International Journal of Computing and Network Technology

Utilization of Steganographic Techniques in Video Sequences

Hamdy M. Kelash[1], Osama F. Abdel Wahab[1], Osama A. Elshakankiry[1], Hala S. El-sayed[2]

[1]Faculty of Electronic Engineering,Computer Science and Engineering Dep.,Menoufia University,Menouf, Egypt.
[2]Faculty of Engineering, Electrical Engineering Dep., Menoufia University, Shebin El-Kom, Egypt

E-mail: nesreen.hamdy156@yahoo.com, osamaf@hotmail.com, elshakankiry75@yahoo.com, hall_hhh@yahoo.com

Received: 19 Aug. 2013, Revised: 23 Oct. 2013, Accepted: 25 Oct. 2013, Published: 1 Jan. 2014

Abstract: The fast growth in the demand and consumption of the digital multimedia content in the previous period has led to some effective concerns over issues such as content security, digital rights management, and authenticity. Hiding Data is an important way of recognizing copyright protection for digital multimedia.

Digital video/ images became very common choice for hiding data (hold large amounts of data) and the selection of suitable pixels in the video frames, which are used to store the secret data is very important for an effective and successful embedding process . If pixels are not selected sensibly, undesired spatial and temporal perception problems occur in the stego-video. This paper will concentrate on the use of digital video/images as cover to hide data. The proposed steganography algorithm based on color histograms for data embedding into Video Sequences directly, where each pixel in each video frame is divided in two parts, the number of bits which will be embedded in the right part are counted in the left part of the pixel. This algorithm is characterized by the ability of hiding bigger size of data and the ability of extracting the written text without errors, besides it gives a high level of authentication to guarantee integrity of the video/ images before being extracted. Additionally, the data were embedded inside the video/ images randomly which gave the video/ images a difficult security and resistance against extraction by intruders.

Keywords: Steganography,cover video, stego-video, secret message, Peak Signal-to-Noise Ratio (PSNR),Mean Square Error (MSE).

I. INTRODUCTION

With the development of the computer and the increase of its use in different areas of life and work, the issue of security of information had increased special importance. One of the concerns of information security is the concept of hidden exchange of information. For this purpose, various algorithms including steganography, cryptography, and so on, have been used [1]. Some of these algorithms depend on hiding data directly in a special domain, where apart of the image is replaced by the secret message. These Algorithms are characterized by the ability of high storage of data (payload) but they can’t resist hacking. There are other algorithms that depend on changing the image shape into another using discrete cosine functions (Transform Domain), then embedding the secret message inside the new shape of the image. These algorithms are characterized by resisting hacking , but it cann’t hide much data [2].

Researches on information embedding , mostly information hiding techniques, have received considerable attention within the last years due to its possible application in multimedia and information security [3].

A. Basic Model

The basic model of proposed algorithm as shown in Fig.1 uses a cover Video (It used to hold secret data inside), the secret message (the secret data that is to be sent) and an embeding algorithm/technique (the procedure to hide secret message inside cover Video). The result of the process is the stego-video which is the digital video that has the secret message hidden inside. Stego-video is sent to the receiver via public communication channel where receiver will get the secret data out from the stego-video by applying an extracting algorithm/technique.

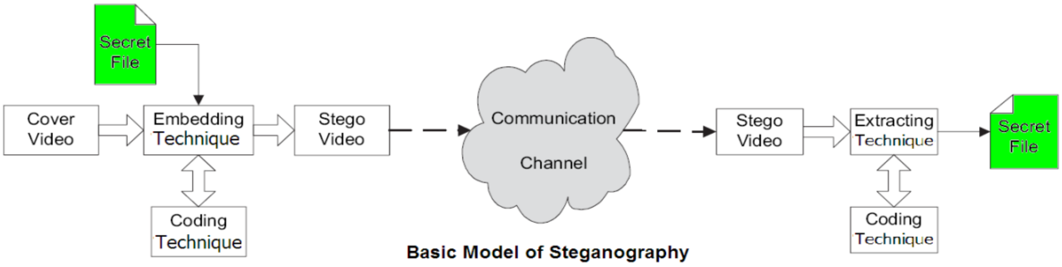

Fig.1 : Basic Model

TABEL 1 – bit Distribution of **16-bit** digital image .

Bit	15	14	13	12	11	10	09	08	07	06	05	04	03	02	01	00
Color	**R**	**R**	**R**	**R**	**R**	**G**	**G**	**G**	**G**	**G**	**G**	**B**	**B**	**B**	**B**	**B**

B. Digital video basics

A digital video consists of a set of frames (images) that are played back at certain frame rates based on the video standards. Quality of the digital video depends on a set of parameters such as the number of pixels in a frame, the fps (frames per second), and frame size .The fps parameter is almost standard (between 24 and 30 fps) in many common video formats, however, the other two parameters present several altered from one video standard to another. Each image, which is called a frame, consists of pixels having three or four color compounds such as RGB (Red–Green–Blue) or CMYK (Cyan–Magenta–Yellow–Black). The rest of the intercessor colors are composed from a mixture of these primary colors [4],[5].Since the human eye is principally sensitive to green color tones, in some video standards the number of bits of each color compound may differ. For example, the red and blue colors are encoded in 5 bits while the green color consists of 6 bits for 16-bit color standard as seen in Table 1. In 24-bit RGB color, each red, green, and blue component is 8 bits long and has 256 variants in color density. In the CMYK standard on the other hand, 32-bit is needed and this standard is ordinarily used in modern computer displays [6].

AVI (Audio Video Interleave), which was advanced by Microsoft and IBM as part of RIFF (Resource Interchange File Format) in 1992, is a most common sequence video format. It acts as containers for various sequences of different data types such as audio and video sequences in which the images are stored in BMP (Bit Map) format. Therefore, capacity and resolution computations on bitmap images can be applied to the AVI video sequences without any major change.

C. Video/Image Steganography

The most popular image formats on the internet are Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and the Portable Network Graphics (PNG). Most of the techniques advanced were set up to use the structures of these formats with some exclusions that use the Bitmap format (BMP) for its simple data structure [6].

The use of digital images for steganography makes use of the weaknesses in the human visual system (HVS), which has a low sensitivity in random pattern changes and luminance. Because of this weakness the secret message can be embedded into the cover video/image without being detected.

As we declared previously, A digital video consists of a set of frames (digital images) that are played back at certain frame rates based on the video standards. The image is a collection of pixels where each pixel is a combination of three colors RGB (Red,Green and Blue). The color of pixel dependent on the numeric value of related with each color. Pixels in the image are displayed row by row horizontally. When data is hidden in the video/images, Stego-video get less troubled as compared to other multimedia files. After hiding data in an image, size of the image increases so compression techniques are necessary. When data is hidden in large size image, the transmission of video/image over the Internet takes more time and needs higher bandwidth. The size of the video/image can be reduced by compression technique. Compression techniques are grouped into two types,

Lossy and lossless.

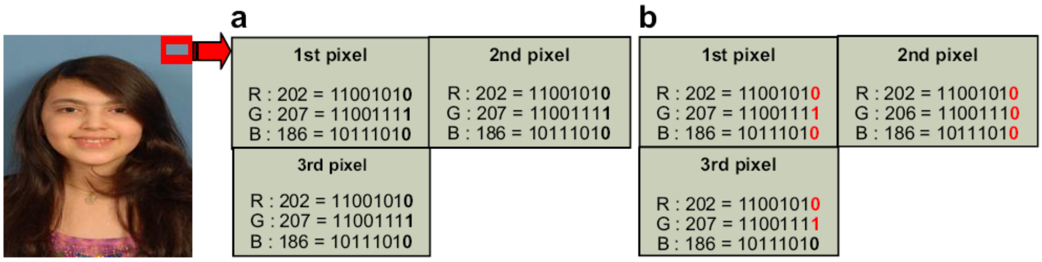

Fig.2 :Embedding the character ‘A’(8-bit ASCII) into an image. (a) Before embedding. (b) After embedding.

There are some of coding techniques are used to hide data in an image and video [7], we are going to discuss some of them below.

1) LSB (Least Significant Bit) Substitution

The LSB is one of the first applied coding techniques in steganography applications [8],[9],[10].This method utilizes spatial embedding techniques and embeds the secret data into the cover image or video in which the pixels are subject to slight alterations. Therefore, it is almost impossible for the HVS to be attracted by these slight changes and the potential adversary attacks will be reduced. Although this coding method integrates a simple mechanism in many applications,it exposures some signs of weakness. For example, to recover the secret data from the cover image or video, the structure of the bit order should be kept as it is. Noise, filtering, clipping, color spatial transformations, and re-sampling are the weakest states of the LSB technique. In addition, this method can be affected by lossy compression algorithms so that the extraction of the secret data cannot be guaranteed in applications where compressed video streams are used.

The character ‘A’ has an ASCII code of 65 in decimal and it matches to binary code of ‘‘01000001’’. To hide the character ‘A’ into the image above, eight bits are needed in the RGB code as seen in Fig.2. Since each pixel can offer three bits (least significant bits of each color compound) for storage, three pixels are sufficient to implement the hiding processes.

2) RGB-weighted

The RGB-weighted coding technique has been accepted from an earlier [11], since the LSB coding technique can’t meet the requirements. In this technique, a pixel collected of three prime colors of RGB (89,143,240) supposes that the distribution of the prime colors will have the following color weights: R = 89, G = 143, B = 240. Let the letter ‘s’ (ASCII code: 115) embed into this pixel. As seen in Fig. 3, initially the last digits of each compound value are reset so we have new RGB codes (R = 80, G = 140, B = 240). After that each digit of character ‘s’ is subtracted from 10 (10 - 1 = 9, 10 - 1 = 9, 10 - 5 = 5) and these digits replace the last digits of the RGB codes. At the end, the latest RGB (R = 89, G = 149, B = 245) is obtained.

In the decoding phase, the last digits of the pixel are subtracted from 10 (10 - 9 = 1, 10 - 9 = 1, 10 – 5 = 5) to recover the original embedded ASCII code ; however, there are some cases where exceptional outcomes appear Fig. 4. If the original RGB values are between 250 and 255, the algorithm produces invalid results. To overcome this problem, each RGB composite is reduced by 10. Another complicated case is that the first digit of the ASCII code starts with zero (A = 065).

In this case, the result is expected as 10 - 0 = 10; however, this is certainly a fault. Therefore, we have adjusted the algorithm accordingly so that the exceptional cases have been Eliminated [12].

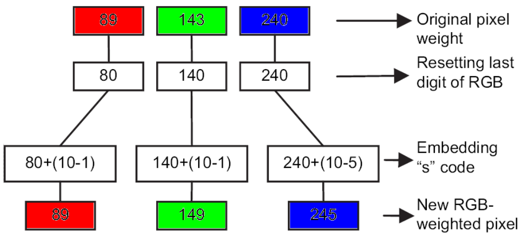

Fig.3 : Hiding an ASCII code into a pixel .

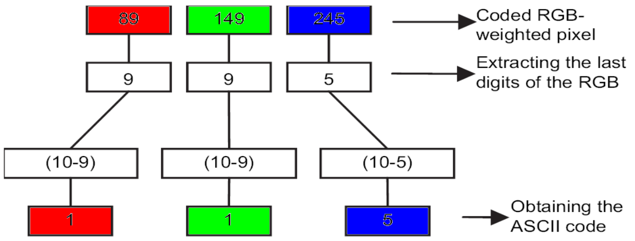

Fig.4 : Extraction process of the ASCII code.

This paper is ordered as follows. Section II, we discuss the relevant research work of the histogram-based data hiding approaches. Section III, describes our proposed method. Section IV demonstrates the experimental results, and conclusions are given in Section V.

II. RELATED WORK

O.CETIIN et al. [12] proposed two new steganographic algorithms are using alike histograms and unlike histograms. Both algorithms are based on selecting appropriate pixel methods by focusing on perceptibility and capacity parameters of the cover video. They used LSB (least significant bit) and RGB-weighted coding techniques. When compared to traditional steganographic techniques, they improved temporal and spatial perception levels in the stego-video, offered a relatively high data-embedding capacity and also enhanced the maximum hiding capacity (MHC) of the cover video, as a result of this the peak signal-to-noise ratio (PSNR) values of the stego-image in each video frame have been enhanced .

Lin et al. [13] studied a several of schemes by which the histogram was constructed using a difference image to realize the task of reversible data hiding. The aim of this treatment was to present a more centralized histogram, which in turn may raise the heights of peak points and thus improve the capacity upon the histogram-based methods. Yang et al. [14] proposed a new scheme utilizing column-based interleaving predictions to enhance the performance of Lin et al.'s histogram-based method.

In this scheme, the odd-column pixels are predicted by pixels in even columns; then the even-column pixels are predicted by pixels in odd columns, or vice versa.

Due to the prediction errors being reduced significantly by these schemes, the embedding capacity can be mostly increased by raising the heights of peak points in the histogram. Moreover, the difference between the original and updated values of each pixel remains within small rang after secret data embedding ,there by warranting that the peak signal-to-noise ratio (PSNR) of the stego-image in each video frame is above 47 dB.

III. Algorithm

Histograms, arrays of values, indicate the distribution of intensity of colors obtained from each pixel's color combination in digital image.The proposed algorithm based on color histograms for data embedding into cover video/images directly, where the cover video is firstly segmented into frames and the histogram values of each frame are calculated. In order to determine suitable pixels in each video frame for data embedding; first, an calculating value is computed using the color and motion transitions in each frame by our application MATLAB software that we have developed. A predefined threshold value, controlled by a track bar control on the software user interface.The threshold value, which can be as much as the highest pixel number of the video frame, indicates a certain level of disparity between successive video frames. Histogram variations of consecutive video frames are compared to the threshold value (Histogram constant Value HCV) and appropriate pixels in those frames are selected for data embedding procedures, the higher the threshold values are ,the more the perceptibility precision is increased at frame transitions in contrast to a decrease in the number of segmented frames. This consequently means a capacity drop for the embedded data. If the threshold value is configured as low, parameter values mentioned above will be inverse, So each pixel in each video frame is divided in two parts, the number of bits which will be embedded in the right part are counted in the left part of the pixel. The detail of the embedding and extracting algorithms are shown in the following subsections.

A. Video's Segmentation and select pixels in frames

The data hiding method is initiated by segmentation of cover-video file into the frames, the average histogram values of frames (Fig. 5) are calculated and appropriate frames are determined in respect to the HCV parameter.The flowchart of our proposed scheme is shown in Fig. 6 and Fig. 7.

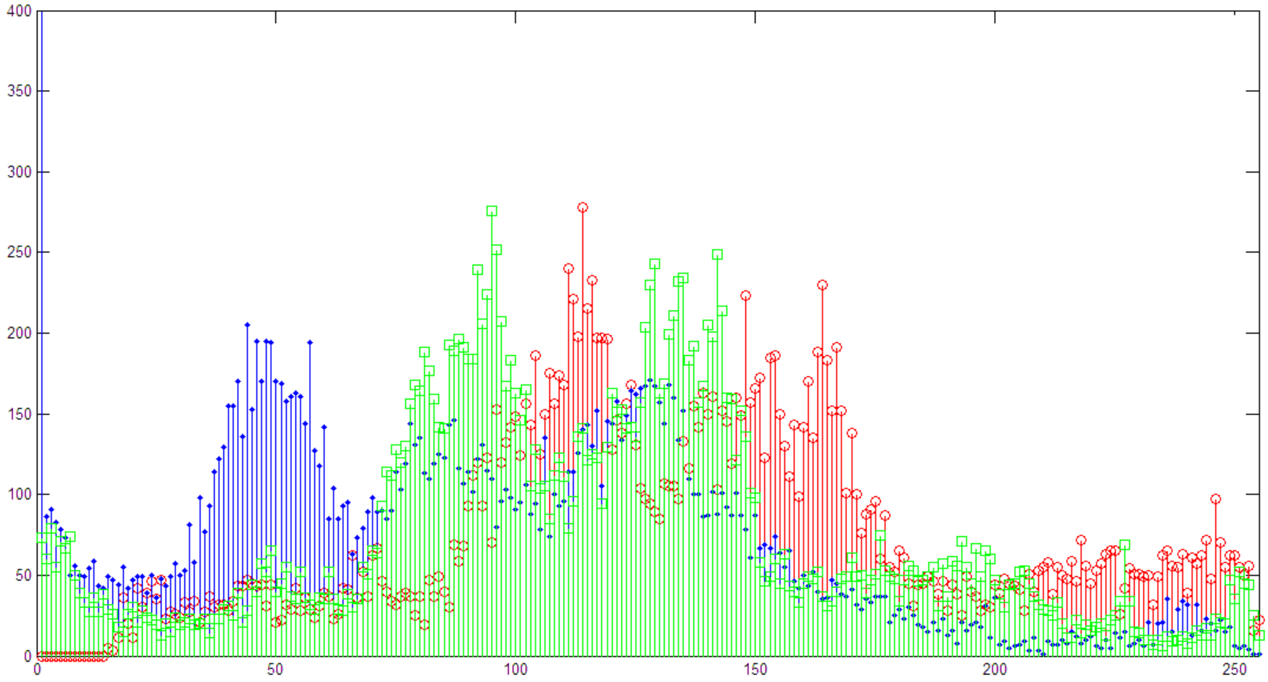

Fig.5 : Histogram of R,G,B Values in one frame of cover video

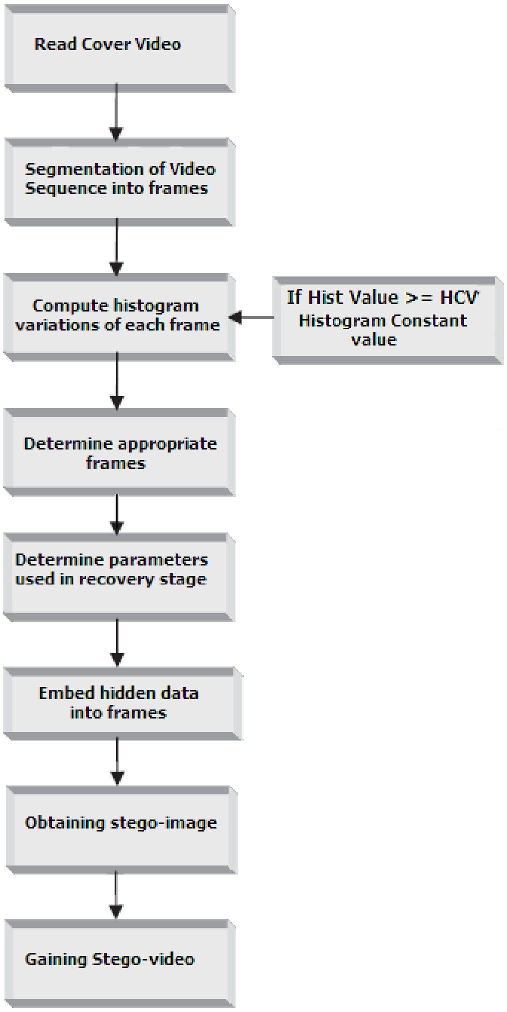
Read Cover Video
Segmentation of Video Sequence into frames
Compute histogram variations of each frame
If Hist Value >= HCV Histogram Constant value
Determine appropriate frames
Determine parameters used in recovery stage
Embed hidden data into frames
Obtaining stego-image
Gaining Stego-video

Fig. 6 : Flowchart of embedding Algorithm

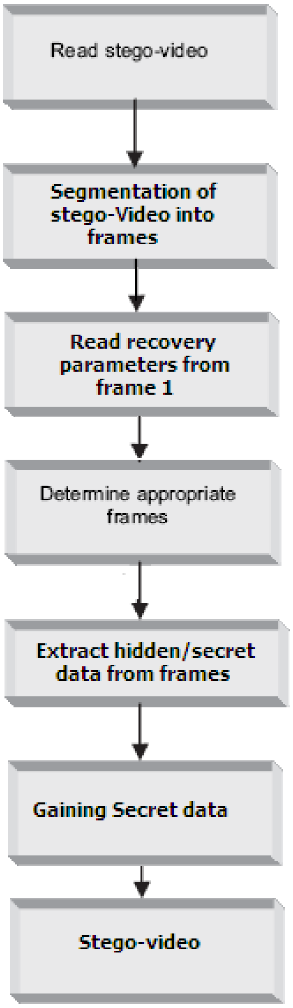
Read stego-video
Segmentation of stego-Video into frames
Read recovery parameters from frame 1
Determine appropriate frames
Extract hidden/secret data from frames
Gaining Secret data
Stego-video

Fig. 7 : Flowchart of extracting Algorithm

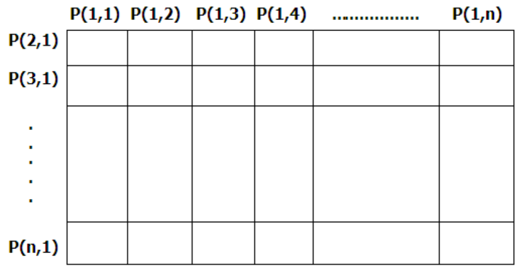

Fig.8 : Frame divided into blocks

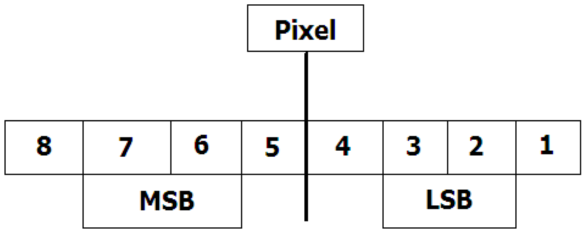

Fig.9 : Pixels divided into 2 parts MSB and LSB

1- Firstly each selected frame will divide into blocks (n x n) as shown in Fig.8 and then appropriate pixels are determined by comparing consecutive blocks in the frame.

2- For each block calculate difference value for each two consecutive pixels ( ) from equation **(1)**

$$\mathbf{D_i} = |(\mathbf{P_i} \quad \texttt{===}\!\!\rightarrow \mathbf{(1)}$$

3- For each block calculate **Median** , then calculate **M** parameter from equation **(2)**

$$\mathbf{M=FIX(} \qquad \mathbf{)} \quad \texttt{===}\!\!\rightarrow \mathbf{(2)}$$

4- Each pixel in each video frame is divided into two parts MSB and LSB as shown in Fig.6 and count **NUM** = numbers of 1's in MSB part .

B. *Embedding Algorithm*

The flowchart is shown in Fig.6.
Input : Secret Data , original selected frames of cover video
Use equations (1) and (2) to Compare for each consecutive pixels with value of M

1-If , then Embed data
in pixels ( ) .
2-If , then no data embed
in pixels ( ) .
3-If NUM = 0 or 4
Embed 1 secret Bit in LSB part.
4-If NUM = 2
Embed 2 secret Bit in LSB part.
5-If NUM = 1 or 3
Embed 3 secret Bit in LSB part.

Output : Stego image , stego-video.

C. *Extracting Algorithm*

The flowchart is shown in Fig. 7.
Input : Stego-video, Stego image for selected frames of Stego-video
Use equations (1) and (2) to Compare for each consecutive pixels with value of M

1-If , then Extract data
from pixels ( ) .
2-If , then no data
in pixels ( ) .
3-If NUM = 0 or 4 Extract 1 secret Bit
from LSB part .
4-If NUM = 2 Extract 2 secret Bit
from LSB part .
5-If NUM = 1 or 3 Extract 3 secret Bit
from LSB part .

Output : Secret Data , stego-video.

IV. EXPERIMENTAL RESULTS

The challenge of using steganography in cover video is to hide as much data as possible with the least noticeable difference in the stego-video. As a performance measurement for image and video distortion , a practicable objective measures for this property are the Mean Squared Error (MSE) and the Peak Signal to Noise Ratio (PSNR) between the cover video and the stego-video .

Mean Square Error (MSE) : It is the measure used to quantify the alteration between the initial and the distorted or noisy video.

Mean Square Error is computed using the following formula [15] :

$$\mathrm{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\|O(i,j) - S(i,j)\|^2 \quad \text{or}$$

$$\mathrm{MSE} = \frac{\sum_{m,n}[O(i,j) - S(i,j)]^2}{m \times n}$$

Where ''O'' and ''S'' are the original video and stego-video respectively to be compared and their image sizes are m X n . From (MSE) we can find Peak Signal to Noise Ratio (PSNR) which measures the quality of the video by comparing the original video with the stego-video. (PSNR) is used to evaluate the quality of the stego-video after embedding the secret message in the cover video. It is computed using the following formula [15]-[22] :

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

Where, MAX is the number of bits that represent a pixel in a frame (image) . For example, MAX is 255 when pixels are presented by 8 bits .The PSNR parameter is computed on the intensity portion of the images.The number of faded bits depends on hidden data capacity (HDC) and the perceptibility level. In fact, conventional PSNR measurements do not correspond to an individual's perception. PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30 dB indicate a fairly low quality, i.e., distortion caused by embedding can be obvious; however, a high quality stego-image should struggle for 40dB and above.

In this section, we report the experimental results comparing our method with the O.CETIIN et al. [12] schemes. To show the performance of the proposed algorithm , we implement the schemas shown by O.CETIIN et al. [12] ,the proposed algorithm in this paper is using MATLAB software. The embedded message was generated by repeat a predefine message until embedded message with required length is generated. We used 'scenevideoclip.avi' and 'vipmen.avi ' as test cover video file from under MATLAB software toolbox folder . We used PSNR (peak signal to noise ratio) to measure the distortion between the original video and Stego-video.

The proposed algorithm able to hide messages within part of the frames or the whole Frames based on HCV value and the random selection of frames and pixels increases the level of security to hide and extract the secret messages.

The obtained outcomes are shown in Table 2. From the obtained results we can conclude that the embedding capacity in the proposed algorithm is very good. also, the PSNR in the table shows that the image quality is very good and has higher level of security as compared to other algorithms.

TABLE 2 : The number of faded pixels in varied coding techniques

Cover video size (byte)	Hiding file size (byte)	Faded pixels in cover video			
		Proposed Algorithm		LSB coding	RGB coding
		Proposed coding	PSNR		
'vipmen.avi ' 1,522,0624	73	69	47.91	195	73
	1800	1710	48.11	4800	1800
	27,648	26,265	48.32	73,728	27,648
	46,080	43,776	48.40	122,880	46,080
	54,784	52,044	48.45	146,091	54,784
	103,424	98,252	48.56	275,798	103,424
	145,408	138,137	48.81	387,755	145,408
	168,960	160,512	48.84	450,560	168,960

V. CONCLUSION

In this paper, The goal of the proposed algorithm is to decrease the faded pixels in each frame , in order to increase the embedding capacity.

The experimental outcomes showed that the proposed algorithm is improve the embedding capacity , maintains the quality of the stego-video, more efficient, simple, appropriate and accurate than other algorithms, as well as it makes the secret message more secure.

REFERENCES

[1] M. H. S. Shahreza and M. S. Shahreza, "Arabic/Persian Text SteganographyUtilizing Similar Letters With Different Codes", the Arabian Journal for Science and Engineering, Volume 35, Number 1b pp. 213 - 222, April 2010.

[2] Kavitha, Kavita Kadam, Ashwini Koshti and Priya Dunghav, "Steganography Using Least Signicant Bit Algorithm", International Journal of Engineering Research and Applications (IJERA), issn: 2248-9622, Vol. 2, Issue 3, pp. 338 - 341, May - Jun 2012.

[3] T.Shanableh," Data hiding in mpeg video files using multivariate regression and flexible macroblock ordering ", IEEE Transactions on Information Forensics and Security , Vol. 7, pp.455-464 , 2012 .

[4] Wang H., Wang S.,"Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM-Voting Systems,Vol. 47, No. 10, pp. 76-82, 2004.

[5] Chincholkar A.A. and Urkude D.A., "Design and Implementation of Image Steganography", Journal of Signal and Image Processing, ISSN: 0976-8882 & E-ISSN: 0976-8890, Volume 3, Issue 3, pp. 111-113, 2012.

[6] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad and Osamah M. Al - Qershi, "Image Steganography Techniques : an Overview", International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue(3) : 2012.

[7] Adhiya K.P., Patil S.A.,"Hiding Text in Audio Using LSB Based Steganography", Information and Knowledge Management, Vol. 2, No. 3, pp. 8-15, 2012.

[8] Noda, Furuta T., Niimi M., Kawaguchi E.,"Application of BPCS steganography to wavelet compressed video", International Conference on Image Processing: (ICIP, 2004), IEEE, Singapore, pp. 2147-2150, 2004.

[9] Wang RZ, Lin CF, Lin JC. Image hiding by optimal LSB substitution and genetic algorithm.Pattern Recognition 2001; 34:671–83.

[10] Akar F, Varol HS. A new RGB weighted encoding technique for efficient information hiding in images.Journal of Naval Science and Engineering July 2004;2:21–36.

[11] Tulu B, Chatterjee S. Internet-based telemedicine: an empirical investigation of objective and subjective video quality.Decision Support Systems November 2008;45(4):681–96.

[12] O.CETIIN and A.OZCERIT, "A new Steganography Algorithm Based on Color Histograms for Data Embedding into Raw Video Streams ", Elsevier Ltd ,Computers & Security, Sakarya University, Turkey,Vol.28, pp. 670-682 , 2009.

[13] Lin C.C., Tai W.L., and Chang C.C.: `Multilevel reversible data hiding based on histogram modification ofdifference images', Pattern Recognition, 2008, 41, pp. 3582-3591.

[14] Yang C.H., and Tsai M.H.: `Improving Histogram-based Reversible Data Hiding by Interleaving Predictions', IET Image Processing, 2010, 4, pp. 223-234.

[15] Netravali AN, Haskell BG. Digital pictures: representation,compression, and standards. 2nd ed. New York, NY: Plenum Press; 1995.

[16] Radwan, A. A., Swilem, A. and Seddik, A. H., " A High Capacity SLDIP (Substitute Last Digit In Pixel) Method", Fifth International Conference On Intelligent Computing And Information Systems (ICICIS 2011), 30 June - 3 July, 2011, Cairo, Egypt.

[17] Rabbani M, Jones PW. Digital image compression techniques, vol. TT7. Bellvue, Washington: SPIE Optical Engineering Press; 1991.

[18] Petitcolas F.A.P., Anderson R. J., Kuhn M. G., "Information Hiding- A Survey", Proc. of the IEEE special issue on protection of multimedia content, Vol. 87, No. 7, pp. 1062–1078, 1999.

[19] Sharma V.K., Shrivastava V.,"A steganography algorithm for hiding image in image by improved LBS substitution by minimize detection", Journal of Theoretical and Applied Information Technology, Vol. 36, No. 1,pp. 1-8, 2012.

[20] Singh N., Bhati B.S., Raw R.S.,"Digital image Steganalysis for computer forensic investigation", Computer Science and Information Technology (CSIT), pp. 161-168, 2012.

[21] Zaidan, A., B. Zaidan,"Novel approach for high secure data hidden in MPEG video using public key infrastructure", International Journal of Computer and Network Security,Vol. 1, No. 1, pp. 71-76, 2009.

[22] Kakumanu P, Makrogiannis S, Bourbakis N. A survey of skin-color modeling and detection methods. Pattern Recognition 2007: 1106–22.

Hamdy M. Kelash received the Eng. Degree from the Institute of Electronic Engineering, Egypt in 1971, MSc degree from Faculty of Engineering Technology , Helwan University, Egypt, in 1979 and the PHD degree from Institute National Polytechnique (INP) , France in 1984. He has been lecturer in 1984 at the Electronic Industry department, Faculty of Electronic Engineering, also a lecturer in 1987 at the Computer Sciences and Engineering department, and an Assistant Professor in 1993 and the Head of Computer Sciences and Engineering department, Faculty of Electronic Engineering, Menoufia University from 2001 to 2007. His main research interests include optical computing, artificial intelligence, network security, image processing, digital systems and parallel computing.

Osama Fouad Abdel Wahab received BSc.Eng. in Computer Science & Engineering from Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt in 1991 and He is now pursuing M.Sc. in computer science .

He is currently working as a ICT consultant and a Lecturer at Kuwait University . His research topics include information, Network, Internet and Multimedia Security, Cryptography, Steganography and steganographic algorithms for video applications.

Osama A. Elshakankiry received a B.S. in Computer Science & Engineering from Faculty of Electronic Engineering, Menoufia University, Egypt in 1998, a M.Sc. in Computer Science & Engineering from Faculty of Electronic Engineering, Menoufia University, Egypt in 2003, and a Ph.D. in Computer Science from School of Computer Science, Faculty of Engineering and Physical Sciences, University of Manchester, UK in 2010. He was appointed as a demonstrator at the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, from 1999 to 2003. He became an assistant Lecturer in 2003 and promoted to a Lecturer in 2011. His research interests cover Network Security, Internet Security, Multimedia Security, Cryptography, and Steganography .

Hala S. El-sayed

received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from Menoufia University, Shebin El-kom, Egypt, in 2000, 2004, and 2010, respectively. She is currently with the Department of Electrical Engineering, Faculty of Engineering, Menoufia University, where she was a Demonstrator from 2002 to 2004 and has been a Lecturer since 2010. Her research interests cover Network security, Wireless sensor network, Secure building automation systems, and Biometrics.