret information is

DOI: 10.14738/tnc.46.2529
Publication Date: 30th December 2016
URL: http://dx.doi.org/10.14738/tnc.46.2529

steganography which is defined as the art of hiding secret information within an ordinary message [3]. In this paper our prime concern is to secure information using steganography approach.

The word Steganography has a Greek origin and is a combination of two words "stegno" which mean "covering" and "graphein" which mean "writing". Today, steganography is being used as a secret communication method in the digital world to conceal the original information within another file such as document, image, video and etc.

The image steganography is an established technique and there are many researches that have already worked on image steganography and its decoding. Generally, the video is comprised of number of images (frames) with or without sound. Therefore, the video steganography can be regarded as an extension of image steganography [4]. Secure information embedded in a stenographic video has a lower probability of interpretation by unauthorized intruder as compared to image steganography. Also, the video steganography is preferred because of the ability to hide relatively large amount of information and thus imposing high security [5].

In this paper, we proposed a novel technique that uses steganography to hide a grayscale image inside a colored video. The robustness of our approach is by using different color layers from each frame. Each layer has been used to conceal a specific part of the secret image. In our approach, the least significant bits (LSBs) method have been used to secure the secret message.

In our approach, six most significant bits (MSBs) have been used to represent the secret image. The justification of using 6 MSBs can be found from Table 1. It can be observed from the table that as you move from MSBs to LSBs, the amount of information that is stored decreases and the last 2 bits contains negligible information.

Table 1- Information percentage contained by each bit in one pixel

Bit Index	Percentage of Information
0	0.392%
1	0.784%
2	1.568%
3	3.137%
4	6.274%
5	12.549%
6	25.098%
7	50.196%

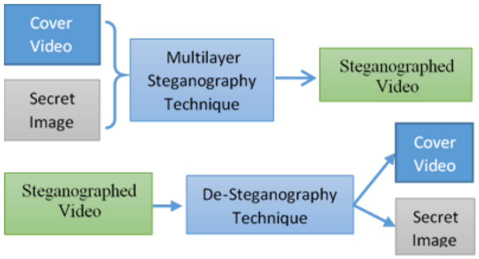


Figure 1 - Multilayer Steganography and De-Steganography Process

Figure 1. Illustrates our technique that is being used to hide an image inside the video – video steganography – and De-Steganography process. More details about our technique is described in Section 3.

The rest of the paper is structured as follows: Section 2 gives a Literature Review about studies that used the steganography technique to hide information in digital images and video. In Section 3, we are discussing our system that is being proposed in this paper. Then Section 4 presents the result analysis and evaluation. And finally, the conclusion and future work are presented in Section 5.

2 Literature Review

There are several studies that worked on video steganography. In this section, we have covered different techniques that are being used in video steganography.

The LSB technique has been used by Khan ***et al.*** [6] to hide information in the cover image. They utilized the pixel value to hide the secret information. The pixel value was used to decide the capacity of the secret information that can be concealed within the message. More information can be hidden in low pixel value as contrast to less information that can be hidden in high pixel value of the cover image. The technique was compared to other existing techniques. However, in this technique they modified at most 4 LSBs. For instance, if the pixel value is between 0 and 31, these 4 bits can affect green colour in RGB cover images which subsequently can affect the proposed technique in terms of security. In our approach, at most 2 LSBs have been modified which doesn't have significant effect on the cover message.

S. K.b. ***et al.*** [7] presented a video steganography approach to conceal the secret information. First, the secret information was encrypted using a key. Afterwards a feedback shifts register (FSR) was used to determine a random frame that contained hidden secret data. This technique is very efficient and has the ability to hide the information in a secure manner. However, this technique has an adverse side effect in term of time. The performance time depends on the generation and comparison of random value as duplicate value would be rejected and recomputed. Moreover, the time efficiency is degraded as secret size is increased and this effect is shown in their research.

Colored video has been used as a video steganography approach by Hasso [8] to disguise the secret text file as a secret message. Firstly, the audio file was isolated from the video after which the cover video was converted into frames. Also, the secret text file was converted into binary format and was hidden inside the cover video by combining audio with the frames. In this work, the author used 10 or 16 bits out of 24 bits to hide the secret message which is a relatively high ratio and considerably increases the susceptibility of intercepting the secret message. Also, all frames in the cover video contain a partial secret information. This further increases the susceptibility to interception as an attacker can analyze each frame and obtain a part of information about the secret message.

Mstafa and Elleithy [9] proposed a video steganography technique based on Kanade-Lucas-Tomasi (KLT) tracking method using Hamming codes. They used a portion of cover video to hide the secret message. Also, pre-processing stage has been used to encrypt the secret message before hiding it inside the carrier. However, this technique depends on face detection inside the video where the process is very costly in term of computation which further affects the processing time. Moreover, face detection is a big challenge in image processing and computer vision.

Indexing method proposed by Balaji and Naveen [10] to hide information inside the video. They placed index in each frame that contain the secret information. The objective of this approach is to reduce the number of frames required to analyze during extraction stage. However, this technique has its weakness and is susceptible in security term because if the index frame can be determined, the secret message can be extracted using De-Steganography.

Muhammad ***et al.*** [11] presented a framework that combine encryption and image steganography to hide the image. First, the original image was rotated 180˚ and then the image was encrypted using a three-level-encryption algorithm. After that, the image was hidden using steganography technique. However, the effect of this rotation on the susceptibility of secret message is not clear in this particular research.

3 The Proposed Technique

We proposed a novel technique to hide a greyscale image (secret message) embedded in a colored video (cover video) using multilayer video steganography technique. In our approach, we used certain number of frames to hide the secret message from the original video which will make the detection of hidden image extremely challenging. The proposed techniques comprise of five stages which are as follows:

1. Generate a random number.
2. Image pre-processing stage.
3. Frame extraction stage.
4. Determination of frame layer.
5. Merging stage.

3.1 Generate a Random Number

The main concept behind the random number is to make our technique more secure such that it is difficult to detect the secret image by attacker or anonymous intruder.

RANDPERM function in MATLAB was used to generate 255 unique random numbers between 1 to 255 and same function was used to generate only one value. The final random number consist of 256 random values that are being generated to determine which pixel will be use to conceal the secret image.

3.2 Image Pre-Processing

In our research, we used various types of grayscale images as a secret image that will be hidden inside the cover video. For instance, we used grayscale cameraman image as a sample secret image. Cameraman image was imported from the USC-SIPI (University of Southern California – Signal and Image Processing Institute) image database.

Figure 2 illustrates our pre-processing technique which comprises of four stages. First, the secret image was read as an input (cameraman image) which was converted into m*n matrix consisting of each pixel value. Then the m*n matrix was converted into one-dimensional array and finally it was divided into N blocks with each block containing 256 pixels.

The main objective behind converting the m*n matrix to one-dimensional array is to enhance the complexity of decoding technique and reduce the ability of interpreting information from each block.

In addition, in order to increase the security, we used the 6 most significant bit from each pixel in the secret message. In the receiver side, we assigned the 2 LSBs to 1 and 0 because the human vision is unable to distinguish between the color value of 153 or 150 as it is almost similar for human eye.

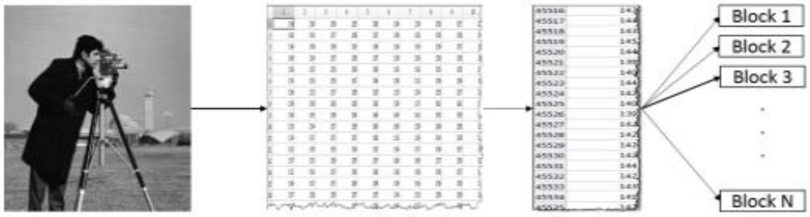


Figure 2 - Image Pre-processing

3.3 Frame Extraction

In general, both colored and grey scale digital videos consist of numerous frames. However, in the colored digital video, each frame has an additional three different layers named as Red, Green and Blue (RGB).

In our research, diverse group of frames were extracted from the cover video. At this stage, a novel technique was used and these frames were divided into three different categories which are secret frames group, index frames group and unused frames group. Each group has been used for different purpose.

The secret frames were used to obscure fragment of the secret image where the ratio between used pixels to unused pixels is 256: (m * n).

The index frames containing the random number, generated in the first stage, was concealed in one pixel. Also, to increase the complexity and reduce susceptibility, one frame was used to hold one random number.

Unused frames were kept unmodified and these frames could be used to conceal more information given two or more secret images or it could be used to accommodate the space required to hide the RGB image. The identification of the random numbers that are being used to extract the secret information during de-steganography phase can be done by an agreement between sender and receiver.

3.4 Determination of Frame

Colored video has been used as a secret carrier. Each frame of this carrier consist of three different layers red, green and blue. In our approach two LSBs were used from each layer.

Figure 3 shows the 24 bits in each RGB pixel. In this technique, each layer contains two MSBs from the secret image and hence the process is called as the 2-2-2 process. In fact, the 2-2-2 technique use LSB bits from cover video in RGB layers to embed the MSBs of secret message. The reason behind using this particular technique is that human vision system is more sensitive to blue colour and any change of more than 2 bits can be observed by the naked eye. Another reason of using this technique is that it used the 6 MSBs from the secret message.

After the determination of the required layer, substitution method was applied between the block of secret message and the layer. In addition, to make our algorithm robust, a random number between 1 and 255 was used to identify the pixel that can be utilized to apply the replacement technique. Afterwards, the random numbers were stored in the index frames.

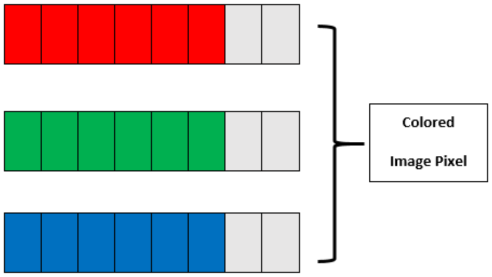


Figure 3 - 24 bits RGB Pixel

3.5 Merging Stage

Now, we have three categories of the frame. The first category is the secret frames that contain a partial secret information from the secret message. The second category is the index frames that have a pivotal role in our technique and contain information about the exact pixel that contain our secret message. The third category is the unused frames that can be utilized for future work.

The Steganographed video comprises of all three frame groups. The merging process combine outputs of the previous stages (secret frames, index frames, and unused frame) in order to create the Steganographed video as shown in Figure 4.

Figure 4 shows the complete flow chart of our approach. In First stage, the cover video was extracted into N frames and the frames were subsequently categorized. For instance, the frame number one in the figure can be used as a secret frame that holds the partial information about the secret message. On the other hand, the frame number two can be kept unmodified and could be categorized under unused frame. This was followed by categorization of frames and the blocks obtained from the pre-processing stage were embedded into the RGB layers of secret frame. Afterward, all the frames were merged together to generate the Steganographed video.

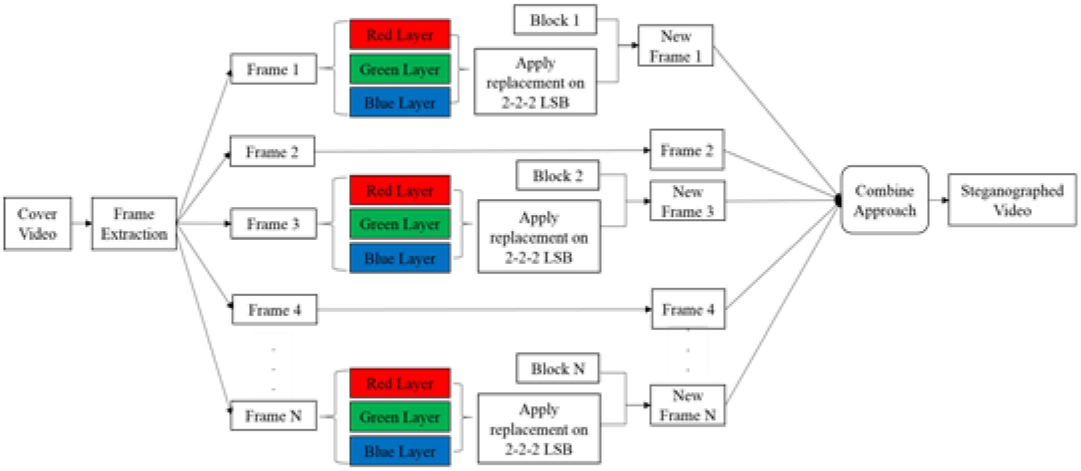


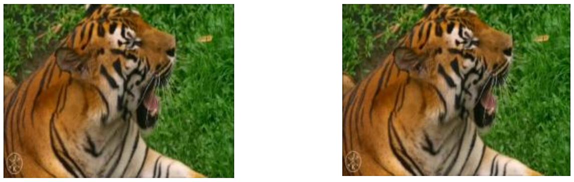
Figure 4 - Multilayer Steganography Technique

4 Results Analysis and Evaluation

In our research, we used MATLAB 2015a as a development tool to perform our simulation in implementing the proposed technique.

It is impossible to display the result of Steganographed video on paper. Hence, in order to validate our proposed technique in term of robustness and invisibility, various types of analysis were performed.

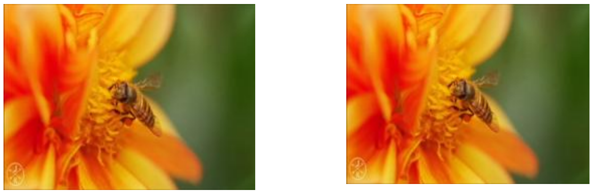
The first type of the experiment analysis was to test human vision ability to detect the difference between the original video and Steganographed video. For this purpose, 20 people were chosen and participated to validate our technique. However, not a single person was able to recognize a significant difference. Also, as a proof-of-concept, we showed two different samples of frames. Figure 5(a) shows the original frame from the cover video while Figure 5(b) shows the same frame from the Steganographed video. In addition, Figure 5(b) shows a secret frame that comprises the partial information from the secret image.



(a) (b)

Figure 5 - Original vs. Secret Frames

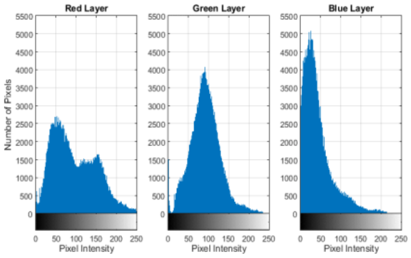
Also, to emphasize that our technique is secure enough, we showed another type of frame, the original frame from the cover video as shown in Figure 6(a), and the index frame as shown in Figure 6(b) which contains information about which pixel we used to hide the secret image.



(a) (b)

Figure 6 - Original vs. Indexed Frames

Another type of experimental analysis that was performed to verify our technique is the histogram analysis. The histogram analysis was used to analyze the color distribution of different types of frames and a comparison of the histogram of the original frame with index and secret frames were carried out. Figures 7 and 8 shows the histograms of the original frame and secret frame.



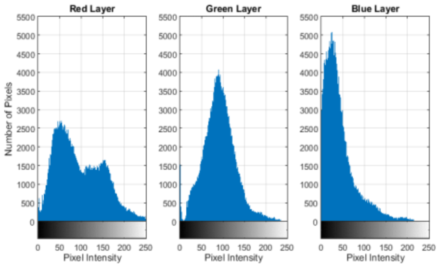


Figure 7 - Histogram of the original frame

Figure 8 - Histogram of the secret frame

Similarly, histogram of the original frame from the cover video and the index frame from Steganographed video are showed in Figures 9 and 10 respectively.

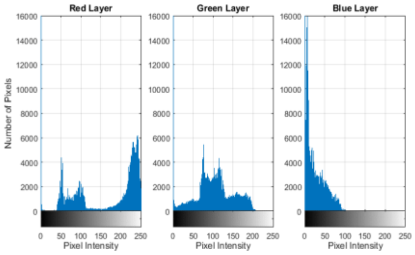


Figure 9 - Histogram of the original frame

Another type of analysis, that has been used to verify our technique validity is to compute peak signal to noise ratio (PSNR) which presents a comparison between the cover video and the Steganographed video. The phrase Peak Signal-to-Noise Ratio (PSNR), is an engineering phrase for the ratio between the value of the maximum possible power of a signal and the value of the power of corrupting noise that affects its representation. PSNR is usually expressed in phrase of the logarithmic decibel scale. PSNR is used by analogue systems as a measure of quality parameter and also a benchmark that has been used in image and video processing [12].

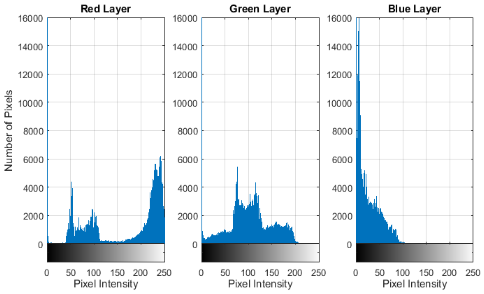


Figure 10 - Histogram of the index frame

The following equations are used to calculate the PSNR:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - k(i,j)]^2$$

$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

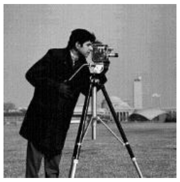
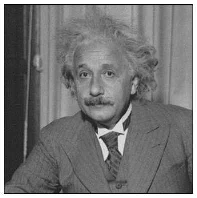
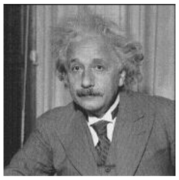
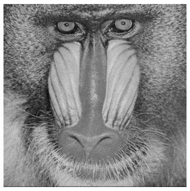
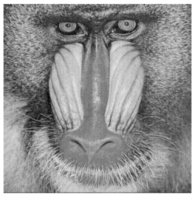
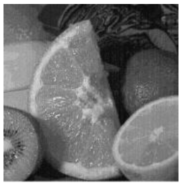
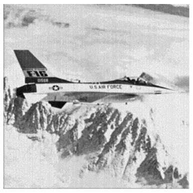
Where MAX is the maximum pixel value of the image, in grayscale images or colored image layer MAX = 255. Table 2 presents the PSNR result of the proposed technique for secret frames, index frames, unused frames and the entire video. Our proposed technique achieved a result that is above 80 dB which is well beyond the acceptability criteria of 50 dB for PSNR evaluation. Also, the PSNR value that is presented in the literature was between 70 to 80 dB as compared to our achieved PSNR of more than 80 dB. Hence, this is a significant improvement from the current studies.

5 Conclusion and Future Work

In this paper, we proposed a novel technique for video steganography by hiding a greyscale image in a colored video. Our approach uses the 6 MSBs from the secret image since theses 6 bits contain more than 98% of the information that is available in the secret message. This will allow the receiver to understand the meaning of the secret message. In addition of making our technique secure, we used random number to decide which pixel will hold our secret information as agreed by sender and receiver. This information can be used in de-Steganographed process to obtain the secret message. Three different types of analyses were used to evaluate our technique showed an improvement in terms of security, robustness and capacity. All of these analysis provide proof that no significant difference can be detected by an attacker or an intruder.

For future work, we will seek to enhance our technique to conceal RGB images as secret message. Also, we will use the sound to hide more secret messages.

Table 2 - The Performance Measures of the Proposed Technique Using PSNR

Secret Benchmark Image	Frames		Entire Video average PSNR	De-steganography Process Output
	Frame Type	Avg. PSNR		
	Secret Frames	76.8298	80.8824	
	Index Frames	68.9541		
	Unused Frames	Inf		
	Secret Frames	77.3236	81.1423	
	Index Frames	69.1972		
	Unused Frames	Inf		
	Secret Frames	77.1079	81.0662	
	Index Frames	69.1972		
	Unused Frames	Inf		
	Secret Frames	77.5089	81.3175	
	Index Frames	69.1972		
	Unused Frames	Inf		
	Secret Frames	76.0844	80.7053	
	Index Frames	69.1972		
	Unused Frames	Inf		

REFERENCES

[1]. Scholar, P. and J.S. Nair., *A Review of Image based Cryptography*, International Journal of Computer Security & Source Code Analysis, 2015. 1(3): p. 13-16.

[2]. Napal, S., et al., *Image Watermark Embedded Using Dwt, Neural Network and RSA*. International Journal of Advanced Engineering Research and Applications (IJAERA), 2015. 1(7): p. 276-284.

[3]. Johnson, N. and S. Jajodia*, Exploring steganography: Seeing the unseen .* Computer, on IEEE, 1998. 31(2): p. 26-34.

[4]. Sadek, M. M., et al., *Video steganography: a comprehensive review*. Multimedia tools and applications, 2015. 74(17): p. 7063-7094.

[5]. Goyal, H. and P. Bansal, *An Analytical Study on Video Steganography Techniques*. International Journal of Advanced Research in Computer Science, 2015. 6(5): p. 50-52.

[6]. Khan, Z., et al., *Threshold based Steganography: A Novel Technique for Improved Payload and SNR.* International Arab Journal of Information Technology [Online]. 2016, 13(4).

[7]. Sudeepa, KB., et al., *A New Approach for Video Steganography Based on Randomization and Parallelization.*, Procedia Computer Science, 2016. 78: p. 483-490.

[8]. Hasso, Abdul-Rhman S., *Steganography in Video Files*. International Journal of Computer Science Issues (IJCSI), 2016, 13(1): p. 32-35.

[9]. Mstafa, R. J., et al., *A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes*. Multimedia Tools and Applications. 2015. p. 1-23.

[10]. Balaji, R. and G. Naveen. *Secure data transmission using video Steganography*. Electro/Information Technology (EIT), on IEEE International Conference, 2011. p. 1-5*.*

[11]. Khan, M., et al., Dual-level security based cyclic18 steganographic method and its application for secure transmission of keyframes during wireless capsule endoscopy , Journal of medical systems, 2016. 40(5): p. 1-16.

[12]. Huynh-Thu, Q. and M. Ghanbari, *Scope of validity of PSNR in image/video quality assessment.* Electronics letters, 2008. 44(13): p. 800-801.