ISSN 2349-4506
Impact Factor: 2.265

Global Journal of Engineering Science and Research Management

AN IMPROVED VIDEO STEGANOGRAPHY TECHNIQUE USING PIXEL VALUE DIFFERENCING AND AES CRYPTOGRAPHY

Shafna P K*
*Computer science and engineering, KMEA College of engineering, India

KEYWORDS: Video steganography, Pixel value differencing, AES encryption, PSNR, MSE, Imperceptible

ABSTRACT

In this work propose a new video steganographic method capable of producing a secret-embedded image that is totally indistinguishable from the original image by the human eye. First the text data is encrypted using AES algorithm. Then derive a difference value from two consecutive pixels by utilizing the pixel-value differencing technique (PVD). The hiding capacity is depends on the difference value of adjacent pixels. In other words, the smooth areas less secret data can be hide, on the contrary, more secret data can be embed in edge areas. This way, the stego-image quality degradation is more imperceptible to the human eye. Second, the remainder of the two adjacent pixels can be computed by using the modulus operation, and then secret data can be embedded into the two pixels by changing their remainder. In this work, there is an optimal approach to alter the remainder so as to highly reduce the image distortion caused by the hiding of the secret text. The values of the two consecutive pixels are changed after the embedding of the secret data by the proposed algorithm. This method avoids the falling-off-boundary problem by using pixel-value differencing and the modulus function.

INTRODUCTION

Advances in digital content transmission have been increased in past few years. Security and privacy issues of the transmitted data have become an important concern in multimedia technology. In this paper, an improved video steganographic method is proposed. For the past decade, many steganographic techniques for images have been presented. A simple and most widely used approach is directly hiding secret data into the least-significant bit (LSB) of each pixel in an image.

The LSB-based methods mentioned above, directly embed the secret text into the spatial without considering the difference in hiding capacity between edge and smooth areas. In general, the alteration tolerance of an edge area is higher than that of a smooth area. That is to say, an edge area can embed more secret data than a smooth area. With this concept in mind, Wu and Tsai presented steganographic scheme that offers high imperceptibility to the stego-image by selecting two consecutive pixels and find its differencing value to embed secret data (Wu and Tsai, 2003). If the difference value is large, that means the two pixels are located in an edge areas, so more secret data can be embed. On the contrary, if the difference value is small, that means the two pixels are located in a smooth area, and less secret data can be embedded. Therefore, their scheme produces stego-images that are more similar to the original images than those produced by LSB substitution schemes.

In this paper, in order to provide a better stego-image quality than Wu and Tsai's scheme (Wu and Tsai, 2003), propose a new technique based on pixel-value difference and modulus function. In Wu and Tsai scheme ,stego-image distortion can happen when the PVD method adjusts the two consecutive pixels to hide the secret data in the difference value. Thus this method suffers from falling-off-boundary problem. In this work, we improve the stego-image quality by adjusting the remainder of the two consecutive pixels instead of the difference value. Besides that, the falling-off boundary problem may probably worsen the situation when the PVD method alone is used, especially either when the two consecutive pixels are located in an extreme edge or smooth area, or when the values of the two consecutive pixels form a contrast. To overcome the falling-off-boundary problem, our new method re-revises the remainder of the two consecutive pixels

MATERIALS AND METHODS

In this proposed method, involves encryption of text message using AES algorithm. Second module involves embedding text data using pixel value differencing method into video frames.

In this work, AES encryption algorithm used for encrypting text data. AES is an algorithm for performing encryption and decryption. AES is a symmetric block cipher. Symmetric block cypher means it uses the same key for encryption and decryption. The algorithm Rijndael allows for a variety of key and block sizes. The key and block can be chosen independently from 128, 160, 192, 224, 256 bits and no need of the same. AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. It is not a feistel structure. The entire data block is processed in parallel during each round using substitutions and

permutations.

AES was designed to achieve the following characteristics:

- Resistance against all known attacks.
- Faster in both hardware and software.
- To attain speed.
- To gain design Simplicity.

The decryption of AES algorithm is not same with the encryption algorithm, but uses the same key. There is also a way of implementing the decryption with an algorithm that is equivalent to the encryption algorithm (each operation replaced with its inverse), however, in this case, the key schedule must be changed.

The Pixel value differencing method, it modifies the remainder of two consecutive pixels P(i,x) and P(i,y) for better stego-image quality. The proposed embedding and extracting algorithms are presented in the following sections below.

The Embedding Algorithm

Step 1: Given a sub-block Fi composed of two continuous pixels P(i,x) and P(i,y) from the cover image, obtain the difference value di, the sub-range Rj such that Rj £ [lj,uj], the width wj = uj - lj + 1, the hiding capacity ti bits, and the decimal value t'i of ti for each Fi by using Wu and Tsai's scheme.

Step 2: Compute the remainder values Prem(i,x), Prem(i,y) and Frem(i) of P(i,x), P(i,y) and sub-block Fi respectively by using the following equations:

Prem(i,x) = P(i,x) mod t'

Prem(i,y) = P(i,y) mod t'

Frem(i) = (P(i,x)(+ P(i,y)) mod t'

Step 3: Embed ti bits of secret data into Fi by altering P(i,x) and P(i,y) such that Frem(i) = t'. The optimal approach to altering the P(i,x) and P(i,y) to achieve the minimum distortion is as follows:

Case 1: (FREM>k && m<=((2^t)/2) && P(i,x)>=P(i,y))

P0=[P(i,x)-ceil(m/2) P(i,y)-floor(m/2)];

Case 2:(FREM>k && m<=((2^t)/2) && P(i,x)<P(i,y))

P0=[P(i,x)-ceil(m/2) P(i,y)-floor(m/2)];

Case 3: (FREM>k && m>((2^t)/2) && P(i,x)>=P(i,y))

P0=[P(i,x)+ceil(m1/2) P(i,y)+floor(m1/2)];

Case 4 :(FREM>k && m>((2^t)/2) && P(i,x)<P(i,y))

P0=[P(i,x)+ceil(m1/2) P(i,y)+floor(m1/2)];

Case 5 :(FREM<=k && m<=((2^t)/2) && P(i,x)>=P(i,y))

P0=[P(i,x)+ceil(m/2) P(i,y)+floor(m/2)];

Case 6: (FREM<=k && m<=((2^t)/2) && P(i,x)<P(i,y))

P0=[P(i,x)+ceil(m/2) P(i,y)+floor(m/2)];

Case 7: (FREM<=k && m>((2^t)/2) && P(i,x)>=P(i,y))

P0=[P(i,x)-ceil(m1/2) P(i,y)-floor(m1/2)];

Case 8: (FREM<=k && m>((2^t)/2) && P(i,x)<P(i,y))

P0=[P(i,x)-ceil(m1/2) P(i,y)-floor(m1/2)];

In the above approach, m = Frem(i) - t'i , m1 = 2 t i -| Frem(i) - t'i | and p'(i,x) ,P '(i,y) are new pixel values after the embedding of ti bits of the secret data into sub-block Fi. After Step 3, P'(i,x) or P '(i,y) overflows the boundary value 0 or 255, then execute Step 4 for revising P'(i,x) and P '(i,y). If not, the purpose of concealing secret data will be completed after the replacement of(P(i,x) or P (i,y))by(P'(i,x) or P '(i,y)) in the cover image.

Step 4: Consider the three situations below where the falling- off-boundary problem happens and revise P'(i,x) and P '(i,y) as follows:

Case 1 : If P(i,x) =0 , P '(i,y) = 0 and P'(i,x) < 0 or P '(i,y) < 0, then re-adjust P'(i,x) and P '(i,y) to be P''(i,x) and P ''(i,y) by

(P''(i,x) , P ''(i,y)) = ((P'(i,x) - 2ti) /2.(P '(i,y) - 2ti) /2))

Case 2 : If P(i,x) =255 , P '(i,y) = 255 and P'(i,x) > 255 or P '(i,y) > 255, then re-adjust P'(i,x) and P '(i,y) to be P''(i,x) and P ''(i,y) by

(P''(i,x) , P ''(i,y)) = ((P'(i,x) - 2ti) /2.(P '(i,y) - 2ti) /2))

Case 3 : If P(i,x) and P '(i,y) = 0 from a great contrast , then re-adjust P'(i,x) and P '(i,y) to be by

After Step 4, (P'(i,x) , P '(i,y)) can be corrected so that the range of (P''(i,x) , P ''(i,y)) cannot go below 0 or over 255. Finally, we put use (P''(i,x) , P ''(i,y)) in place of (P(i,x),P(i,y)) in the cover image and the embedding algorithm is accomplished.

Suppose we have a sub-bock Fi with two successive pixel values P(i,x) = 32 and P(i,y) = 32. Then, the remainder value Frem(i) of Fi is 0. If the 3 bits (i.e. ti = 3, and ti'= 23 = 8) of the secret data are selected to be embedded into Fi, P(i,x) and P(i,y) will be modified to hold the 3-bit secret data. Table 2 demonstrates that our scheme has better performance in reducing the difference between (P(i,x) and P(i,y)) and (P'(i,x) and P'(i,y)). Next, explain an example to show how the mechanism of keeping the pixel values from exceeding the range [0, 255] after secret data embedding. As shown in Table 3, we reassume P(i,x) = 0 and P(i,y) = 0 in the previous example, and then the falling-off-boundary problem happens such that P(i,x) < 0 and P(i,y)< 0when the decimal value of the secret data is 5, 6, or 7. However, P'(i,x) and P'(i,y) can be re-adjusted by adding up to 4 synchronously. After that, the values of (P''(i,x) and P''(i,y)) will fall within the range of 0–255.

RESULTS AND DISCUSSION

Steganography technique is characterized mainly by imperceptibility and capacity. Imperceptibility means the embedded data must be perceptually invisible to the observer. In order to evaluate the performance of the stego video, there are some quality measures such as SNR, PSNR, MSE, and BER. Efficiency of the algorithm can be found out by taking into consideration, the evaluation measures, Peak signal-to-noise ratio and Mean squared error.

Steganography technique is characterized mainly by imperceptibility and capacity. Imperceptibility means the embedded data must be perceptually invisible to the observer. The performance of the proposed technique is evaluated using two different video streams (shakyc_car.avi, wildlife) and one secret text (text_to_hide.txt).The perceptual imperceptibility of the embedded data is indicated by comparing the original video with its stego_video. When we hide secret text in video there will be no loss in quality of video and even none can guess the presence of data within a video.

Table 1: The results of embedding cypher text using proposed method

Video file	**Capacity**	**PSNR**	**MSE**
Wildlife.mp4	1388790	86.3670	1.5010e-04

Shaky_car.avi	116615	53.4360	0.2948
Fall.mp4	523183	56.0066	0.1631
ocean1.mp4	520207	79.0865	8.0247e-04
Stream1.mp4	531704	79.0865	8.0247e-04
bikeRace.mp4	360794	79.5198	7.2627e-04

From above table we observed that by using secure text transmission using pixel value differencing technique, we get more PSNR and hiding capacity. If the video has large hiding capacity we can obtain more hiding capacity and gives more PSNR and small MSE. It gives different values of PSNR which deals with quality of video. For different resolution this quantity shows variation.

CONCLUSION

In this work, propose a novel scheme to enormously reduce the visibility of the hiding effect present in the pixel value differencing method. The proposed method is efficient and good for hiding data in video. One of the important features of the proposed work is it helps to transmit data securely by embedding it in a video file and without disclosing to the unintended receiver and without any alternation in secret message. The data embedded in the video is not visible to the naked eye. An efficient AES encryption algorithm is used for the encryption of the text data. The proposed scheme utilizes the remainder of the two consecutive pixels to record the cypher text which gains more flexibility, capable of deriving the optimal remainder of the two pixels at the least distortion. The proposed method can also solve the falling-off-boundary problem by re-revising the remainder of the two pixels. With the combination of the cryptography and steganography information security can be increased.

ACKNOWLEDGEMENTS

I am highly indebted to Mrs. Viji Mohan for their guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project.

REFERENCES

1. Chung-Ming Wang a, Nan-I Wu a, Chwei-Shyong Tsai b, Min-Shiang Hwang “A high quality steganographic method with pixel-value differencing and modulus function”, journal of systems and software , 24 January 2007
2. B.SUNEETHA, CH.HIMA BINDU & S.SARATH CHANDRA ―SECURED DATA TRANSMISSION BASED VIDEO STEGANOGRAPHY‖International Journal of Mechanical and Production Engineering (IJMPE) ISSN No.: 2315-4489, Vol-2, Iss-1, 2013
3. Kousik Dasgupta, J.K. Mandal and Paramartha Dutta,‖ Hash based Least Significant Bit Technique‖, International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012
4. A. Swathi 1, Dr. S.A.K Jilani,, ―Video Steganography by LSB Substitution Using Different Polynomial national Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5
5. Mritha Ramalingam: Stego Machine – Video Steganography using Modified LSB Algorithm World Academy of Science, Engineering and Technology Vol:50 2011-02-26
6. Ashawq T. Hashim*, Dr.Yossra H. Ali** & Susan S. Ghazoul*‖ Developed Method of Information Hiding in Video AVI File Based on Hybrid Encryption and Steganography‖ Engg.and tech journal, vol 29,No.2,2011.
7. R. Shanthakumari1 and Dr.S. Malliga, ―Video Steganography Using LSB Matching Revisited Algorithm‖, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. IV(Nov – Dec. 2014), PP 01- 06
8. Mritha Ramalingam, “Stego Machine Video Steganography using Modified LSB Algorithm”, in World Academy of Science, Engineering and Technology, 50, pp. 497-500, 2011.

9. Pritish Bhautmage, Prof. Amutha Jeyakumar, Ashish Dahatonde, "Advanced Video Steganography Algorithm", International Journal Of Engineering Research And Applications "(IJERA) , Pp.1641-1644 1641 Vol. 3, Issue 1, January -February 2013.
10. Satya Kumari, K.John Singh, "A Robust And Secure Steganograph Approach Using Hash Algorithm", International Journal Of Latest Research In Science And Technology, Volume 2,Issue 1 :Page No.573-576 , January-February (2013).