HASH BASED LEAST SIGNIFICANT BIT TECHNIQUE FOR VIDEO STEGANOGRAPHY(HLSB)

Kousik Dasgupta[1], J.K. Mandal[2] and Paramartha Dutta[3]

[1]Department of CSE, Kalyani Govt. Engineering College, Kalyani-741 235, India
kousik.dasgupta@gmail.com
[2]Department of CSE, Kalyani University, Kalyani-741 235, India
jkm.cse@gmail.com
[3]Department of CSS, Visva-Bharati University, Santiniketan-731 235, India
paramartha.dutta@gmail.com

ABSTRACT

Video Steganography deals with hiding secret data or information within a video. In this paper, a hash based least significant bit (LSB) technique has been proposed. A spatial domain technique where the secret information is embedded in the LSB of the cover frames. Eight bits of the secret information is divided into 3,3,2 and embedded into the RGB pixel values of the cover frames respectively. A hash function is used to select the position of insertion in LSB bits. The proposed method is analyzed in terms of both Peak Signal to Noise Ratio (PSNR) compared to the original cover video as well as the Mean Square Error (MSE) measured between the original and steganographic files averaged over all video frames. Image Fidelity (IF) is also measured and the results show minimal degradation of the steganographic video file. The proposed technique is compared with existing LSB based steganography and the results are found to be encouraging. An estimate of the embedding capacity of the technique in the test video file along with an application of the proposed method has also been presented.

KEYWORDS

Steganography, Video Steganography, cover video, cover frame, secret message, LSB

1. INTRODUCTION

Steganography is hiding private or secret data within a carrier in invisible manner. It derives from the Greek word steganos, meaning covered or secret, and graphy (writing or drawing) [1]. 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.

Application of Steganography varies from military, industrial applications to copyright and Intellectual Property Rights (IPR). By using lossless steganography techniques messages can be sent and received securely [2]. 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 [3], [4]. 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.

DOI : 10.5121/ijsptm.2012.2201

Video based steganogrpahic techniques are broadly classified into temporal domain and spatial domain. In frequency domain, images are transformed to frequency components by using FFT, DCT or DWT and then messages are embedded in some or all of the transformed coefficients. Embedding may be bit level or in block level. Moreover in spatial domain the bits of the message can be inserted in intensity pixels of the video in LSB positions. The advantage in the method is that the amount of data (payload) that can be embedded is more in LSB techniques. However most of the LSB techniques are prone to attack as described in [5] and [6]. This makes research fraternity interested in designing new methods. Techniques other than LSB substitution also exist in literature and have been discussed in the next section.

In this paper a hash based LSB Techniques is proposed in spatial domain. An application of the algorithm is illustrated with AVI (Audio Video Interleave) file as a cover medium. The results obtained are significant and encouraging. Effort has also been taken to study the steganalysis of the proposed scheme.

The rest of the paper is arranged as follows, section 2 does Literature survey of the recent steganographic techniques. In section 3 the proposed video steganographic technique has been described. The algorithm is proposed in section 4 with an application of it in AVI carrier file and illustration. Section 5 gives results and performance evaluation with other LSB technique with steganalysis of the technique. Conclusion and future work are presented in Section 6.

2. 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 [7] a robust image steganography technique based on LSB insertion and RSA encryption technique has been used. Masud et.al [8] 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. Other Examples of LSB schemes can be found in [9], [10]. Whereas EzStego developed by Machado [11] embed information into an image in the GIF format. It sorts the palette to ensure the difference between two adjacent colors is visually indistinguishable. Tseng and Pan [12] presented a data hiding scheme in 2-color images, it embeds the information in any bit where at least one of the adjacent bits is the same as the original unchanged bit. Kawaguchi et. al. [13] proposes bit plane complexity segmentation (BPCS) method to embed information into the noisy areas of the image. These techniques are not limited to the LSB. Existing steganographic software, such as Steganos, S-tools and Hide4PGP [14], are based on LSB.

Video steganography of late has also gained quite significance for researchers. Various techniques of LSB exists, where [15] 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 [16] selected LSB steganography algorithm is proposed. Other steganography techniques in uncompressed raw video, is illustrated [17], [18] and [19]. Steganography techniques for compressed video stream can be found in [20], [21] and [22]. Another video steganography scheme based on motion vectors and linear block codes has been proposed in [23].

3. PROPOSED TECHNIQUE

The technique is a Hash based Least Significant Bit (HLSB) technique for Video Steganography has been proposed. The flow diagram of the same is given in Figure 1.

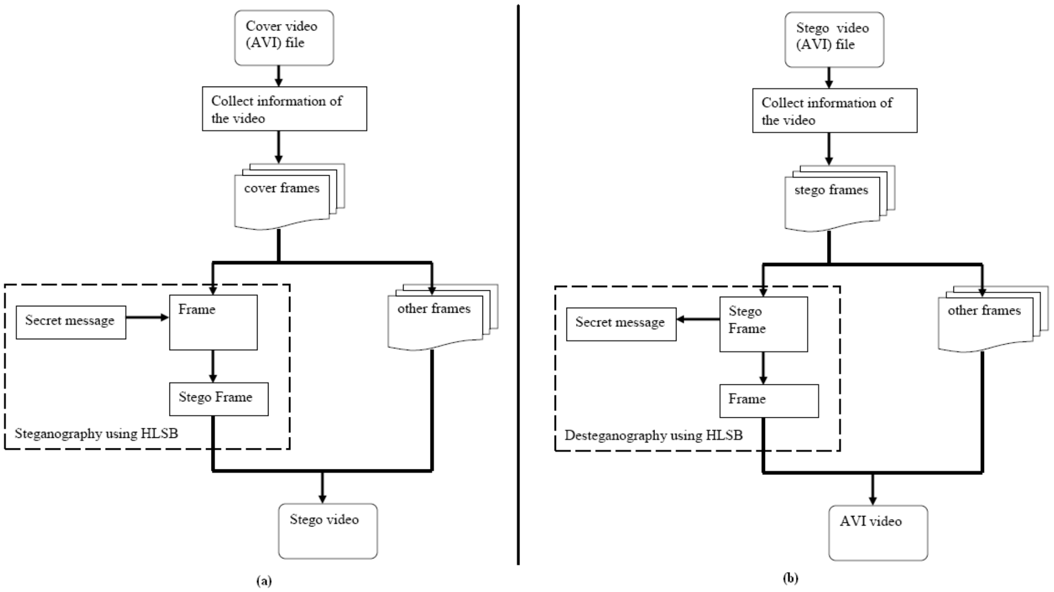


Figure 1: Block diagram of HLSB Video Steganography technique (a) Encoding and (b) Decoding

A video stream (AVI) consists of collection of frames and the secret data is embedded in these frames as payload. The information of the cover video (AVI) such as number of frames (n), frame speed (fp/sec), frame height (H) and width (W) are extracted from the header. The cover video is then broken down into frames. Now the proposed LSB based technique has been applied to conceal the data in the carrier frames. The size of the message does not matter in video steganography as the message can be embedded in multiple frames.

The proposed technique takes eight bits of secret data at a time and conceal them in LSB of RGB (Red, Green and Blue) pixel value of the carrier frames in 3, 3, 2 order respectively. Such that out of eight (08) bits of message six (06) bits are inserted in R and G pixel and remaining two (02) bits are inserted in B pixel. The detailed technique has been depicted in Figure 2. An illustration of the same is given in section 4.3. This distribution pattern is taken because the chromatic influence of blue to the human eye is more that red and green pixel. Thus the quality of the video is not sacrificed but we could increase the payload. Also this small variation in colours in the video image would be very difficult for the human eye to detect.

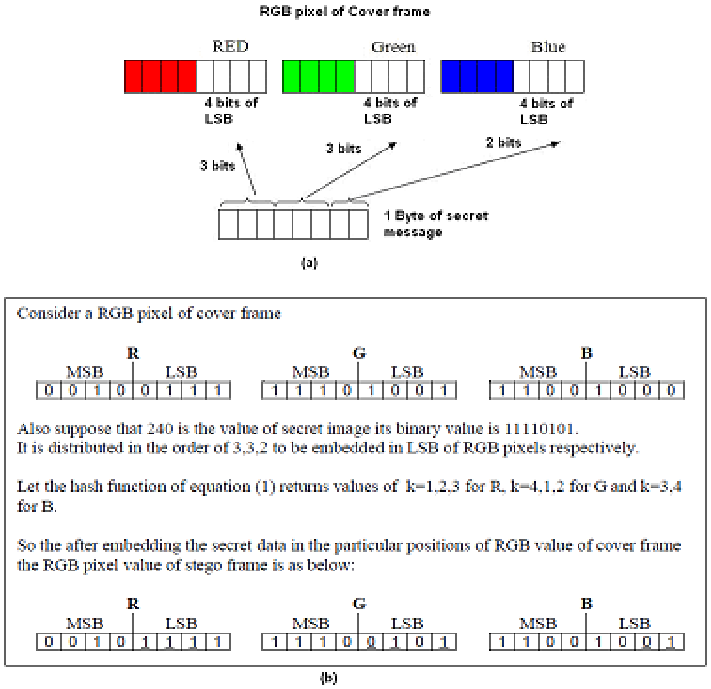
The embedding positions of the eight bits out of the four (4) available bits of LSB is obtained using a hash function of the form,

$$k = p\%n \tag{1}$$

where, k is LSB bit position within the pixel, p represents the position of each hidden image pixel and n is number of bits of LSB which is 4 for the present case.

The bits are distributed randomly during fabrication which increases the robustness of the technique compared to other LSB based techniques [15, 16]. After concealing data in multiple frames of the carrier video, frames are then grouped together to form a stego video, which is now an embedded video to be, used as normal sequence of streaming.

The intended user follows the reverse steps to decode the secret data. During decoding the setgo video is again broken into frames after reading the header information. Using the same hash function which is known to the intended user, the data of the secret message is regenerated. The extracted stream of the secret information is used to authenticate the video. The algorithm of the proposed technique has been outlined in section 4.



Consider a RGB pixel of cover frame

R: MSB				R: LSB				G: MSB				G: LSB				B: MSB				B: LSB			
0	0	1	0	0	1	1	1	1	1	1	0	1	0	0	1	1	1	0	0	1	0	0	0

Also suppose that 240 is the value of secret image its binary value is 11110101.
It is distributed in the order of 3,3,2 to be embedded in LSB of RGB pixels respectively.

Let the hash function of equation (1) returns values of k=1,2,3 for R, k=4,1,2 for G and k=3,4 for B.

So the after embedding the secret data in the particular positions of RGB value of cover frame the RGB pixel value of stego frame is as below:

R: MSB				R: LSB				G: MSB				G: LSB				B: MSB				B: LSB			
0	0	1	0	1	1	1	1	1	1	1	0	0	1	0	1	1	1	0	0	1	0	0	1

Figure 2: Proposed hash based LSB embedding technique (a) shows secret data embedded in 4 bits of LSB in 3,3,2 order in corresponding RGB pixels of carrier frame and (b) example of embedding of bits using hash function

4. ALGORITHM OF HLSB WITH AN APPLICATION

The proposed algorithm, both for encoding and decoding along with application are given in this section. Encoding technique is given in section 4.1 whereas decoding technique is given in section 4.2. The proposed technique is illustrated with an example in section 4.3 and an application of the proposed technique is given in section 4.4.

4.1. Algorithm of Encoding

Step 1: Input cover video file or stream.
Step 2: Read required information of the cover video.
Step 3: Break the video into frames.
Step 4: Find 4 LSB bits of each RGB pixels of the cover frame.
Step 5: Obtain the position for embedding the secret data using hash function given in equation 1.

Step 6: Embed the eight bits of the secret image into 4 bits of LSB of RGB pixels of the cover frame in the order of 3, 3, 2 respectively using the position obtained from step 5.
Step 7: Regenerate video frames.

4.2. Algorithm of Decoding

Step 1: Input stego video file or stream.
Step 2: Read required information from the stego video.
Step 3: Break the video into frames.
Step 4: Find 4 LSB bits of each RGB pixels of the stego frame.
Step 5: Obtain the position of embedded bits of the secret data using hash function given in equation 1.
Step 6: Retrieve the bits using these positions in the order of 3, 3, 2 respectively.
Step 7: Reconstruct the secret information.
Step 8: Regenerate video frames.

4.3. Illustration of HLSB technique

Consider a RGB pixel value of the cover frame as below

R: 10110111
G: 10010100
B: 11001001

and a byte of message to be inserted in LSB as:

10001001

LSB is lowest bit in a series of binary numbers, so in this case for R it will be 1, 0 for G and 1 for B. The proposed technique is applied in four lowest LSBs in each pixel value. So the LSBs for the above RGB values are:

R : 0111
G : 0100
B : 1001

The message is embedded in groups of 3, 3 and 2 in the respective RGB LSBs positions. The positions are obtained from the hash function given in equation (1). The value of n number of bits of LSB for the present scenario is 4. Using the hash function let the position of insertion k returned for a particular iteration are,

k = 1,2,3 for R.

k = 4,1,2 for G

k = 3,4 for B

Considering the above positions of insertion, the bits from the message are inserted in four LSB positions and resulting RGB pixel value are as given below.

R: 1011**100**1
G: 1001**10**0**0**
B: 110010**01**

Thus all the eight bits of the message are embedded in three bytes and number of bits actually changed is five (05) out of twenty four (24) bits. Further these five (05) bits are randomly distributed among which increases the robustness of the scheme.

To decode the message, the valid user follows the reverse step. As the hash function (1) is known to the intended the user, it calculates the k values to get the position of insertion. Taking the same embedded RGB value as above,

R: 10111001
G: 10011000
B: 11001001

The hash function will return the following k values for this particular iteration.

k = 1,2,3 for R.
k = 4,1,2 for G
k = 3,4 for B

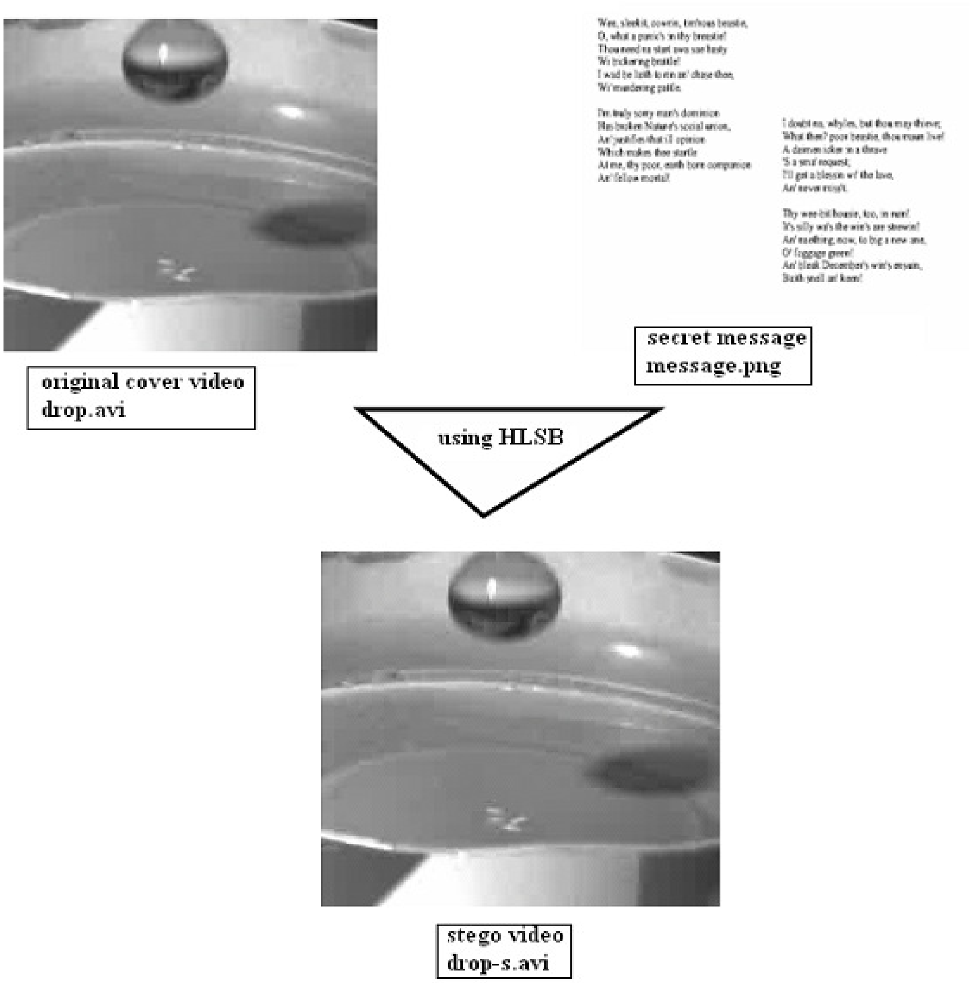
using these k values which represent the four LSB positions, the data of the secret message is found as below,

10001001

Which is same as the data of secret message as considered above.

4.4. Application of HLSB technique

A simulation environment has been created using Visual C++ 2010 as IDE and Opencv 1.0 as the graphics library. An application of the proposed algorithm with a test video (drop.avi) has been shown in figure 3. It shows a carrier video (drop.avi) and a secret image (message.png) and after steganography the output stego file is as given in drop-s.avi. On decoding the secret message (message.png) is obtained back without any loss or noise. The quality of the secret data can be analyzed by using the Peak Signal to Noise Ratio (PSNR) value of original secret image and image. The value of Mean Square Error (MSE) comes infinity (∞), meaning that the two images are identical.



Wee, sleekit, cowrin, tim'rous beastie,
O, what a panic's in thy breastie!
Thou need na start awa sae hasty
Wi bickering brattle!
I wad be laith to rin an' chase thee,
Wi' murdering pattle.

I'm truly sorry man's dominion
Has broken Nature's social union,
An' justifies that ill opinion
Which makes thee startle
At me, thy poor, earth born companion
An' fellow mortal!

I doubt na, whyles, but thou may thieve;
What then? poor beastie, thou maun live!
A daimen icker in a thrave
'S a sma' request;
I'll get a blessin wi' the lave,
An' never miss't.

Thy wee-bit housie, too, in ruin!
It's silly wa's the win's are strewin!
An' naething, now, to big a new ane,
O' foggage green!
An' bleak December's win's ensuin,
Baith snell an' keen!

Figure 3. Application of the proposed HLSB technique

5. RESULTS AND PERFORMANCE EVALUATION

Any Steganography technique is characterized mainly by two attributes, imperceptibility and capacity. Imperceptibility means the embedded data must be imperceptible to the observer (perceptual invisibility) and computer analysis (statistical invisibility). The performance of the proposed technique is evaluated using three different video streams (drop.avi, flame.avi and american football.avi) and one secret data (message.png).

The perceptual imperceptibility of the embedded data is indicated by comparing the original image or video to its stego counterpart so that their visual differences, if any, can be determined. Additionally, as an objective measure, the Mean squared Error (MSE), Peak Signal to Noise Ratio (PSNR) and Image Fidelity (IF) between the stego frame and its corresponding cover frame are studied. The quantities are given as below,

$$MSE = \frac{1}{H * W} \sum_{i=1}^{H} (P(i, j) - S(i, j))^2 \qquad (2)$$

where, MSE is Mean Square error, H and W are height width and P(i,j) represents original frame and S(i,j) represents corresponding stego frame.

$$PSNR = 10 \log_{10} \frac{L^2}{MSE} \qquad (3)$$

where, PSNR is peak signal to noise ratio, L is peak signal level for a grey scale image it is taken as 255.

Maximum payload (bits per byte/bpb) for the technique has also been obtained i.e. maximum amount of data that can be embedded into the cover image without losing the fidelity of the original image. In the proposed scheme eight bits of data are embedded in 3 pixels of the cover frame.

The cover file video details are given in Table 1 and results are tabulated in Table 2.

Table 1. Cover Video File details.

S.No	**Cover video file information**				**Secret message Resolution W_1 *H_1**
	Name of video file	**Resolution (W*H)**	**Frame /sec.**	**No. of frames**	
01	drop.avi	256 * 240	30	182	640 * 480
02	american football.avi	176 * 184	30	455	
03	flame.avi	256 * 240	30	294	

Table 2. Results obtained from HLSB and LSB techniques

Name of the video file	**Results obtained using HLSB**				**Results obtained using LSB[15]**			
	PSNR	**Avg. MSE**	**IF**	**Payload (bpB)**	**PSNR**	**Avg. MSE**	**IF**	**Payload (bpB)**
drop.avi	44.34	0.34	0.23	2.66	48.56	0.42	0.32	1
american football.avi	45.67	0.34	0.25	2.66	52.34	0.52	0.34	1
flame.avi	42.66	0.34	0.35	2.66	48.56	0.38	0.38	1

5.1 Steganalysis of video

Several image Steganalysis technique exist in literature [24], [25], [26]. However these techniques does not work very well with video and yield very low performance. In recent times researchers have developed some video steganalysis techniques. In [27] a technique for video steganalysis by using the redundant information present in the temporal domain as a deterrent against secret messages embedded by spread spectrum steganography has been proposed. Kancherla et. al. [28] has proposed a video steganalysis method using neural networks and support vector machines to detect hidden information by exploring the spatial and temporal redundancies. Literature survey suggests that when temporal redundancies are used as video steganalysis then performance is more satisfactory than in spatial domain. Where as in [30] a steganalysis algorithm has been proposed that uses the correlation between adjacent frames to detect a special distribution mode across the frames. This is considered to work well with AVI file formats. However every carrier media is supposed to have its own special characteristics and thus it behaves differently when a message is embedded in it. To summarise, existing video steganalysis technique may not work very well to detect the presence of secret message using the proposed HLSB technique. However one can make a detailed analysis of the same.

6. CONCLUSION

A secured hash based LSB technique for video steganography has been presented in this paper. This technique utilizes cover video files in spatial domain to conceal the presence of sensitive data regardless of its format. Performance analysis of the proposed technique after comparison with LSB technique is quite encouraging. The proposed technique is applied to AVI files, however it can work with any other formats with minor procedural modification. For compressed video files like MPEG the video needs to first decompress then the technique can be applied to the uncompressed video. Where as for Flash Video FLV files the technique can be applied without modification. A software based Steganographic Engine for video steganography is the future scope of the technique.

REFERENCES

[1] E. Cole and R.D. Krutz, Hiding in Plain Sight: Steganography and the Art of Covert Communication, Wiley Publishing, Inc., ISBN 0-471-44449-9, 2003.

[2] Stefan Katzenbeisser and Fabien A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House Books, ISBN 1-58053-035-4, 1999.

[3] D. Stanescu, M. Stratulat, B. Ciubotaru, D Chiciudean, R. Cioarga and M. Micea, Embedding Data in Video Stream using Steganography, in 4th International Symposium on Applied Computational Intelligence and Informatics, SACI-2001, pp. 241-244, IEEE, 2007.

[4] Feng Pan, Li Xiang, Xiao-Yuan Yang and Yao Guo, Video Steganography using Motion Vector and Linear Block Codes, in IEEE 978-1-4244-6055-7/10/, pp. 592-595,2010.

[5] A. Westfield, and A. Pfitzmann, Attacks on Steganographic Systems, in Proceedings of 3rd Info. Hiding Workshop, Dresden, Germany, Sept. 28–Oct. 1, pp. 61-75, 1999.

[6] J. Fridrich, R. Du, and L, Meng, Steganalysis of LSB Encoding in Color Images, in Proceedings of ICME 2000, Jul.-Aug. 2000, N.Y., USA.

[7] 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

[8] 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.

[9] Hema Ajetrao, Dr. P.J.Kulkarni and Navanath Gaikwad, A Novel Scheme of Data Hiding in Binary Images, in International Conference on Computational Intelligence and Multimedia Applications, Vol.4, pp. 70-77, Dec. 2007.

[10] Sachdeva S. and Kumar A, Colour Image Steganography Based on Modified Quantization Table, in Proceedings of Second International Conference on Advanced Computing & Communication Technologies (ACCT-2012), pp. 309-313, 2012.

[11] R. Machado, http://www.securityfocus.com/tools/586/scoreit, .EzStego., Nov. 1996. [last accessed on 16-04-2012]

[12] Y. C Tseng and H. K Pan, Data Hiding in 2-color Image in IEEE Transactions on computers, Vol. 51, No. 7, pp. 873-878, July 2002.

[13] E. Kawaguchi and R. O. Eason, Principle and applications of BPCS-Steganography, in Proceedings of SPIE Int'l Symp. on Voice, Video, and Data Communications, pp. 464-473, 1998.

[14] Steganographic software, http://www.jjtc.com/Steganography/toolmatrix.html [last acessed on 16-04-2012]

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

[16] 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.

[17] 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.

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

[19] 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.

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

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

[22] 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.

[23] 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.

[24] N. F. Johnson and S. Jajodia, Steganalysis of Images Created using Current Steganography Software, in Lecture Notes in Computer Science, vol. 1525, pp. 32 – 47, Springer Verlag, 1998.

[25] S. Dumitrescu, X. Wu and N. Memon, On Steganalysis of Random LSB Embedding in Continuous tone Images, in Proceedings of the International Conference on Image Processing, vol. 3, pp. 641 – 644, June 2002.

[26] J. Fridrich, M. Goljan, D. Hogea and D. Soukal, Quantitative Steganalysis of Digital Images: Estimating the Secret Message Length,” in ACM Multimedia Systems Journal, Special issue on Multimedia Security, vol. 9, no. 3, pp. 288 – 302, 2003.

[27] U. Budia, D. Kundur and T. Zourntos, Digital Video Steganalysis Exploiting Statistical Visibility in the Temporal Domain, in IEEE Transactions on Information Forensics and Security, vol. 1, no. 4, pp. 502 – 516, December 2006.

[28] K. Kancherla and S. Mukkamala, Video Steganalysis using Spatial and Temporal Redundancies, in Proceedings of International Conference on High Performance Computing and Simulation, pp. 200–207, June 2009.

[29] Y. Su, C. Zhang, L. Wang and C. Zhang, A New Video Steganalysis based on Mode Detection, Proceedings of the International Conference on Audio, Language and Image Processing, pp. 1507–1510, Shanghai, China, July 2008.

Authors

Kousik Dasgupta did his Bachelors in Engineering in Electronics and Power Engineering from Nagpur University, Nagpur, India in 1993. Subsequently, he did his Masters in Computer Science & Engineering in 2007 from West Bengal University of Technology, Kolkata, India. He is currently Assistant Professor in the Department of Computer Science and Engineering of Kalyani Government Engineering College, Kalyani, India. He served industries like ABB and L & T during 1993-1996. He is c o-author of two books and about 10 research publications. His research interests include soft computing, computer vision and image processing and steganography. Mr,. Dasgupta is a Life Member of ISTE, India, Associate Member of The Institute of Engineers, India and Chartered Engineer [India] of The Institute of Engineers, India. He is a Fellow of OSI. India

Jyotsna Kumar Mandal, M. Tech.(Computer Science, University of Calcutta), Ph.D.(Engg., Jadavpur University) in the field of Data Compression and Error Correction Techniques, Professor in Computer Science and Engineering, University of Kalyani, India. Life Member of Computer Societ y of India since 1992 and life member of Cryptology Research Society of India. Dean Faculty of Engineering, Teachnology & Management, working in the field of Network Security, Steganography, Remote Sensing & GIS Application, Image Processing. 25 years of teaching and research experiences. Eight Scholars awarded Ph.D., one submitted and 8 are pursuing. Total number of publications is more than two hundred.

Paramartha Dutta did his Bachelors and Masters in Statistics from Indian Statistical Institute, Kolkata, India in 1988 and 1990, respectively. Subsequently, he did his Masters in Computer Science in 1993 from Indian Statistical Institute, Kolkata, India. He did his Ph.D. in 2005 from Bengal Engineering and Science University, Shibpore, India. He is currently a Professor in the Department of Computer Science and Engineering of Kalyani Government Engineering College, Kalyani, India. He was an Assistant Professor and Head of the Department of Computer Science and Engineering of College of Engineering and Management, Kolaghat, India during 1998–2001. He has served as a Research Scholar in the Indian Statistical Institute, Kolkata, India and in Bengal Engineering and Science University, Shibpore, India. He is a co-author of four books and about 120 research publications. His research interests include evolutionary computing, soft computing, pattern recognition and Network security.