Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.365 – 370

RESEARCH ARTICLE

A Secured Text Transmission Through Video Using Modified Status Bit LSB along With RSA Cryptography

Rajakumar Loni[1], Mrs. D.Kavitha[2]

[1]M.Tech Digital Electronics and Communication MVJ College of Engineering, Bangalore, India

[2]Asst. Professor, Department of Electronics and communication, MVJ College of Engineering, Bangalore, India

[1] rajkumarloni73@gmail.com

[2] kavis_san04@yahoo.com

Abstract— Using steganography techniques the data can be hidden inside a cover media such as text, audio, video, and image. In the proposed technique, a new steganography technique is being developed to hide large data in Bitmap image using filtering based algorithm, which uses MSB bits for filtering purpose. This method uses the concept of status checking for insertion and retrieval of message. The traditional LSB method has imbalanced embedding distortion and vulnerable to steganalysis. The proposed method will able to hide large data in a video retaining the advantages and discarding the disadvantages of the traditional LSB method. For better security RSA cryptography technique has also been used in the proposed method. Before applying the steganography technique, RSA cryptography will change the secret message into cipher text to ensure two layer security of the message. In the proposed method, video is distributed into the photo frames using a mat lab code and all the frames are sequentially stored. Using new steganography technique text data is embedded in each frame. After the completion of embedding data all the images are placed in a sequential manner and then all the frames are cascaded for generation of the original video file with encryption.

Keywords- LSB steganography, RSA Cryptography, Darker pixel, Lighter pixel

I. INTRODUCTION

Communicating secret data through an open insecure medium poses many security threats. So in order to transmit the data securely information hiding concept is introduced. The best known Steganographic method that works in the spatial domain is the Least Significant Bit (LSB) method, which replaces the least significant bits of pixels selected to hide the information. The medium where the secret data is hidden is called as cover medium; this can be image, video or an audio file. Any stego algorithm removes the redundant bits in the cover media and inserts the secret data into the space. Higher the quality of video or sound more redundant bits are available for hiding. Traditionally, steganography was based on hiding secret information in image files. But modern work suggests that there has been growing interest among research fraternity in applying steganographic techniques to video files as well. The advantage of using video files in hiding information is the added security against the attack of hacker due to the relative complexity of the structure of video compared to image files.

Sometime steganography will not cover the total security of secret massage. So an additional security need to the secret message. For this purpose we combine cryptography technique with steganography. In the proposed technique RSA (Rivest-Shamir-Adleman) cryptographic algorithm is used for additional security. RSA is an asymmetric algorithm based on Chinese

Remainder Theorem i.e. factoring two large prime numbers. The key sizes ranges from 1024 to 4096 bits and it is secure so far as per NIST. It employs two different keys related mathematically such that one is used for encryption and the other for decryption.

II. LITERATURE SURVEY

Several steganographic methods have been proposed in literature and most of which are performed in pixel domain. However major contribution is in the domain of Image Steganography. The existing methods are mainly based on LSB where LSBs of the cover file are directly changed with message bits. In [3] a robust image steganography technique based on LSB insertion and RSA encryption technique has been used. Masud et.al [4] has proposed a LSB technique for RGB true color image by enhancing the existing LSB substitution techniques to improve the security level of hidden information. S. Roy and R. Parekh proposed an improved steganography approach for hiding text messages within lossless RGB images which will suffer from withstanding the signal processing operations [5]. Video steganography of late has also gained quite significance for researchers. Various techniques of LSB exists, where [6] proposes the data is first encrypted using a key and then embedded in the carrier AVI video file in LSB keeping the key of encryption in a separate file called key file. Whereas in [7] selected LSB steganography algorithm is proposed. Other steganography techniques in uncompressed raw video, is illustrated [8], [9] and [10]. Steganography techniques for compressed video stream can be found in [11], [12] and [13].Another video steganography scheme based on motion vectors and linear block codes has been proposed in [14].

III. OVER VIEW OF PROPOSED TECHNIQUE

In the proposed technique, .AVI file is taken as cover video and secret text is taken from notepad as input. At the transmitting end, the cover video is segmented into frames. Simultaneously secret text is segmented in such way that the distribution of text in each frame is same. First step of encoding is that to convert the secret text into cipher text using RSA algorithm. Next step is to hide the text inside the frame using Status Bit LSB Steganographic technique. These two steps are applied to each frame. After the completion of hiding the text in frames, all the frames arranged together in sequential manner to make video. The video containing the secret text is called stego video.

At the receiving end, stego video is segmented into frames. Then each frame is taken one by one and cipher text hidden is retrieved using Status Bit LSB de-steganography technique. This cipher text is decrypted into secret text using RSA decryption algorithm. These two steps are applied to all the frames. The secret text obtained from each frame is combined to make original text.

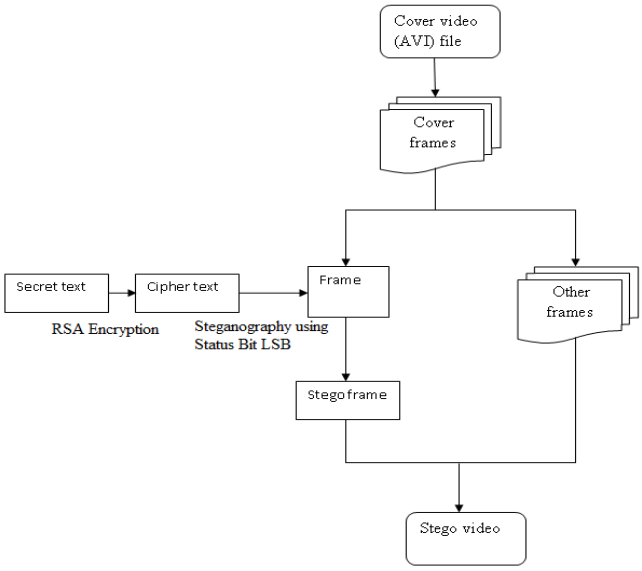


Fig1: Encoding block diagram

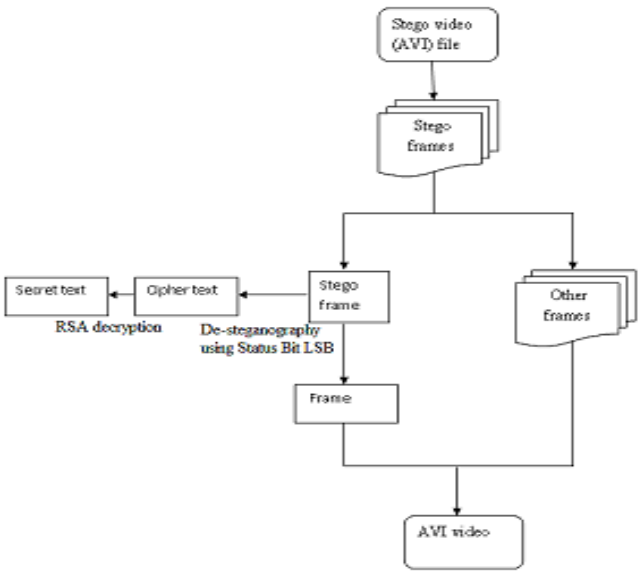


Fig2: Decoding block diagram

IV. NEW STEGANOGRAPHIC TECHNIQUE

A digital frame consists of different pixels. A colored pixel consists of red, green and blue color component. Each color level is represented by 8 bits in binary notation. Therefore 24 bits (3 bytes) are required to denote a pixel. In the proposed technique, a bit of the entire text data is embedded into the pixel. This technique uses MSB (Most Significant Bit) bit for hiding the information.MSB bit specifies the area where to embed the text. This technique has the concept of randomly select a frame and find if it is lighter or darker frame. Lighter frame means MSB bits of Red, Green, and Blue component of a pixel consists of at

least 2 bit 1's and darker frame means MSB bits of Red, Green, and Blue component of a pixel consists of at least 2 bit 0's. If darker pixel is greater than lighter pixel, a darker pixel area is selected to embed the text and vice versa. Following figure depicts this concept.

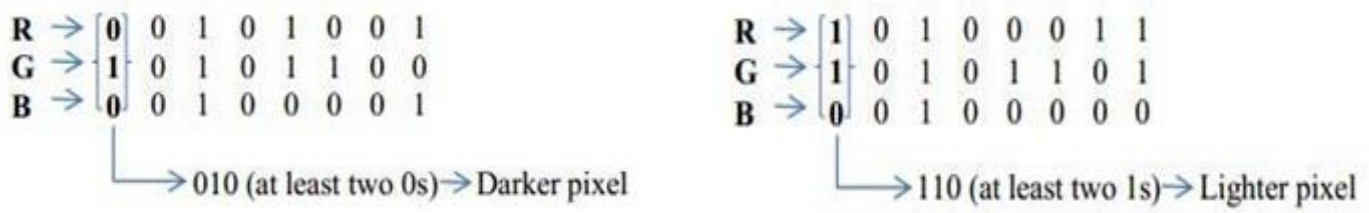


Fig3: Concept of lighter and darker pixel

A. Embedding Process: First step is to collect the MSB bit of Red, Green and Blue component of pixel one by one. Next step is to find the number of lighter and darker pixels in a frame. If the number of lighter pixels is greater than darker pixels, a text data is embedded only in lighter area and if the number of darker pixel is greater than the lighter pixels, a text data is embedded only in darker area.

1) Embedding Text in Lighter Area: If the MSB bits Red, Green and Blue component consists of at least two bit 1, and then this pixel is chosen for hiding the text bit. The decimal equivalent representation D_n of the MSB bits are used for validating the LSB bit. If the text bit T_n and the bit position D_n of 3rd byte (blue color component) are same, that means true, then change the LSB of 3rd byte into 1 or 0, otherwise. In this approach the text bit is embedded into the cover frame.

2) Embedding Text in Darker Area: If the MSB bits Red, Green and Blue component consists of at least two bit 0, and then this pixel is chosen for hiding the text bit. The decimal equivalent representation D_n of the MSB bits are used for validating the LSB bit. If the text bit T_n and the bit position D_n of 3rd byte (blue color component) are same, that means true, then change the LSB of 3rd byte into 1 or 0, otherwise. Here there is one more condition that is if all 3 bits of MSB are 0, then decimal equivalent value of MSB bits is 0. In this situation text bit will be directly embedded into the LSB of Blue color component. In this approach the text bit is embedded into the cover frame.

3) Embedding flowchart:

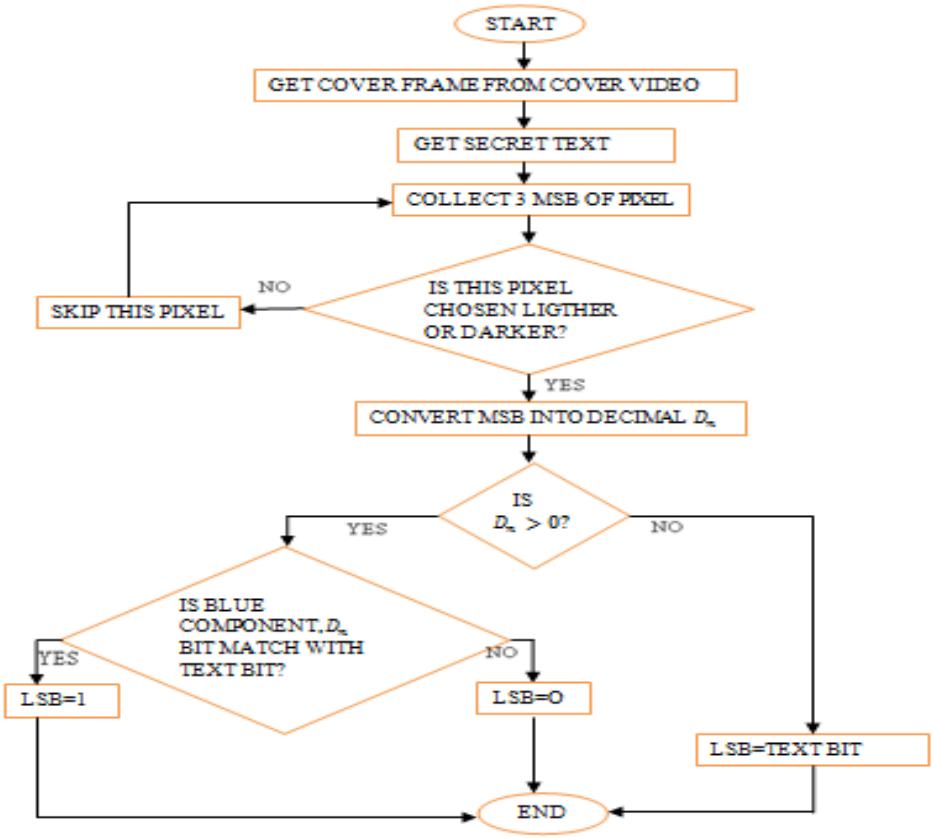


Fig4: Embedding flowchart

B. Extracting Process

First step is to collect the stego frame. Check whether it is lighter or darker frame. If it is lighter frame then the text is extracted from corresponding lighter pixels and if it is darker frame then the text is extracted from corresponding darker pixels.

1) ***Extracting Text from Lighter Pixel:*** First, collect the 3 byte of a pixel. Then collect the MSB bit of the 3 byte and check whether it consists of at least 2 bits with 1. If it contains at least 2 bits with 1, then the decimal equivalent representation D_n of the 3 MSB bits is taken. The LSB bit of the 3rd byte of the chosen pixel indicates the cipher text bit. If LSB bit is 0 that's mean false then the bit position D_n of 3rd byte checked. If D_n bit is 0, extract text bit 1 or 0, otherwise. If the LSB bit is 1 that's mean true then the bit position D_n of 3rd byte checked and extract the text bit as same as the D_n bit of the 3rd byte. This approach will be continued until all the text bit is extracted from the stego frame.

2) ***Extracting Text from Darker Pixel:*** First, collect the 3 byte of a pixel. Then collect the MSB bit of the 3 byte and check whether it consists of at least 2 bits with 0. If it contains at least 2 bits with 0, then the decimal equivalent representation D_n of the 3 MSB bits is taken. The LSB bit of the 3rd byte of the chosen pixel indicates the cipher text bit. If LSB bit is 0 that's mean false then the bit position D_n of 3rd byte checked. If D_n bit is 0, extract text bit 1 or 0, otherwise. If the LSB bit is 1 that's mean true then the bit position D_n of 3rd byte checked and extract the text bit as same as the D_n bit of the 3rd byte. Here there is one more condition that is if all 3 bits of MSB are 0, then decimal equivalent value of MSB bits is 0. In this extracted text bit will be the LSB of Blue color component. This approach will be continued until all the text bit is extracted from the stego frame.

3) Extracting flowchart

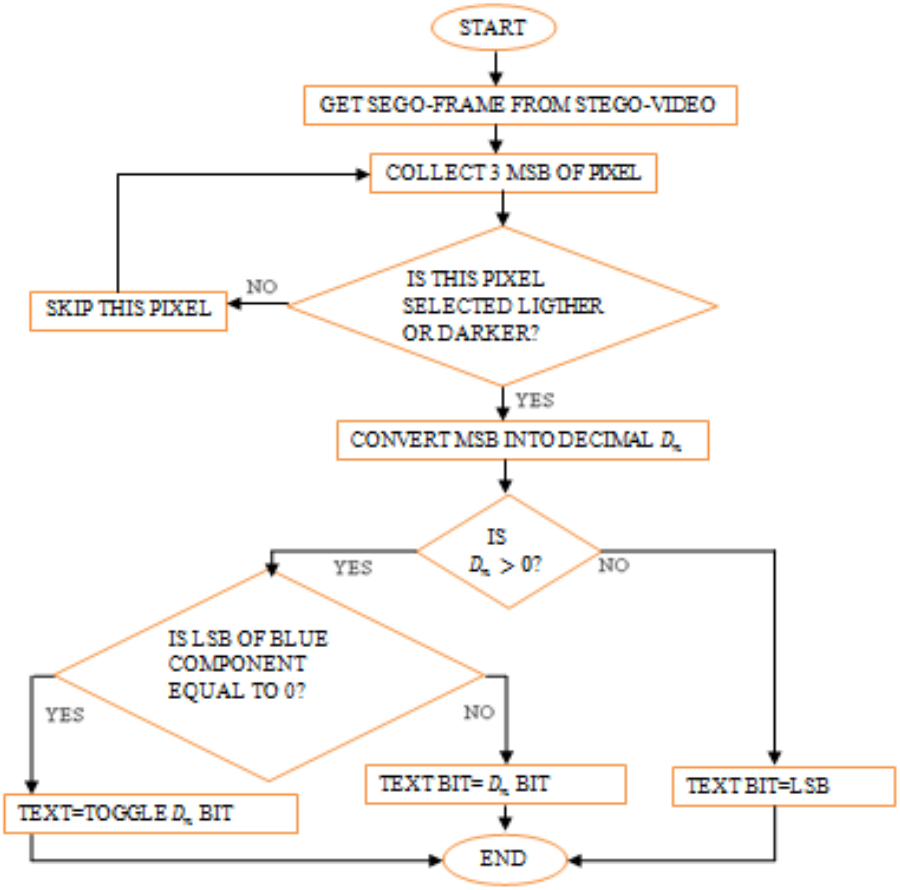


Fig5. Extraction flowchart

V. SIMULATION RESULTS

Experiments are carried on a computer system, having Intel core to duo processor 2.0 GHz clock and 2 GB RAM. After breaking the video into frames, a color component has been chosen into which the message is embedded. The simulation tool is MATLAV v8.1. I have used the functions for video processing on the uncompressed AVI format. Secret information will be kept in windows DAT file and supporting information will be stored in the MATLAB data files.

A. Secret message input and output of RSA algorithm: The secret message that the sender wants to send to the receiver is kept in a data file. We are not taking it from the console since it should not be visible to everyone. The person responsible for the secret

message can give this message file input to the sender module. This text will be read from the file and will be converted into binary message string. This string will now be the secret information to transferred and embedded into the video frames.

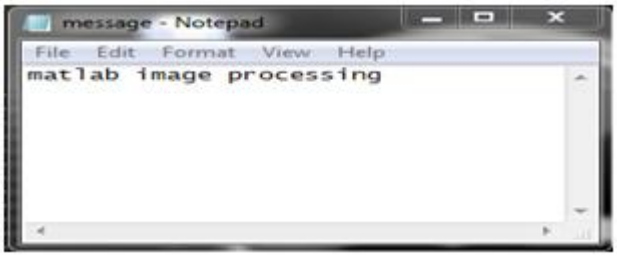


Fig 6: Input

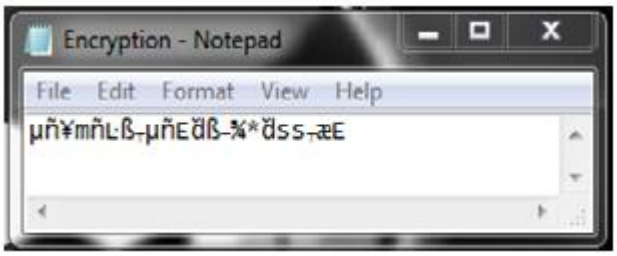


Fig 7: Output of RSA

B. Visual comparison of frames:

The randomly selected frame from the original video and same frame from the Stego video are shown in the figure below. There is no visually perceptible difference in the proposed algorithm.

Fig 8: Original frame

Fig 9: Stego frame

C. Histogram Comparison of the frames before and after data:

Following histograms represents the frequencies of various intensities in a randomly chosen frame before and after the embedding. There is no difference in the histograms. The peaks are same in both so a histogram comparison cannot predict that the data is contained in the video and our message is safe.

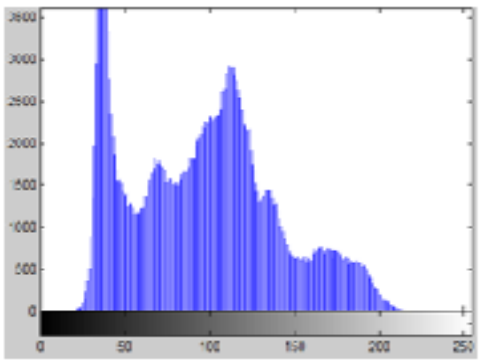


Fig 10: Histogram of original frame

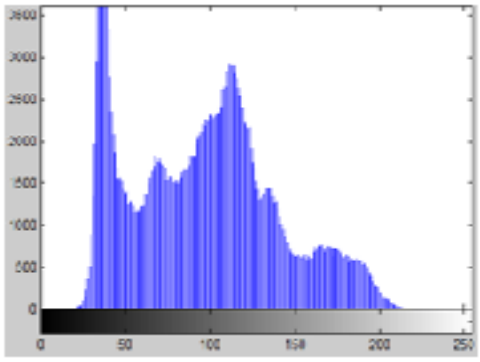


Fig 11: Histogram of stego frame

D. Peak Signal to noise ratio:

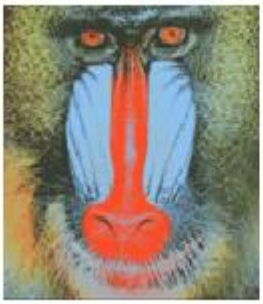
Peak Signal-to-Noise Ratio (PSNR) measures the quality of two images, the watermarked image and the original host image. The PSNR and the NC are calculated as follows:

$PSNR = 10\ log_{10}(255^2/MSE)$

$$MSE = \frac{1}{A \times B}\sum_{i=0}^{A}\sum_{j=0}^{B}(X(i,j) - Y(i,j))^2$$

Where X and Y are the original and watermarked images respectively of size A*B represent the height and width of the images. The calculated PSNR values for standard 512×512 images by applying modified status bit LSB algorithm are as follows.

Lena.png



Baboon.bmp

Cover Image	No of bits Hidden	PSNR (in db)
Lena.png	10,000	70.0674
	20,000	67.0839
	50,000	63.0741
Baboon.bmp	10,000	70.0648
	20,000	67.0515
	50,000	63.1350

Table1. PSNR of different cover images

VI. CONCLUSION

In the proposed technique, the goal is not to increase the capacity of the message but tried to make it difficult to the unauthorized person to determine the presence of a secret cipher. In ordinary LSB Steganography technique only message bit will be replaced with the LSB bit of the image but out algorithm does not just replace the message bit but it would replace the status of the message bit. Moreover, we merge Cryptography with it so that the secret message can be secured by two security layers. So, the proposed technique fulfills the requirement of Steganography technique.

REFERENCES

[1] Viral, G.M. ; Jain, D.K. ; Ravin, S. *"A Real Time Approach for Secure Text Transmission Using Video Cryptography",* proceedings of 2014 Fourth International Conference on Communication Systems and Network Technologies (CSNT), IEEE Conference Publications, pp 635-638, 2014.

[2] Islam, M.R. ; Siddiqa, A. ; Uddin, M.P. ; Mandal, A.K. ; Hossain, M.D. *"An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography",* proceedings of 2014 International Conference on Informatics, Electronics & Vision (ICIEV), IEEE Conference Publications, pp 1-6, 2014.

[3] Fillatre. L, *"Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption, IEEE Transactions on Signal Processing",* Volume 60, Issue:2, pp. 556-569, Feb, 2012

[4] Masud K. S.M. Rahman, Hossain, M.L., *"A new approach for LSB based image steganography using secret key",* in Proceedings of 14th International Conference on Computer and Information Technology (ICCIT-2011), pp.-286-291, Dec. 2011.

[5] S. Roy and R. Parekh, *"A Secure Keyless Image Steganography Approach for Lossless RGB Images."* Proceedings of International Conference on Communication, Computing & Security, ACM Publications, 573-576, 2011.

[6] Mritha Ramalingam, Stego Machine,*"Video Steganography using Modified LSB Algorithm",* in World Academy of Science, Engineering and Technology 74 2011, pp. 502-505, 2011.

[7] Juan Jose Roque and Jesus Maria Minguet, *"SLSB: Improving the Steganographic Algorithm LSB",* in the 7th International Workshop on Security in Information Systems (WOSIS 2009), Milan, Italy, pp.1-11, 2009.

[8] A.K. Bhaumik, M. Choi, R.J. Robles and M.O. Balitanas,*"Data Hiding in Video",* in International Journal of Database Theory and Application Vol. 2, No. 2, pp. 9-16, June 2009.

[9] J. J. Chae, B. S. Manjunath, "*Data Hiding in Video",* Proceedings of the 6th IEEE International Conference on Image Processing, pp.311-315, 1999.

[10] Melih Pazarci, Vadi Dipcin, *"Data Embedding in Scrambled Digital Video",* in Proceedings of the 8th IEEE International Symposium on Computers and Communication, pp. 498-503, 2003.

[11] A. Giannoula, D. Hatzinakos,*"Compressive Data Hiding for Video Signals",* in Proceedings of International Conference on Image Processing, pp. I529- I532, 2003.

[12] Giuseppe Caccia, Rosa Lancini, "*Data Hiding in MPEG2 Bit Stream Domain",*in Proceedings of International Conference on Trends in Communications, pp.363-364, 2001.

[13] Jun Zhang, Jiegu Li, Ling Zhang, *"Video Watermark Technique in Motion Vector",* in Proceedings of XIV Brazilian Symposium on Computer Graphics and Image Processing, pp.179-182, 2001.

[14] Feng Pan, Li Xiang, Xiao-Yuan Yang and Yao Guo, *"Video steganography using motion vector and linear block codes",* in Proceedings of IEEE International Conference on Software Engineering and Service Sciences (ICSESS- 20100), pp. 592-595, 2010.

