A Blind Video-Steganography Technique Based on Visible Light Wavelength for Raw Video Streams

Özdemir Çetin
Computer Systems Education, Sakarya University, Sakarya, Turkey
ocetin@sakarya.edu.tr

Ahmet Turan Özcerit
Computer Systems Education, Sakarya University, Sakarya, Turkey
aozcerit@sakarya.edu.tr

Abstract: Steganography techniques, which are a set of data hiding algorithms utilizing mathematical methods, have revealed significant advancement by means of latest computing technologies. Although many distinct steganography techniques have been suggested and implemented, an ideal solution has not been reached so far. The primary objective for steganography is to achieve a secure data transfer through a communication channel without attracting attention of unauthorized third parties. Since encryption methods do not meet the steganography requirements, a couple of data masking methods are also required. The performance of a steganography method can be assessed with the statistical similarity between cover media and stego media. In this paper, we have developed a blind steganography technique based on Human Vision System (HVS) using visible light wavelength approach. The proposed technique maintains virtually imperceptible alterations in the stego-video by means of the HVS approach. In addition, the technique developed does not require the cover video in the recovery phase so that it provides more secure manner in many types of applications.

1. Introduction

Accessing digital data has not been so easy ever with the dawn of the Internet, especially in the last decade. This reality has also caused many troubles that have not been considered before such as privacy, security, and sharing. In order to create feasible solutions to such issues, many researchers have focused on cryptographic techniques in company with data embedding and data hiding techniques e.g. steganography and watermarking. Although both steganography and watermarking techniques present similar properties, each technique retains individual purposes. While the former is usually used for secure data communication, the latter is used for copyright protection intents (Cetin 08).

In Steganography, the secret data is usually embedded into multimedia files (image, video, audio, etc.). In addition, the media files in the end of steganography routines can be used directly at the destination without requiring extra decrypting procedures. The most distinctive feature of the steganography compared to cryptography is that unauthorized individuals are not aware of the hidden data in the stego-media (Cetin, Ozcerit 08)

Initial steganography techniques have been first applied to images; however, the video streams have attracted a lot attention recently since they can assure a large amount of capacity increase for hidden/secret data (Koz&Alatan 05). The hidden data can be embedded either into image or into audio part of the video streams. The DCT (Discrete Cosine Transform) and the DWT (Discrete Wavelength Transform) are the most frequently used methods for these purposes.

In this paper, we developed a new technique to determine the appropriate pixels, which are the target regions to store hidden data, in the cover-video frames based on the HVS method. Besides, the chief objective of this study is to keep the perceptibility level of the secret data in the cover video as much as insignificant so that external suspicions or attacks can be prevented. In order to realize these requirements, the HVS method is used and supported by visible light wavelength and the color deficiency of human vision at extreme frequencies. We have evaluated the picture quality difference between the stego-video and cover-video with the PSNR (Peak Signal to Noise Ratio) criterion.

2. Previous Work

One of the first studies on raw video steganography developed by Hartung and Girod and they were inspired from spread spectrum communication (Hartung& Girod 96). Hartung also applied data embedding techniques directly on raw video streams. In the recovery phase of the secret data, a correlation method is used at the receiver side and the secret data capacity achieved up to 50 bit/s according to the experimental results. Hartung applied his method to the compressed video streams by embedding secret data into either intra-frames (I-frames), forward predicted frames (P-frames) or bi-directional predicted frames (B-frames) of the MPEG video. The secret data is embedded into the frames using 8×8 DCT coefficients. Hartung claimed that his method achieved more robust outcome against standard signal attacks according to the obtained results (Hartung& Girod 98).

In another study, Swanson proposed the multi-scale watermarking method in which temporal low-pass and high-pass frames are obtained by applying temporal wavelet transform to each frame (Swanson et al. 98). However, the original video stream is needed to recover the watermarking data and this requirement can be considered as a serious drawback.

3. Proposed Steganographic Algorithm

In this work, we have designed and developed a new data hiding method for raw video streams based on the HVS (Cetin 08). Unlike earlier studies, the method developed uses visible light wavelength approach to determine the most appropriate pixel locations, in which the bytes of secret data are stored, in the cover video frames. We have utilized the imperceptible light wavelengths (ultraviolet, infrared) for this purpose (Jonathan et al. 99).

In Figure-1, the process steps of the proposed algorithm are illustrated as a block diagram. Having selected the embedding method, the secret data is embedded into the cover video by means of specially designed embedding and coding algorithms. The stego-video obtained is then forwarded into the communication channel i.e. Internet. At the receiver side, the extraction methods are selected first in accordance with the methods determined at the sender side. The stego-video is then applied to selected extraction and decoding procedures and the secret data is recovered when all procedures is completed.

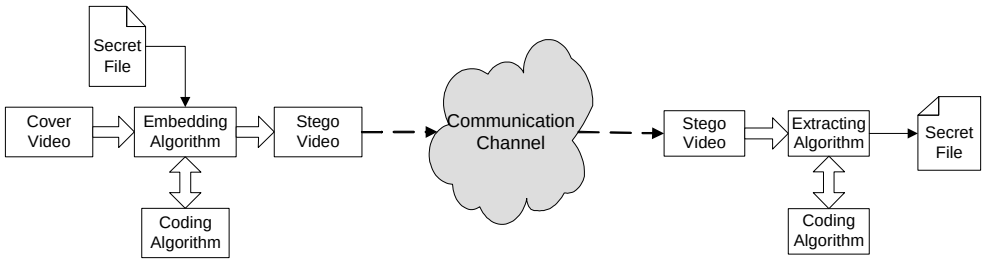

Figure-1 General block diagram for the proposed algorithms

3.1. Visible Light Wavelength Approach

In wavelength approach, the data embedding procedures are implemented by utilizing the imperfection of the color vision. The pillar of the approach is based on the determination of appropriate pixels in the video frames by the help of visible light spectrum data perceived by the HVS. The pixels having the boundary values (~380nm or ~750nm) of visible light spectrum in the cover video frames, in which the secret data is stored, are determined. In other words, the pixels having a wavelength in the range of infrared or ultraviolet colors are searched for in the cover video frames. It is a well-known fact that the human eyes cannot easily perceive minute changes at the visible light spectrum extremities.

The data embedding procedures are initiated by the segmentation of cover video into the frames. The wavelength values of each pixel in the frames of cover video are resolved by the developed algorithm. Since each pixel has three color compounds (Red, Green, and Blue), each color compound of the pixels are individually recorded into a table as given in Table-1. However, only a particular wavelength range (380-400nm

or 730-750nm) of each color compound is significant for the pixel selection procedure. The corresponding wavelength range of the R, G, and B compounds are also listed for violet and red colors in Table-1 accordingly.

Wavelength	R - color intensity	G - color intensity	B - color intensity
Violent: 380~400	97~130	0~30	97~175
Red: 730~750	161~200	0~30	0~50

Table 1. Wavelength range of primary colors

For instance, a pixel having an RGB (100,0,105) code can be evaluated as appropriate pixel for data embedding procedures according to Table-1. Having determined the appropriate pixels in video frames, the secret data is embedded into those selected pixels by the developed algorithms. In this step, the modified pixels are further checked to see whether their current wavelength is within the acceptable limits. If so, each pixel is labeled as "1" meaning appropriate, otherwise labeled as "0" meaning inappropriate.

The amount of pixel wavelength deviation is one of the most crucial criteria for pixel selection procedures. The wavelength deviation should be kept to the minimum for the perceptiveness, which is another important criterion for data embedding method quality assessment. In other words, the stego-video stream should not imply a manipulation in the video frames during the movie.

4. Experimental Results

We have evaluated the performance of our steganography method based on both capacity and perceptiveness criteria. In the performance evaluation stage, the 'vipmen.avi' video file is selected and used as a reference since it is a very popular experimental video stream among researches and it is a raw type video (AVI) stream as well. The experimented vipmen.avi video file has 283 frames and each frame consists of 160x120 pixels.

In the evaluation period, in order to measure the statistical quality of stego-video streams, the PSNR (Peak Signal to Noise Ratio) parameter has been used. The PSNR value presents the similarity ratio between the original video and stego-video. Typically accepted range of the PSNR is between 30dB and 50dB for statistical quality parameter which is computed at the end of each statistical calculation period (Netravali&Haskell 95). The higher values imply high degree of similarity between the original video and stego-video. Since each person has a distinct sense of color and color tones, the PSNR metric cannot provide a perfect evaluation criterion. Therefore, we have used 12 people as test subjects creating another criterion to validate the methods developed.

To compute the PSNR parameter between two video files, the MSE (Mean Squared Error) value is calculated first (Netravali&Haskell 95). Either Equation-1 or Equation-2 can be used for the calculation.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left\|I(i,j)-K(i,j)\right\|^2 \quad (1)$$

$$MSE = \frac{\sum_{M,N}\left[I(i,j)-K(i,j)\right]^2}{M\times N} \quad (2)$$

K (modified video frame) and I (original video frame) parameters in Equation-1 are compared with each other. The size of video is represented by m×n. The PSNR is computed having calculated the MSE value according to Equation-3 (Rabbani&Jones 99).

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right) \quad (3)$$

The MAX parameter in Equation-3 represents the bit size of each pixel. For example, the MAX is 255 when the color depth is selected as 8-bit.

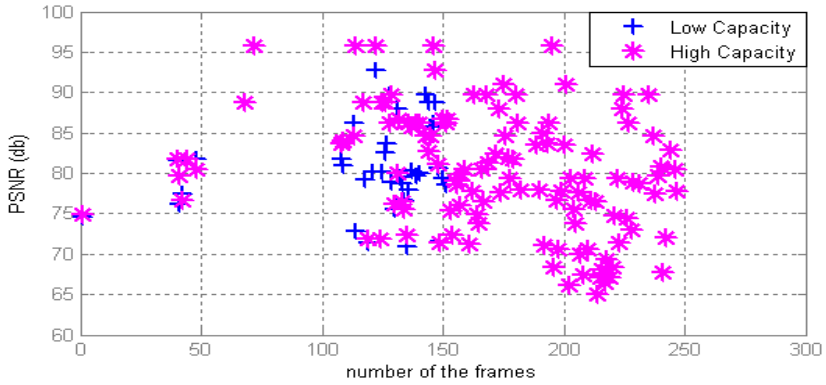

Figure-2 Experimental results relating to the PSNR parameter

The experimental results obtained from data embedding procedures in the wavelength method have been given in Figure-2. The data embedding algorithms developed have been executed for both a low data capacity video labeled as '+' and a high data capacity video labeled as '*'. As seen in Figure-2, the PSNR values for both high data capacity video and low data capacity video are higher than 65dB, which is within acceptable limits compared to the PSNR values for lossy image/video compression standards (Netravali&Haskell 95).

The secret data can be in compressed form such as 'zip' or 'rar' and in this case, more storage capacity for secret data can be achieved in the stego-video file. Another great advantage is that data compression applications can also provide encryption technologies to some extent. Therefore, the secret data can be compressed and encrypted before steganography in order to utilize the benefits of the applications mentioned above.

5. Conclusion

A novel video-steganography method has been proposed to embed secret data into appropriate pixels of a video stream based on visible light wavelength approach. The true advantage of this approach is to determine appropriate pixels that have colors near to visible light wavelength limits i.e. infrared or ultraviolet and this characteristic maintains a better mechanism to conceal the alterations implemented on the pixels because of the weakness of the HVS. The experimental results show that obtained PSNR values for each scenarios are in the acceptable limits and the developed algorithm have worked with the HVS without causing any significant drawback.

References

Cetin, O. (2008), "*A Data Embedding Algorithm Design for Video Applications Using a New Steganography Approach*," Ph.D. dissertation, Elect.&Comp. Edu., Sakarya Uni., Sakarya, Turkey

Cetin, O., Ozcerit, A.T., (2008), "*A Novel Video-Stego Method Based On HVS (İGS Tabanlı Yeni Bir Video–Sırörtme Yöntemi)"* 3rd Information Security&Cryptology Conference with International Participation, Ankara, Turkey, pp.84-88

Koz, A., Alatan, A., (2005), "*Oblivious Video Watermarking Using Temporal Sensitivity of HVS*", Proceedings of the 2005 International Conference on Image Processing (ICIP 2005), Genoa, Italy, September 11-14

Hartung, F., Girod, B., (1996) "*Digital watermarking of raw and compressed video*" in Proc. SPIE 2952: Digital Compression Technologies and Systems for Video Communication, Berlin, Germany, pp. 205–213.

Hartung, F., Girod, B., (1998), "*Digital watermarking of uncompressed and compressed video*", Trans. Of Signal Processing – Sprecial Issue on Copyright protection and Access Control for Multimedia Services, 66(3):283-301

Swanson, M.D., Zhu, B., Tewfik, A.T., (1998), "*Multiresolution scenebased video watermarking using perceptual models*", IEEE J. Select. Areas Commun., vol. 16, pp. 540–550, 1998.

Swanson,M.D. Zhu, B., Tewfik, A.T., (1997), "*Data Hiding for Video-in-Video*", Proc.ICIP'97, Santa Barbara, CA, 2:676-679.

Cetin, O., Ozcerit, A.T., Cakiroglu, M., (2006), "*A New Data Embedding Method into Motion Pictures*" The 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing, Las Vegas, USA.

Jonathan, K.S., Hartung, F., Girod, B., (1999), "*Digital Watermarking Of Text, Image, And Video Documents Comput.&Graphics"*, Vol. 22, No. 6, pp. 687±695, Elsevier Science

Netravali, A.N., Haskell, B.G., (1995), "*Digital Pictures: Representation, Compression, and Standards (2nd Ed*)", Plenum Press, New York

Rabbani, M., Jones, P.W., (1991), "*Digital Image Compression Techniques*", Vol. TT7, SPIE Optical Engineering Press, Bellvue, Washington