Digital Color Video Steganography Using YCbCr Color Space and Dynamic Least Significant Bit (DLSB)

Ahmed Toman Thahab
College of Engineering/University of Karbala
toeahmed@gmail.com

Abstract

Steganography is essential in secure data exchanging and other numerous types of applications, therefore; it has become one of important fields to researchers. Steganography is the process of implanting secret information in an information cover without causing severe degradation neither to the cover information nor the secret information implanted in the cover. Most of the steganography techniques are applied on images, texts and protocols. In this paper a new technique of video steganography is proposed to implant a secret video data in to a cover video data using YCbCr color space and dynamic least significant bit algorithm (DLSB). The Least significant bit algorithm is used to hide text data in image or hiding an image in image data but this paper will propose a new technique which will utilize the LSB dynamically in embedding video clip in video data. The performance of the proposed algorithm has been gauged by peak signal to noise ratio (PSNR) for the stego, cover and secret videos while most of the papers which deal with steganography show the PSNR for the stego image only. The paper also shows reconstructed frames of the videos conducted by the algorithm. The results articulate that the algorithm is a good new method for video steganography.
Keywords: color space, dynamic least significant bit, APSNR, YCbCr, most significant bit.

الخلاصة

الاخفاء هو عملية اساسية في تبادل البيانات لذلك اصبح مجال الاخفاء من اهم المجالات للباحثين والذي يتضمن انواع متعددة من التطبيقات. الاخفاء هو عملية اخفاء معلومات سرية في معلومات الغطاء دون التقليل من جودة المعلومات سواء كانت السرية او معلومات الغطاء.أغلب تقنيات الاخفاء يخص ملفات الصور،النصوص والبروتوكولات. في هذا البحث تم اقتراح طريقة لاخفاء معلومات فديوية سرية في معلومات فديوية اخرى والتي تسمى بالغطاء بأستخدام الفضاء اللوني (YCbCr)وتقنية البت الاقل أهمية الديناميكية. تستخدم خوارزمية البت الاقل أهمية في أخفاء الكتابات في الصور أو الصور في بيانات الصور لكن هذا البحث يقترح استخدام هذة التقنية ديناميكيا في أخفاء الفديو في بيانات الفديو. تم قياس جودة هذا النظام بأستخدام نسبة قمة الاشارة الى الضوضاء (PSNR).أغلب البحوث في مجال الاخفاء الصوري تظهر نسبة قمة الاشارة الى الضوضاء للفديو المخفي فقط. النتائج تظهر جودة هذة الخوارزمية في الاخفاء الفيديوي.

الكلمات المفتاحية: الفضاء اللوني،البت الاقل اهمية الديناميكي، معدل نسبة قمة الاشارة الى الضوضاء، البت اكثر اهمية.

1. Introduction

Steganography is originated from the Greek word "steganos" meaning covered or secret while graph capitalizes the meaning of writing or drawing [E.Cole and *et al*, 2003]. It is known as the process of hiding private or secret data (message, image)in a cover data, usually; steganography was invented to hide secret information in image data file [Stefan Katzenbeisser *et al*, 1990].The data which the information data is carried in is called the carrier. The common concept behind stego algorithms is that unnecessary bits in the cover data will be removed and replaced by bits of the secret. Large scale of applications are implemented in steganography field commencing from military, industrial, intelligence agencies and agents in the field to watermarking.

Image data file can be easily attacked by hackers, therefore; the introductions of video cover files are robust for hackers to intrude on and extract secret information. According to video stenographic technique, information can be sealed or embedded in the frequency domain of the cover using one of the signal processing transform DWT, FFT and DCT. Secret information can be embedded either on per pixel level or group of pixels called blocks [Ankur.M.Mehta *et al*, 2008].[Fillatre. L, 2012] used LSB insertion and RSA encryption technique to produce a good image steganography. [E.

Kawaguchi *et al*, 1998], embedded information into areas where the image is noisy; this technique is achieved to what was proposed as bit plane complexity segmentation (BPCS). [Mritha Ramalingam, 2011] embedded the data after encrypted in an avi video file carrier; the key of the encryption is stored in file called the file key.[Yi-zahen *et al*, 2011] had proposed a new adaptive algorithm for steganography technique. The algorithm splits the image in to blocks and finds the statistical properties of the block such as variance and mean.[A.Westfield *et al*, 2000] used the least significant bit of direct coefficients the cover image to hide messages in the cover, a random pseudo-code was used to seal the message.

In this paper a video steganography is proposed using LSB algorithm dynamically, the algorithm is stated and illustrated in section 4. Section 5 shows the results of the algorithm between various detailed video data files. Section 6 is conclusions and future work suggestions.

2. Color Space

A color image can be regarded as a three channel positive function defined on a plane. The representation of this image can be viewed as a three dimension matrix:

i. RGB color space

One of the simplest and most popular color spaces is called RGB. Most of the images are displayed in this color space. It is a mixture of red, green and blue layers. These layers are highly correlated which implies that if the two layers are constant, small changes of the values will be very sensitive to human observation for the remaining layer. Although RGB color space is not very efficient for compression, it is commonly used as a storage format [Plataniotis K *et al*, 2000].

ii. Illumination and chrominance color space

The color space uses three numbers to represent each color similar to RGB. RGB can be linearly transformed to YCbCr generating one luminance space Y and two chrominance (Cr and Cb) spaces (layers) using the equations below [Iain E.G Richardson, 2003]:

$$Y = 0.299\ R + 0.587\ G + 0.114\ B \quad \ldots\ldots\ldots\ldots (1)$$

$$Cb = ((R - Y) / 1.6) + 0.5 \quad \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

$$Cr = ((B - Y) / 2) + 0.5 \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

This color space reflects the features of the human's eye. An advantage of using these layers is that the human eyes are more sensitive to the change of brightness than the color layers Cb and Cr spaces [A. Westfield et al, 1999].

3. Least Significant Bit(LSB) Algorithm

Digital images are two dimension matrix pixels which are discrete numbers, each number represent a function of intensity as a function of spatial locations. The idea behind the LSB is that small changes in the least significant bit will not degrade the digital pixel value. Digital binary strings format consist from most significant bit and least significant bit, the most significant bit is located to the left hand side of the string while the least significant bit is located on the right hand side of the string as shown in fig(1):

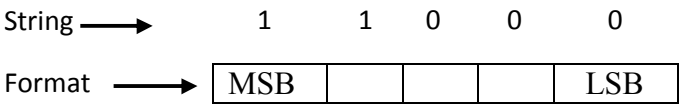


Fig. (1) Binary string format

Applying changes to the least significant bit will not alter a great deal of the coefficient value. If changes are applied to the most significant bit the total value will decrease significantly resulting to degrade in pixel quality and image quality as a whole.It can be noticed that altering the most significant bit of an eight bit binary string,it will change of the fully half of the value [Jassim.M. Ahmed et al, 2011]. An example will illustrate the concept:

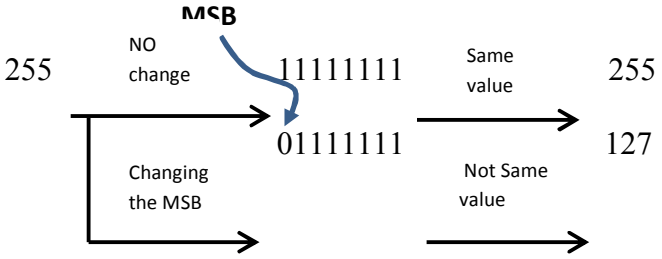


Fig. (2) Changing the value of the MSB

As shown, the recovered value is half the original value when altering the first position of MSB. Tackling another example to illustrate the concept of the LSB is shown in fig. (3),[Juan Jose Roque *et al*, 2009].

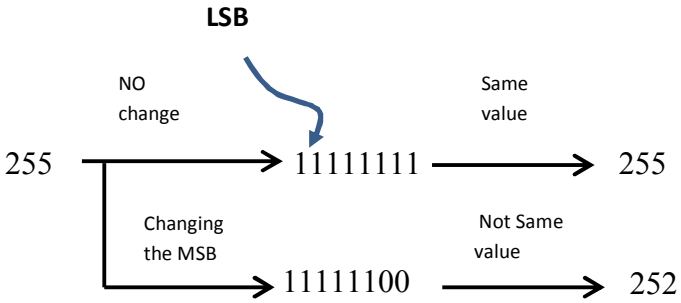


Fig. (3) Changing the value of the LSB

Dynamic implies to the level of LSB bits necessary to be processed, the more deep of LSB bits is changed, the more distortion is introduced to the recovered. In conclusion altering the MSB will enhance significant distortion to the recovered value. LSB will introduce limited degradation to the original value. The LSB algorithm is generally applied on image data coefficients which mainly used to embed data text or image in image data.

4. Proposed Color Video Steganography Technique

An illumination and two chronimic (YCbCr) color space based video steganography is utilized to hide video data inside video cover data. The technique is founded on the basis of the least significant bit (LSB) algorithm. The block diagram of the proposed video steganography is shown in fig (4).

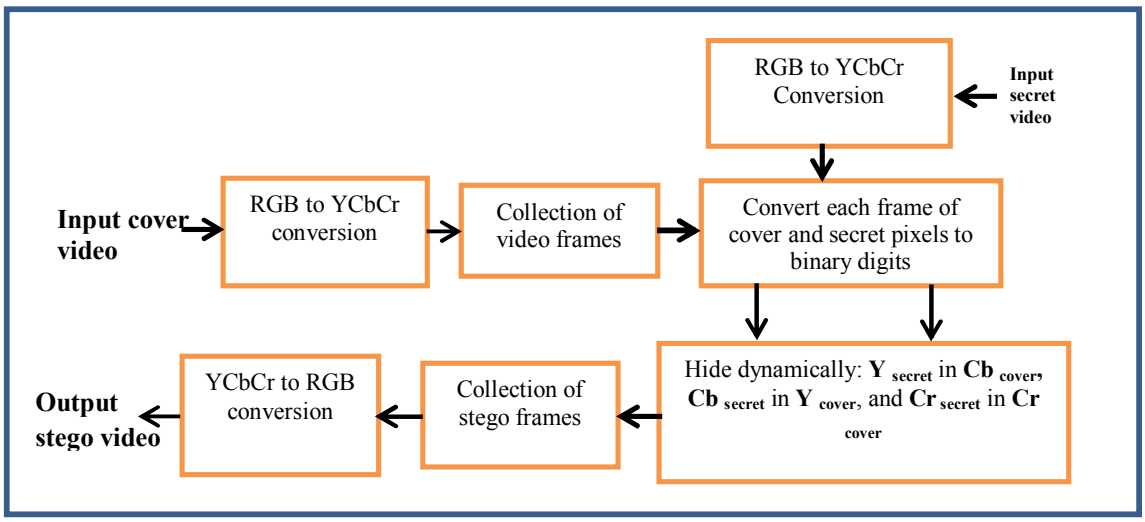


Fig. (4) Proposed digital color video steganography diagram using YCbCr color space and DLSB

The video input is first separated into frames which are three dimension image consists of three layers in RGB color space. A conversion from RGB color space into YCbCr color space is applied to the video frames. The reason behind using YCbCr color space is luminance layer Y is more important than the two other color layers Cb and Cr, therefore; the information in Y component of the cover and secret ought to be softly eradicated than the other two color components Cb and Cr, as a result, the algorithm proposes to hide the important Y component of the secret video in the cb component of the cover video, color component Cb of secret is embedded in Y cover component and Cr secret is embedded in the Cr cover components.

In order to preserve the importance of the Y component, the proposed algorithm utilizes the LSB with dynamic bit eradication. As the bits of the Y component of cover is important, the most significant bit of Cb cover is hidden in the least significant bit of the Y component in a dynamic fashion, while the most significant bit of the Cb is embedded in the least significant bit of the Y component in a dynamic fashion as shown below:

(Cb secret 0101~~0011~~)+ (Y cover 10110~~101~~) = (stego010110110)
(Y secret 10010~~101~~) + (Cb cover 0101~~0011~~) = (stego100100101)
(Cr secret 10010~~101~~) + (Cr cover 1101~~0011~~) = (stego10011101)

The number of bits eradicated from the cover Y components is less than Cb secret since it is essential to preserve Y component information, while the number of bits eradicated in the Cb cover is more than the bits of Y secret, since Y secret is more important than Cb cover. The other color components are equally eradicated. The algorithm embeds video data without degrading neither the stego video nor the secret and cover video when retrieving them back. The algorithm can be briefed by these following steps:

Step1: Read cover and secret video.
Step2: Convert secret and cover video to YCbCr color space.
Step3: Separate the Y, Cb, Cr components of the cover video.
Step4: Separate the Y, Cb, Cr components of the secret video.
Step5: Convert the coefficients from binary to decimal for components of both videos.
Step6: Embed N bits secret Y into M bits of Cb cover video.
Step7: Embed n bits secret Cb into m bits of Y cover video.
Step8: Embed x bits of secret Cr into x bits of Cr cover video.

Step9: Collect frames of stego video.
Step10: Convert the stego video to RGB color space.
Step11: Compute the average PSNR for the stego video.

The process of extracting the original and secret videos is the de-steganography process or steganography analysis, the proposed steganography analysis block diagram is shown in fig. (5). Two videos are the output of the de steganography which will be tested for video quality.

The block diagram illustrates the inverse process of the steganography operation; a conversion from RGB to YCbCr color space is applied. Each layer of the single stego frame is converted to digital bits in YCbCr domain. Extraction process will be conducted on each frame to extract the secret and cover videos from the stego video frames. The bits of the Y component coefficients will be extracted from the bits coefficients of the Cb component, Cb secret component will be extracted from the Y cover component bits and Cr secret will be extracted from the Cr cover bits.

After extraction is conducted, the frames of the secret and cover will be individually collected. The video frames of the two mentioned videos will be converted to RGB color space and replayed.

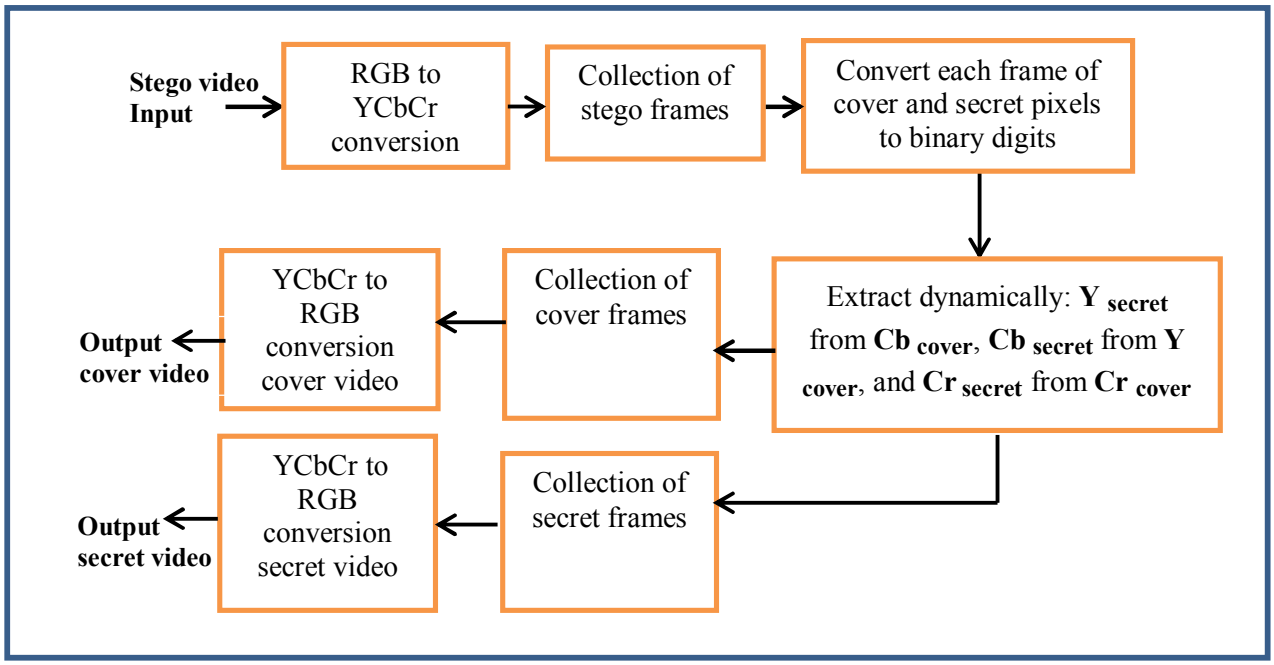


Fig. (5) Proposed digital color video de- steganography diagram

For the de-steganography or Steganography Analysis, the following steps are executed:
Step1: Read the length, dimension and number of frames for the stego video.
Step2: Convert the stego video to YCbCr color space.
Step3: Separate the Y, Cb and Cr components for each frame of the stego video.
Step5: Convert the coefficients from decimal to binary for components of stego video.
Step 6: Extract N bits secret Y from M bits of Cb cover video.
Step 7: Extract n bits of the secret Cb from m bits of Y cover video.
Step 8: Extract x bits of the secret Cr from x bits of Cr cover video.
Step9: Collect frames for secret and cover video individually.
Step10: Convert each video frame to RGB color space.
Step11: Calculate Average PSNR for the secret and cover video.

5. Results and Discussion

In order to investigate the performance of a particular algorithm, performance parameters are essential to illustrate and evaluate the algorithms output and its ability to produce blooming results. The Peak signal to noise ratio (PSNR) is the performance parameter which is used to measure the reconstructed image in most image processing algorithm. The general equation for PSNR for equal dimension frame image is given by eq. (4):

$$PSNR(dB) = 10\log_{10}\frac{(B-1)^2}{\frac{1}{N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}[R(i,j)-O(i,j)]^2} \quad \ldots\ldots\ldots\ldots (4)$$

Where: B=256

R (i,j): is the recovered image frame either, stego, cover or secret frames.

O (i,j): is the recovered image frame either, stego, cover or secret frames.

i,j: image pixel index.

N: Dimension of image.

Noble reconstructed video frames are achieved as the PSNR is increased. The APSNR will be calculated for the reconstructed video by taking the PSNR for a single frame and average along the number of frames in the video movie.

The algorithm is tested with various color videos at different dimensions. Inputs to the system are two video files; cover video and secret video which will be embedded in the cover video. The output will be the stego video. Color videos which are inputted to the algorithm are taken from matlab videos with dimensions 240*320, 240*360. The algorithm has been processed in MATLAB R2010b with 2GB RAM and core2 Duo processor.

Table (1) Practical results of Proposed Video Steganography Technique

EXP.	Name of cover video	Name of secret video	Frames of cover and secret video	APSNR of stego video	APSNR of cover video	APSNR of secret video
1.	Rhinos.avi	Shaky_car.avi	80	28.34	26.84	23.20
2.	Rhinos.avi	Vidnowa.avi	45	28.96	27.24	23.65
3.	Screen video clip.avi	Traffic.avi	72	30.72	25.0	22.7
4.	Rhinos.avi	Vipfly.avi	80	28.44	27.31	21.79
5.	Rhinos.avi	Vipmosack.avi	68	27.84	28.99	25.17
6.	Shaky car.avi	Videparture.avi	110	30.73	38.12	32.39
7.	Rhinos.avi	Vidparture.avi	100	31.05	30.19	25.17
8.	Shaky_car.avi	Vipfly.avi	80	30.23	39.62	25.86
9.	Vipuoad.avi	Viptraffic.avi	84	29.35	30.96	26.10

Table (1) shows that APSNR for the stego, cover and secret video frames, which are the average of all video frames, are highly efficient. High APSNR for the secret video demonstrates high resolution and the secret video can be highly and efficiently restorable. The table also shows that the quality of cover video looks similar to the stego videos which capitalize that video frames can be recovered efficiently without degradation. In experiment 3&4, APSNR for the secret video is decreased since only four bits were utilized for the Y component depriving secret video representation in each pixel of illumination component, while other experiments show better results since each pixel was represented by five bits.

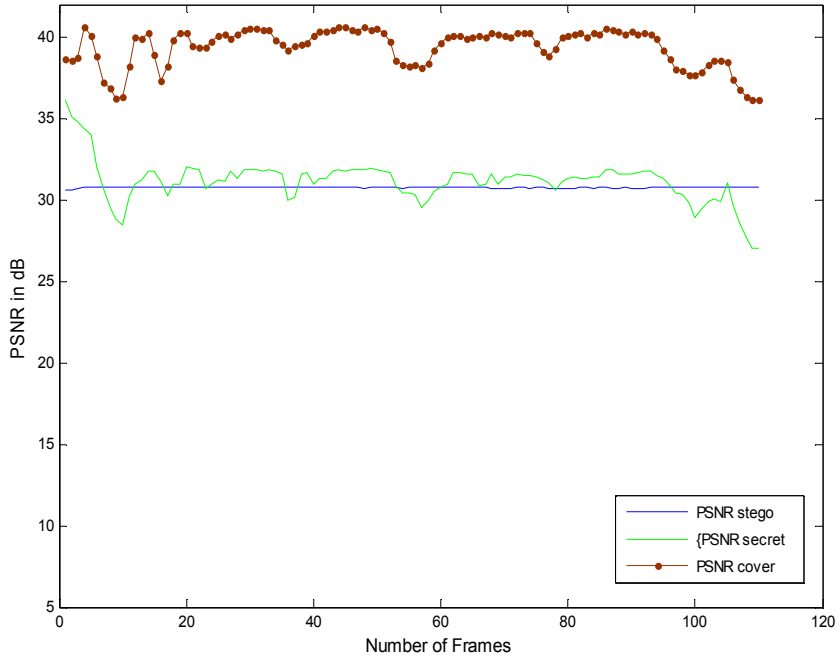


Fig. (6) Shows PSNR of each frame for stego, cover and secret video for experiment.6

Figure.(6) illustrates the PSNR for each frame of experiment six for the secret, stego and cover movie, the stego video frames which holds the secret data has a good PSNR and almost constant along the hiding process.

.

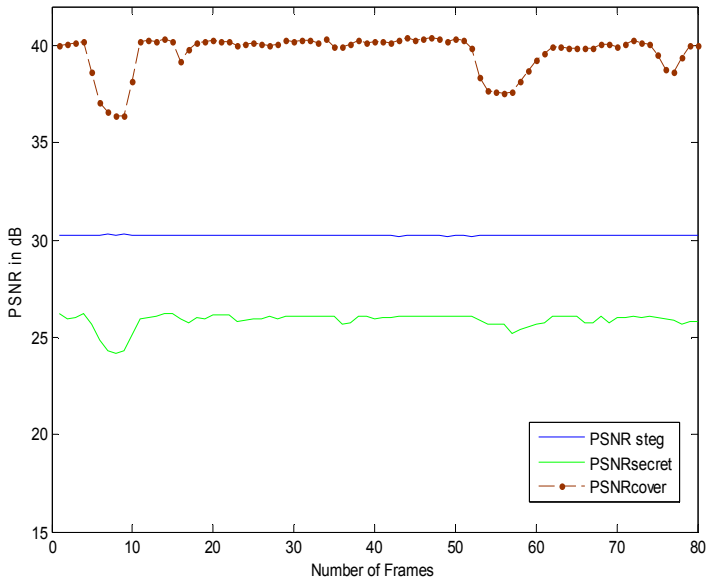


Fig. (7) Shows PSNR of each frame for stego, cover and secret video for experiment.8

Figure (9) shows the reconstructed frames for experiment 3; it shows degradation for the secret video frames since the Y component is being lost with less number of bits.





A. Original **B. Original secret frame** **C. Original cover frame**

Fig. (8)Shows the original frames for the cover and secret frames





Fig. (9) Shows the stego and recovered secret and cover frames for Exp.3

The reconstructed frames shown in figures. (11&13) Show good quality of reconstruction for experiment (9&5), secret video can be recovered efficiently and the stego-video frames have an undisputed quality throughout the video clip.





A. Original frame **B. Original secret frame**

Fig.(10) Shows the original frames for the cover and secret frames





A, Stego frame **B. Recovered secret frame** **C. Recovered cover frame**

Fig.(11) Shows the stego, and recovered secret and cover frame for Exp.9



A. Original frame **B. Original secret frame** **C. Original cover frame**

Fig. (12) Shows the original frames for the cover and secret frames



A. Stego frame

Fig. (13) Shows the stego and recovered secret and cover frame for Exp.5

6. Conclusion

A digital color video steganography technique is presented in this paper. The technique utilizes the property of the luminance and chronic layers with DLSB algorithm. Using fewer bits in the illumination component frames for the secret video cause's degradation when retrieving the reconstructed frames. However, observing the results shown in table (1), it can be shown that the algorithm shows high APSNR for the stego, cover and secret video. For future work, the principle can be applied on HLS color space features with modification on each component. Signal transform like discrete wavelet transform, or discrete cosine transform would be applied using the same principle illustrated in this paper. Increasing the efficiency of the algorithm can be achieved by dividing the video in to group of frames with similar scenes. The algorithm can also be applied on image data steganography.

7. References

A.Westfield and A.P. Fitzmann, Sept. 28-oct, 1999"Attacks on steganographic Systems", in Proceedings of 3rd Info. Hiding Workshop Dresden, pp. 61-75.

Ankur. M. Mehta, Steven Lanzisera and Kristofer. S. J,December 2008 "Steganography 802.15.4 wireless communication" in conference Advanced Networks and Telecommunication Systems,2008. 2nd International Symposium, pp. 1-3.

Kawaguchi, E. and R. OEason,1998 "Principle and application of BPCS-Steganography", in Proceedings of SPIE Int. Symposium on voice, Video and data communications, pp. 464-473.

Cole, E. and Krutz, 2003 "Steganography and the art of covert communication", Willy Publishing, Inc., ISBN 0-471-44449-9.

Fillatre. L,2012 “Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption”, IEEE transaction on Signal Processing, volume 60, issue: 2, PP. 556-569.

Iain E.G Richardson,2003 "H.264 and MPEG-4 Video Compression, John Willy & Sons Ltd.

Jassim. M. Ahmed and Zulkarnain Md Ali, April, 2011 “Information Hiding using LSB Technique”, in IJCSNS International Journal of Computer Science and Network Security, Vol.11, No.4.

Juan Jose Roque and Jesus Maria, 2009 “Improving the Stenographic Algorithm LSB”, in the 7th International Workshop on Security in Information Systems (WOSIS 2009), Milan, Italy, P1-11.

Mritha Ramalingam, 2011 “Stego Machine Video Steganography using Modified LSB Algorithm”, in world Academy of science, Engineering of technology 74 2011, PP. 502-505.

Plataniotis K. and Venetsanopoulos, 2000 “Color Image Processing and Application”, Springer.

Stefan Katzenbeisser and Fabien A. P. Patitcolas, 1990” Information Hiding Techniques for steganography and digital watermarking”, Artech House Books, ISBN 1-5853-035-4.

Yi-zhen chen,Zhi Han, Shu-ping Li, Chun-Hui, Xiao-Hui Yao, 2010 "An Adaptive Steganography algorithim Based on Block Sensitivity Vectors using HVS Features", 3rd International Congress on Image and Signal Processing, ISBN: 978-1-4244-6513-2, pp1151 – 1155.