International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

An Improved Video Steganographic Approach to Enhance the Security of Embedded Message

Manveer Kaur Garcha
Department of Information Technology
Chandigarh Engineering College,
Landran, India

Jaskiran Kaur, Harsimran Kaur
Department of Computer Science
Chandigarh Engineering College
Landran, India

***Abstract*—In the discipline of information hiding, steganography can be stated as the science of inserting confidential information to be communicated inside any multimedia signal. This paper is aimed at embedding the secret message inside a video signal. Primarily, the video is divided into frames followed by logical frame selection on the basis of six digit secret key. Then, the message is embedded into the selected frame based on the concept of error factor between the actual pixel values and modified pixel values. To flash a bright light on the validity of proposed algorithm, it is endorsed using peak signal to noise ratio, structural similarity index measure and correlation coefficient.**

Keywords—Steganography;Secret Key;Embedding; Extraction.

I. INTRODUCTION

Steganography is the art and science in which confidential information is concealed in any other sort of data. The word steganography comes from Greek dictionary; it is the combination of two different words stegano and graphie. Stegano means cover and graphie means writing. In other words, it can be stated as invisible writing [1]. Cover data can be any multimedia object like image, audio and video. Dominant purpose of using multimedia objects is to hide confidential information from cyberpunks during transmission over public channel [2].

The general block diagram of image steganography is shown in Fig. 1. The cover object can be any multimedia object which is used for embedding the information. Secret information can be any confidential information which can only be shared between familiar parties. Embedding algorithm is a technique used for embedding confidential data in cover object. It can be blind or semi-blind. After embedding the data, the generated object is called stego-object. Stego-object is transferred over communication channel. At the receiving end, the extraction process is performed which is the reverse of embedding process. If blind approach is used to embed data, then blind approach will use during extraction or if it is semi-blind then extraction must be semi-blind [3].

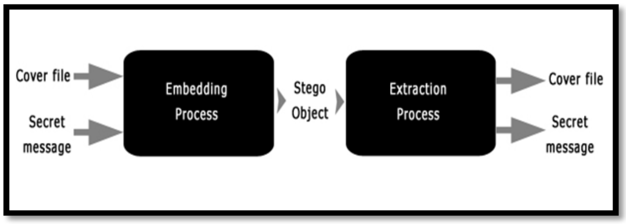

Fig. 1. Basic model of Steganography

In digital image steganography, images are the cover objects. Secret information can be any text file. Both blind and semi-blind algorithm can be used for embedding and extraction. Stego-object will be an image which contains data or secret information in its graphics. The use of secret key is optional in an image steganography, if it is used in embedding, it must be necessary in extraction. Image steganography can be achieved in spatial domain and frequency domain [2].

i. Spatial domain – In spatial domain approach, secret data can be directly embedded on pixels. Least significant bit (LSB) insertion method is mainly adopted in many techniques. Optimal pixel adjustment process (OPAP) and optimal least significant bit (OLSB) methods come under the spatial domain digital image steganography methods.
ii. Frequency domain – In this approach, before performing embedding process, various kinds of image transform methods are applied on cover image such as discrete cosine transform (DCT) , discrete fourier transform (DFT) etc. Image steganography based on entropy thresholding scheme and image steganography using block level entropy thresholding technique methods come under the frequency domain digital image steganography methods.

In this paper, a video steganographic approach is carried out. The frame is logically selected on the basis of secret key in which message has to be embedded using the concept of error factor. It helps to maintain the imperceptibility of message in the frame. The remaining paper is summarized as follows. Section II describes the literature review followed by the proposed technique in Section III. Then, results are discussed in next Section IV followed by conclusions in Section V.

II. LITERATURE REVIEW

In the broad history of steganography, number of algorithms has been developed. Some of these are outlined below.

Anderson and Petitcolas (1998) clarified what steganography is and what it can do. Steganography is contrasted with related disciplines of cryptography and traffic security [4]. Goljan et al. (2001) introduced a general approach for high capacity data embedding. A loseless steganographic approach is proposed which is distortion free in the sense that after the embedded information was extracted from the stego-image, an exact copy of original image was reverted [5]. Ji et al. (2006) presented an optimal block mapping least significant bit method based on genetic algorithm. Additionally, a rule was discussed to select the best block size. The main idea was to minimize the degradation of the stego image by finding a best mapping function between host and secret image blocks at global scope [6]. Chang and Tseng (2009) proposed a two hybrid least significant bit substitution methods. The first method coupled the optimal least significant bit substitution and optimal pixel adjustment process to improve the quality of steganographic image. The second method was the variation of the first one which replaces the optimal LSB substation with the worst LSB substitution [7]. Chanalli and Jadhav (2009) presented a method to hide information on the billboard display. This method can be used for announcing a secret message in the public place. The secret key to be used for embedding or extracting is generated from the pixel values of cover image rather than exchanging key between the two communicating parties [8]. Hong and Chen (2010) proposed a reversible data hiding method based on image interpolation and the detection of smooth and complex regions in cover images. In complex regions, more reference pixels were chosen and thus fewer pixels were used for embedding image degradation. In smooth regions less reference pixels were chosen which increased the embedding capacity without introducing significant distortion [9]. Khalaf and Sulaiman (2011) introduced a robust technique of hiding data in image based on least significant bit insertion and RSA encryption technique. The key of proposed technique was to encrypt the secret data for high security level [10]. Al-Shatnawi (2012) presented a standalone steganographic technique that hides the secret message based on searching about the identical bits between the secret message bits and image pixel values. It was clear that results are better than traditional LSB because fewer changes take place in proposed [11]. Dhanarasi and Prasad (2012) introduced a novel steganographic approach to embed secret message into image using block complexity in wavelet domain. This technique worked on the basis of wavelet transform coefficients and aimed at improving the trade off between high steganographic quality and capacity of message that can be embedded in image [12]. Mishra et al. (2012) used a spatial domain least significant bit substitution method, however, in order to achieve higher security of message, Arnold transformation was successively applied twice in two different phases [13]. Moon and Raut (2013) used video frames as the cover image for hiding the message. Message is embedded using 1 LSB, 2LSB, 4LSB and 4LSB is found to be most suitable for hiding large chunks of information [14].

III. PROPOSED WORK

The proposed steganographic approach is aimed at embedding the secret message inside a video signal. It is a standalone steganographic approach based on least significant bit substitution method. Primarily, the video is divided into frames followed by logical frame selection on the basis of six-digit secret key. Then, the message is embedded into the selected frame based on the concept of error factor between the actual pixel values and modified pixel values. Some of the data used at the time of embedding is required for extracting the message, thus making an extraction process a semi-blind process. Furthermore, this adds to the security of message making extraction difficult for an unauthorized receiver if the attacker ever comes to know about the presence of message. Both the embedding procedure and extraction procedure are discussed in detail in following sub-sections.

A. Embedding Procedure

The flowchart of embedding process is shown in Fig. 2. It unveils the various steps involved in the insertion of message into video. At a first glance, it is crystal clear from the figure that it takes three inputs, i.e., secret message, original video file and secret key. Secret message is the confidential as well as sensitive information, which needs protection from unintended recipients. Video file can be any video of .avi or .wmp format which acts as envelope to cover the secret message. Next is the secret key. It is a 6-digit alphanumeric password. This key is a symmetric key, i.e., it is same for the sender and receiver. Without the knowledge of this key, it would be impossible for the recipient to pluck out the message from the steganographic video.

To embed the message, initially the logic is performed on the secret key. It performs the addition of all digits. If it is a character, then its ASCII code is used for addition. Addition is performed until unless the resulting number, say x comes out to be a two-digit number. On the other hand, the video is converted into frames. Then the frame number x is picked out of all the frames to embed information in it. Then, the selected frame is divided into RGB layers and green layer is chosen for embedding message.

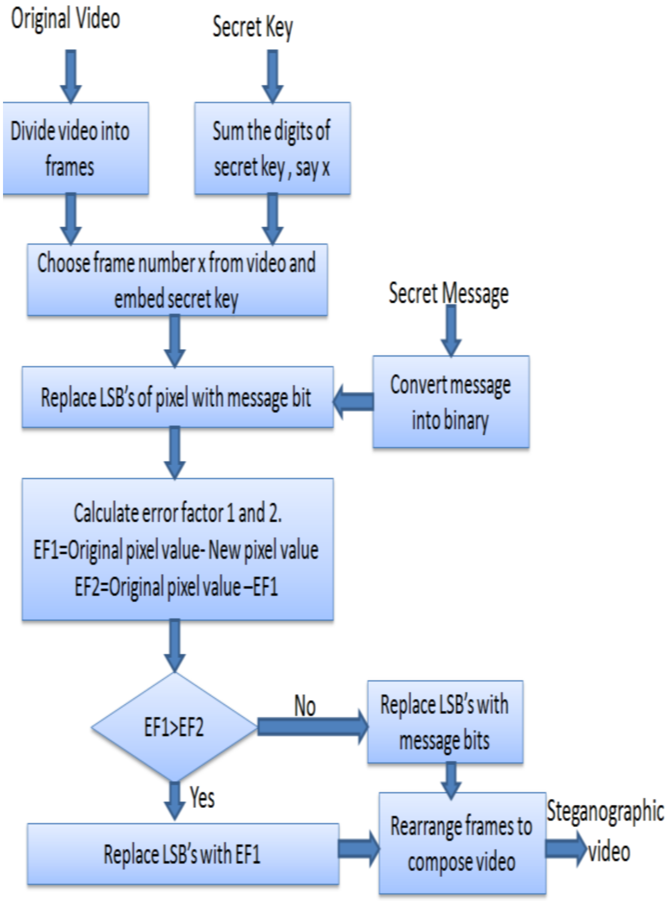
Original Video
Secret Key
Divide video into frames
Sum the digits of secret key, say x
Choose frame number x from video and embed secret key
Secret Message
Replace LSB's of pixel with message bit
Convert message into binary
Calculate error factor 1 and 2.
EF1=Original pixel value- New pixel value
EF2=Original pixel value –EF1
EF1>EF2
No
Replace LSB's with message bits
Yes
Replace LSB's with EF1
Rearrange frames to compose video
Steganographic video

Fig. 2. Embedding process of proposed work

To insert the message, it is first converted to binary format. Then two by two digits are inserted into the selected pixel based on the concept of error factor as illustrated in the following examples, where error factor represents the change in the original pixel value after the information has been embedded into it.

Consider the first pixel of green layer has value: 01101001. And the first two message bits are 11. Then, the two error factors, namely, EF1 and EF2 are calculated using the following method. Firstly, the two LSB's of pixel value are replaced with message bits and the value here turns to be 01101011. Then, two LSBs of original pixel are subtracted from this value to calculate EF1.

EF1= (11 – 01) = 01

Afterwards, the two LSBs of original pixel are replaced with EF1. Again the original LSBs are subtracted from EF1 as follows.

EF2= (01-01) = 00

It is now crystal clear from the two error factors that replacing the original pixel values with EF1will add less error (which is nil error in this case), rather than directly changing the pixel values with message bits.

To generalize, it can be said that LSBs are changed as per the error produced. If EF1 is greater than EF2, then pixel bits are changed with EF1 else the pixel bits are changed with message bits. The colour variations in the pixel values here would be very less as compared to tradition least significant bit substitution method. The above-mentioned repeats itself until the whole message is embedded into the selected video frame. The replacements are recorded into table named less_error to keep information about whether the pixels are replaced with message bits or EF1.

B. Extraction Procedure

The extraction procedure unfolds the sequence of steps to pluck out embedded steganographic message from the steganographic video. It is conspicuous from the figure that it takes two inputs, i.e., steganographic video and secret key that were used at the time of embedding also.

The secret key acts as a password. Crosscheck is performed at this stage. If the passed secret key does not match with the key used for embedding, it will produce an error. If wrong secret key is passed three times, the message gets destroyed and the receiver will not be able to extract that message. This is done for the security of message from unauthenticated receivers.

The extraction process is the reverse of embedding process. It reads the two least significant bits of pixels in which information was embedded. And then it arranges them to form the binary secret message followed by its conversion to human understandable character form.

IV. RESULTS AND DISCUSSIONS

The proposed work is tested on four videos, namely, test.avi taken from MATLAB library and bars_100.avi, toy_plane_liftoff.avi and wildlife.wmv taken from Google. It is evaluated using three performance metrics namely, peak signal to noise ratio (PSNR), structural similarity index measure (SSIM) and correlation coefficient (CC) [3].

PSNR is used to evaluate the difference between original frame and steganographic frame. It is measured in decibel (dB) and can be calculated as follows [10]:

$$PSNR = 10\log 10\left(\frac{255\times 255}{MSE}\right) \qquad (1)$$

where, MSE can be described as the mean of square of differences in the pixel values of two frames. The lower will be the MSE, the lower will be the error and it is calculated as follows [10].

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{i=0}^{N-1}\left[\{x(i,j)-y(i,j)\}^2\right] \qquad (2)$$

CC is used to detect the similarity between the two frames of same size. The value of CC lies between 0 and 1 where 1 is the ideal value. It can be calculated using formula given in Eq. (3), where *C* and *S* represents cover frame and steganographic frame respectively and *M1* is mean pixel value of *C* and *M2* is mean pixel value of *S* [3].

$$CC = \frac{\sum (C(i,j)-M1)(S(i,j)-M2)}{\sqrt{\sum (C(i,j)-M1)^2}\sqrt{\sum (S(i,j)-M2)^2}} \qquad (3)$$

SSIM is used to explore the structural information of distorted frame with respect to the original frame. Structural information, here, can be defined as those attributes which represents structure of objects in an frame independent of the frame contrast and luminance [15]. The PSNR, CC and SSIM values for proposed algorithm between cover frame and steganographic frame are shown in Table 2 when the following message is embedded in selected video frame.

Message: "Hello, this is secret message. I don't want anyone to read me. I don't wish anyone to detect my existence except the sender and intended recipient. Help me please."

TABLE 1. COMPARISON OF COVER AND STEGANOGRAPHIC IMAGE

Video	Performance Metrics		
	PSNR	*CC*	*SSIM*
Test.avi	72.3511	0.9999	0.9999
Test3.avi	73.9403	1.00	1.00
Bars_100.avi	80.1678	1.00	1.00
Wildlife.wmv	68.9602	0.9999	0.9999

For an ideal case, the correlation factor should lie between 0 and 1. By the proposed algorithm, similarity between pixels of cover frame and steganographic frame is much higher so result for correlation factor and structural similarity index measure is highest.

V. CONCLUSION

The proposed method is the combination of already existing methods. Primarily, the video is divided into frames followed by logical frame selection on the basis of six-digit secret key. Then, the message is embedded into the selected frame based on the concept of error factor between the actual pixel values and modified pixel values. The results discussed in Table 1 show that proposed algorithm offers very favorable steganographic quality in terms of PSNR, CC and SSIM.

For future scope, the robustness of message can be taken into account i.e. message should not destroy under intentional or unintentional attacks.

REFERENCES

[1] N. Provos and P. Honeyman, “Hide and seek: An introduction to steganography,” IEEE Security and Privacy Magazine, vol. 1, 2003.

[2] J. Singh, G. Kaur and M. K. Garcha, “Review of Spatial and Frequency Domain Steganographic Approaches,” International Journal of Engineering research and Technology, vol. 4, pp. 1122-1124, 2015.

[3] P. Kaur, H. Singh, A. Gupta and A. Girdhar, “an improved steganographic approach to diminish data modification for enhancing image quality,” International Conference on Medical Imaging, m-Health and Emerging Communication Systems, pp. 329-333, 2014.

[4] R. J. Anderson and F. A. P. Petitcolas, “On the limits of steganography,” IEEE Journal of Selected Areas in Communications, pp. 474-481,1998.

[5] M. Goljan, J. Fredrich and R. Du, “Distortion-free data embedding for images,” Proceedings of the 4th International Workshop on Information Hiding, pp. 27-41, 2001.

[6] R. Ji, H. Yao, S. Liu and L.Wang, “Genetic algorithm based optimal block mapping method for LSB substitution,” IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 215-218, 2006.

[7] C. C. Chang and H. W. Tseng, “Data hiding in images by hybrid LSB substitution,” Third International Conference on multimedia and Ubiquitous Engineering, pp. 360-363, 2009.

[8] S. Channalli and A. Jadhav,"Steganography: An Art of Hiding Data",International Journal on Computer Science and Engineering Vol.1, pp. 137-141 2009.

[9] W. Hong and T. S. Chen, “Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism,” ELSEVEIR, pp. 131-140, 2010.

[10] E.T. Khalaf and N. Sulaiman, “A robust data hiding technique based on LSB matching,” World Academy of Science, Engineering and Technology, pp. 117-121, 2011.

[11] A. M. Al-Shatnawi, "A new method in image steganography with improved image quality", Applied Mathematical Sciences, vol. 6,2012.

[12] G. Dhanarasi and A. M. Prasad, “Image steganography using block complexity analysis,” International Journal of Engineering Science and Technology, vol. 4, pp. 3439-3445, 2012.

[13] M. Mishra, S. Kumar and S. Mishra, “Security enhanced digital image steganography baed on successive Arnold transformation”, Advances in Intelligent Systems and Computing, vol. 167, pp. 221-229, 2012.

[14] S. K. Moon and R. D. Raut, “Analysis of secured video steganography using computer forensics technique for enhance data security,” Second International Conference on Image Information Processing, pp. 660-665, 2013.

[15] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, “Image quality assessment: From error visibility to structural similarity,” IEEE Transactions on Image Processing, vol. 13, pp. 600-612, 2004.