INNOVATIVE DATA HIDING SECURITY MODEL USING FORENSIC AUDIO VIDEO CRYPTO-STEGANOGRAPHY

Sunil K. Moon¹ and Rajeshree D. Raut²

¹Department of Electronics and Telecommunication Engineering, Pune Institute of Computer Technology, India ²Department of Electronics and Communication Engineering, Shri Ramdeobaba College of Engineering and Management, India

Abstract

Secret information concealing using steganography is simple but to maintain its security, perceptibility, robustness, embedding capacity and good recovery of both cover as well as secret information are the major issues. In this paper we have applied Block Plane Coding Technique (BPCT) for concealing the secret data into the randomly obtained frames of video and Least Significant Bit (LSB) algorithm for audio of same video. We have obtained the key security parameters like Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Normalize Cross Correlation Factor (NCCF), Bit Error Rate (BER), histogram and spectrograph before embedding and after recovering the protected data from stego video using forensic technique to increase the data security. Moreover, the proposed scheme provides a large hiding capacity, more security for secret data and good visual recovery of both secret data and original video than any other existing methods. Through many attack during transmission on stego video, it is found that the suggested approach is more robust than any other existing methods.

Keywords:

Audio Video Steganography, BPCT, Information Hiding, 4LSB, Visual Attack, Histogram

1. INTRODUCTION

As every communication use the digital media through Facebook, YouTube, Twitter and WhatsApp which contain videos, so it is better to apply security of such digitally transmitted videos. Steganography is used for good as well as bad purpose depending on its application. Subhedar et al. in 2015 gave a survey of existing image steganography and its key issues. It also elaborates the fundamental concepts, evolution measures and data security of current steganography techniques in different domain which provides the present research trends and direction to improve data security of existing methods [1]. Since last ten years there is tremendous growth in the field of data hiding using steganography for security purpose and different approaches have produced for steganography to `increase the hiding capacity, security, robustness, and perceptibility. Sadek et al. gave the literature survey of existing video steganography techniques in different domain and suggested the advantages and disadvantages since last five years. Hence to produce ideal and perfect video steganography approach, it should provide large embedding capacity, high imperceptibility, robustness and tamper resistance but unfortunately no such algorithm does exist in reality. All the reviewed methods have its own advantage and disadvantage in term of hiding capacity and security depending on its application. Hence it is always better to design appropriate video steganography algorithm for given application [2]. So we have motivated to increase the security, perceptibility, robustness using video steganography. The term steganography is used to hide any secret data behind a cover file. The main use of any type of steganography is for authenticity and security of secret data. To produce high level data security using data hiding technique, embedding capacity, data security, good visual recovery of hidden data, robustness are the major problem. As per today's requirement and concept of cryptography, steganography and forensic detection, we have proposed a new data embedding security model to enhance information security and embedding capacity for stego video to produce triple security of hidden secret data [3]. The main used of any type steganography is to increase the secret data security and embedding capacity Guizani et al. focused on comparison of BPCS and 4LSB [4] methods for high capacity steganography technique and obtained 63% hiding capacity and PSNR = 26.79 dB for lower order statistical attack. Bansod et al. have suggested hybrid crypto-steganography using BPCS algorithm [5] for hiding more secret data having PSNR value for R = 43.2, G = 34.8, B = 43.9dB. Bhattacharyya et al. have proposed the method based on PMM (Pixel Mapping Method) using BPCS algorithm to improve the robustness of secret data [6]. It is applicable to only gray scale image having PSNR = 36.87 dB. Shi et al. suggested that BPCS technique can be used for information hiding where embedding capacity [7] is increased around 50% and it also gives an idea on improved steganography text based on chaos and BPCS algorithm for higher security and reliability with PSNR is 38.03dB. It is most secured technique and provides high security. English et al. [8] suggested the comparison of high capacity steganography techniques using 4LSB and BPCS algorithm for hiding secret data and found to be BPCS algorithm are more efficient in terms of hiding capacity is 63%, PSNR is 26.79dB as compare to 4LSB technique hiding capacity is 50%, PSNR = 39.84dB. Moon et al. in 2013 have introduced [9] the video cryptography using forensic detection technique using 4LSB insertion method in selected frames of video and obtained the hiding capacity up to 50% and it is more secured. Kelash et al. [2013] have applied video steganography on color (.avi, .flv) as well as gray video as original video and color image and gray image as secret image and found better security [10]. There are many approaches present for finding the PSNR of a color image. Eye is more sensitive to luma information, hence we have calculate the PSNR for color images by converting the color image to a color space that separates the intensity (luma) channel, such as Y Cb Cr. The Y (luma), in YC_bC_r represents a weighted average of red, green, and blue. As green color is the most weighted color and because of the human eye can perceives it most easily as compare to red and blue color [11]. In the paper [12] [13] the respective author applied 1LSB, 2LSB, 3LSB, 4LSB. SLSB, OLSB, OPAP algorithm to hide secret information having less hiding capacity and PSNR. Bagade et al. in 2014 proposed the high quality steganography method using morphing and give better hiding capacity, stego image quality and imperceptibility having PSNR is 51.99dB and hiding capacity is 262144 bytes [14].

This paper is organized as follows: In the next section 2, the suggested security model and theoretical background of video crypto steganography using computer forensic technique is discussed. The simulation results and discussion is noted in section 3. PSNR, MSE, BER and NCCF as authentic security parameters are explain in section 4. Security through Robustness and perceptibility are justified in section 5. In the last section 6 the conclusion and references are indicated respectively.

2. THE MAJOR OBJECTIVE AND CONTRIBUTION

In the proposed algorithm we have embedded two secret images into randomly selected frames of video and audio. We have divided two secret images into eight equal parts and each part is embedded into randomly selected frames of video and audio using Block Plane Coding Technique (BPCT) and Least Significant Bit (LSB) algorithms hence hiding capacity and security has been increased. We have calculated PSNR, MSE, BER, NCCF, histogram and spectrograph of secret data before embedding and after recovering from stego video using forensic detection technique and applied different types of attacks. As we have applied video steganography, cryptography and forensic technique hence hidden data become triple secured.

3. PROPOSED SECRET DATA SECURITY MODEL

The original video is converted into the number of frames and selects any random frames to embed the secret data as text and image. As we have applied randomly selected frames of video to conceal secret data hence obtained the complexity of randomly selected frames of video. Before embedding the secret data (Data Encryption Standard) DES algorithm is used to encrypt or scramble the secret data so that large amount of secret data can be embed. Receiver end is used to cross check the secret information by forensic detection technique which adds an extra layer of data security. This stego video is then sent from transmitter to receiver. At receiver end it is very difficult to understand in which part of video the secret data is hidden. The key security parameters like PSNR, MSE, NCCF, BER, and histogram of original secret data is calculated before hiding and after recovering secret data from stego video. In the encoding process to get the audio-video file back, such that the viewers of video should not come to know whether data is hidden behind the audio or video file. Computer forensic block is used for cross checking whether incoming data is correct or not. It will check the height, width, size of secret data, video, PSNR, BER, MSE and histogram of incoming stego video. If incoming data is correct, then stego video is sent to receiver end otherwise it stops in forensic block. The Fig.1 shows the proposed block diagram of our system. The proposed algorithm is not video format dependent and the results are tested on .avi, .mp4, .wmv and it gives the better results than any other existing methods. We have sent the values of PSNR, MSE, BER, NCCF, histogram of secret data along with secret key, so before recovering secret data from video we want to produce the correct key as password. If the key is wrong, then it cannot recover the secret information. If we applied the correct secret key and values of PSNR, MSE, BER,

NCCF, then the hidden information can be recovered in the forensic block. If the values of PSNR, BER, MSE, NCCF and secret key before embedding and after recovering from stego video are exactly match, then it is transfer to receiver, if it is not match then it will stop in forensic block.

3.1 DATA HIDING IN AUDIO

- Obtain the original .wav, .mp3 audio file at transmitter end.
- Observe the .wav or mp3 audio file using wavread function and store its sample's amplitude value in variable y and frequency in fs. Open original audio file in read mode using function open



Fig.1. Proposed block diagram of data security model

- Read .wav or mp3 audio file's first 40 bytes of header using fread function and store it in a variable header.
- Then read all its data after 40th byte using same function and store it in data variable.
- Stop the file using fclose function.
- Calculate the length of text or size of image and store it in a variable msg. Convert the message into binary form.
- Change the binary message into column vector as the secret data is hidden in LSB of audio file. Calculate length of binary message.
- Accept secret key from user. Convert it into binary and calculate its size and length. Convert it into binary form.
- If the secret key is wrong and if it is greater than 9 letters, then error generated Hide the size of identity key in further 20 bytes and identity key in further bytes of .wav or mp3 file.
- Open a new .wav or mp3 file to overwrite the hidden data on it. Copy header as it is in new open file and then modified data on further audio data file. This creates stego audio file.

3.2 DATA HIDING IN VIDEO

- Select the .avi, .flv, .mp4, .wmv video file as a cover video.
- Read the video file using video reader function and store it in to variable.
- Convert the frames into R, G and B planes as block.
- Split each R, G, B planes into 8 planes as block
- Find the complexity of each RGB block to find number of transitions from 0 to 1 and 1 to 0 and divide it by maximum value.
- · Read the secret data and convert it into binary form.
- Replace the bits of block having complexity greater than 0.2 (threshold value) by the secret data bits.

• Obtained the stego video by replacing original frames with stego frames.

3.3 RECOVERY OF DATA FROM VIDEO

- · Obtain the stego video and convert into frames.
- Extract the message lengths from audio decoder.
- Recover the stego frames from video in which message is hidden.
- Slice the frame into 24 bit plane as a block.
- Extract the bits up to length from the plane.
- Convert those binary bits into decimal form using bin2decfunction.
- Obtained decimal format into unicode and display the secret message

3.4 AUDIO RECOVERY FORM STEGO VIDEO

- Open stego audio file as wav or mp3 in read mode using function fopen. Audio file is read using function wavread,
- Sample data is stored in y.
- Read the wav or mp3 file's first 40 bytes of header using fread function and store it in a variable header.
- Then read all its data after 40th byte using same function and store it in data1 variable.
- Close file using fclose function.
- Accept secret key from user and compare entered secret key with recover secret key.
- Recover and the size of identity key from LSB of .wav file or .mp3
- Recover secret key from further bits of .wav, .mp3 audio file.

If both the keys are matched then only the user can recover the hidden secret data else the processes will be aborted. As the secret key is matched, recover the size of text or image from further bits of .way, .mp3 audio file. This algorithm gives good results for color and natural videos. Image is split into bits planes. For 24 bit color image = RGB = 8bit R + 8bit G + 8bit B (R =MSB, B = LSB). Find out the complexity of bits such that LSB Bit for group of two planes 0-1, 1-0 (used to embed the secret data). If 0-0 and 1-1(not used to embed the secret data). We have obtained the pixel pair groups for B block plane (0-1, 2-3, 4-5, 6-7), for G block plane (8-9, 10-11, 12-13, 14-15) and for R block plane fluctuation in the input image data type. The block plane 16-17, 18-19, 20-21, 22-23 and so on as indicated in Table.1. In the cover video there are plenty number of frames available to embed the secret data hence every block plane is concealed into randomly obtained frames block plane of cover video using Block Plane Coding.

R (MS	SB)	G		B (LSB)		
23 (MSB)	1110 0010	15	0110 1101	7	0011 1110	
22	0011 1101	14	0011 1100	6	00001100	
21	1111 0000	13	0101 1001	5	1100 0011	
20	0101 1110	12	0011 1010	4	1100 1001	
19	0111 0001	11	1110 0101	3	1001 1000	
18	0011 1000	10	0101 1100	2	0011 1111	
17	1001 0110	9	0011 0010	1	11010101	
16	1110 0111	8	1000 1110	0 (LSB)	1001 0010	

4. SIMULATION RESULTS AND DISCUSSION

Through number of standard data sets of images and video formats we have performed the different attacks on stego video using BPCT and LSB algorithms. The Fig.2(a) and Fig.2(b) indicates the selected frames of original and stego video which are complementary to each other. The Fig.3(a) - Fig.(c) shows the selected frame of original video and stego video and its individual RGB histograms which are similar to each other while Fig.4(c) and Fig.5(a) are the recover two secret images from stego video without any loss of information which improves the novelty of proposed system. The Table.2 shows the obtain results for BPCT algorithm on .avi, .flv and .mp4 video format with PSNR is 49.84 dB, hiding length = 163200 and NCCF = 0.99. The Table.3 indicates the comparison between [5] [7] [8] existing techniques and our BPCT algorithm on video. It is observed that the proposed method is better in terms of EC, PSNR, BER and NCCF, hence provides the more security. The Table.4 is the results obtain for audio 1 and audio 2. The Table.5 is the comparison of [08] BPCS or 4LSB and our BPCT approach. It is found that the suggested technique is better than English [8]. The Table.6 gives the comparison of [12]-[14] and our approach has better results in terms of PSNR, EC, BER and NCCF. The Table.7 shows the results obtain using 8-4-2-1 LSB coding for audio video steganography with different attacks. It is observed from Table.7 the values of PSNR, MSE, NCCF are very good, hence we recovered secret data without any loss of information. The Table.8 indicates the results obtain for BPCT algorithm through different attacks. We have tested our results on .avi, .flv, .mp4 videos of 512×512 and secret image of 512×512, 256×256 and .wav audio format. Before and after attack, the values of PSNR, MSE and NCCF does not change, hence the proposed system is more robust than any other existing approach.

Table.1. RGB block planes of secret data

5. PSNR MSE, BER AND NCF AS AUTHENTICATE PARAMETERS

5.1 PEAK SIGNAL TO SIGNAL RATIO (PSNR)

Peak Signal to Signal Ratio (PSNR) is use to find the similarity between original and stego video. To compute the PSNR, first calculates the Mean-Squared Error (MSE) using the following Eq.(1), Eq.(2) and Eq.(3). MSE and PSNR are the two important security parameters of any type of steganography [6][11].

$$MSE = \frac{1}{MN} \sum_{x=1} \sum_{y=1} \left(M_{xy} - N_{xy} \right)^2$$
(1)

where, x, y are the pixel values, M, N are the dimension of the images, M_{xy} is the stego image and N_{xy} is the original images.

$$MSE = \frac{MSE}{3} [R + G + B] \text{ for color image}$$
(2)

$$PSNR = 10\log_{10}\left[\frac{X_{\text{max}}^{2}}{MSE}\right]$$
(3)

where, X_{max} the maximum value of original images, MSE is the mean square error [6][11]. In the Eq.(3), X is the maximum

5.2 BIT ERROR RATE (BER)

BER is the ratio of number of error bits to the total number of bits. Secret information extracted from the stego video should contained minimum BER. It also express how many bits of stego frames are affected after hiding and transmitting stego video from transmitter to receiver[6][11]. The bit error rate of an algorithm is calculated using Eq.(4).

BER = (Number of error in bis)/(Total number of bits) (4)

5.3 NORMALIZE CROSS CORRELATION FACTOR (NCCF)

Normalize Cross Correlation Factor (NCCF) is used to obtain how much close extent to each other the cover and stego video are, even after embedding data the secret data [15][16]. The typical value of NCCF is 1. Proposed algorithm has very high NCCF (for text it is almost 1 and for image/audio it is 0.99 as shown in Eq.(5).

$$NCCF = \Sigma \left(\frac{\left(\Sigma \left(X * X_T \right) \right)}{\left(\Sigma \left(X * X_T \right) \right)} \right)$$
(5)

where, * is element to element multiplication, X is original pixel matrix of selected frame of video and X_T is stego pixel matrix of selected frame of video.

5.4 HISTOGRAM AND SPECTROGRAPH

In the suggested algorithm we have check the histogram of secret image before concealing and after recovering from stego video and audio which are similar to each other. The histogram of color secret image before embedding and recovering from stego video is indicates in Fig.4(a) and Fig.4(b) shows the spectrograph of original and stego audio, hence the proposed technique is more secured and perceptible.

6. SECURITY THROUGH ROBUSTNESS AND IMPERCEPTIBILITY

6.1 VISUAL ATTACK

In this attack we have replace LSB of every selected frames of stego video and original video [17]. By replacing LSB bits of original and stego frames of video, there is no loss of information. Hence security level increased as shown in Fig.5(b) and Fig.5(c).

6.2 POISSON NOISE

In the Poisson noise we have created some malfunctioning to every frames of stego video before transmission. This shows that the proposed technique can also tolerate Poisson noise very effectively as indicates in Fig.6(a) [15][16].

6.3 SPECKLE NOISE

Speckle noise is very common type of noise which is caused by some errors during data transmission [15][16]. Here we have change some stego pixel 0 by 1 and 1 by 0 as indicated in Fig.6(b).

6.4 SALT AND PEPPER NOISE

We have applied salt and pepper noise effect on selected pixels values in the selected frames of stego video which are very different in intensity from its neighboring pixels. The different in intensity pixel value of noisy stego video pixel has no significance to the intensity of its surrounding pixels [15][16]. If some noise is added to stego frame then it can be remove by median filter as shown in Fig.7(a), Fig.7(b) and Fig.7(c)

6.5 ROTATIONAL ATTACK

In rotational attack we have rotated the secret image by 50, 100, 150, 200, 250 and 300 degree and embedded into selected frames of video and recovered back without any loss of information with same values of key security parameters[15][16]. The rotation of 90 degree of secret data is given by Fig.6(c).



Fig.2. (a) Selected frame and (b) stego frame of video





Fig.3. Original and stego RGB frames of video



Fig.4. (a). Original and stego RGB histogram (b). Original and stego spectrogram of audio 1 (c). Recovery of gray Lena secret image



Fig.5. (a). Recovery of color secret image (b). Visual attack before embedding secret data (c). Visual attack after recoverying secret data



(u)

)

Fig.6. (a). Effect of poisson noise (b). Speckle noise (c). rotational attack





Fig.7. (a). Effect of paper and salt noise (b). median filter and (c). recover image



Fig.8. (a). Secret image (b). 4 LSB secret image and (c). recover secret image

Table.2. Results for BPCS algorithm

Video	EC %	PSNR	Hiding Length	NCCF
Color (.avi)	70.83	49.16	163200	0.99
Nature (.flv)	75	54	691200	0.99
Gray (.mp4)	77	55.34	702389	1

Table.3. Comparison of existing BPCS and our approach

Algorithm	EC %	PSNR	BER	NCCF
[8]	63	26.79		
[05]	118140 byte	47.7		
[07]	760864	38.03		
Proposed (Color image)	70.83	49.16	0.005	0.99
Proposed (Nature image)	75	54	0.006	0.99

Table.4. Result obtain for audio1 and audio2

Audio (LSB)	EC %	PSNR	BER	Hiding Length	NCCF
.wav	62.63	49.16	0.006	537452	1
.mp3	64.56	50.65	0.004	491247	0.99

Table.5. Comparison of [08] BPCS/4LSB and our approach

Rosane English [08]			Our approach on color image				
Param- eters	EC	PSNR	EC(bits)	PSNR	BER	MSE	NCCF
BPCS	63%	26.79	75% (BPCS)	54	0.04	0.5	0.99
4LSB	50%	39.91	3686400 (4LSB)	51.99	0.5	0.5	0.99
Attacks	Yes	Yes	Yes				
Type of stegan- ography	Image	-	Video and Audio				
Security	less		More				

(c)

Swain et al. [12], Mare et al. [13], Bagade [14]			Proposed method				
	PSNR (dB)	EC(bits)	PSNR	EC (bits)	BER	NCCF	
1LSB	51.11	32400	51.13	921600	0.5	0.99	
2LSB	44.39	65536	44.37	1843200	0.5	0.99	
4LSB	33.88	131044	32.15	2764800	0.49	0.99	
SLSB [12]	44.36	131072	51.13	921600	0.49	0.99	
[14]	51.12	262144	51.13	921600	0.49	0.99	

Table.6. Comparison of [12]-[14] and our approach

Table.7. Results for 8-4-2-1 LSB coding

Video	LSB	PSNR	MSE	Attacks	PSNR	MSE	NCCF
.avi	1	60.63	0.05	Speckle	59.12	0.05	0.99
512*512	2	56.69	0.04	Visual	56.20	0.04	0.99
(Lena)	3	54.34	0.05	Poison	54.23	0.04	0.99
512*512	4	51.99	0.04	Rotational	51.02	0.04	0.99
.mp4	1	59.23	0.07	Paper and Salt	59.01	0.05	0.99
512*512	2	55.98	0.03	Speckle	55.12	0.02	1
Cat	3	52.13	0.04	Poison	51.23	0.05	0.99
256*256	4	50.24	0.04	Paper and salt	49.90	0.03	0.99
	1	49.23	0.04	Speckle	49.01	0.03	0.99
WOW	2	47.13	0.04	Rotational	46.21	0.04	0.99
.wav Audio 1	3	44.98	0.05	Paper and Salt	44.01	0.04	0.99
	4	38.83	0.05	Visual	37.20	0.08	0.96

Table.8. Results obtain for BPCT algorithm	
--	--

Video	Algorithm	PSNR	Attacks	PSNR	NCCF
			Speckle	69.76	0.99
.avi 512*512		70.83	Poison	70.12	0.99
(Lena) 512*512	(Lena) BPCT	70.83	Paper and salt	70.32	0.99
512 512			Rotational	70.23	0.99
		70.83	Speckle	69.09	0.99
.flv 512*512 Cat 256*256	BPCT		Paper and salt	7012	0.99
			Poison	70.21	0.99
			Rotational	70.45	0.99

7. CONCLUSION

In this paper we have applied BPCT and LSB algorithm to embed the secret data as text, image and audio. For video steganography BPCT method shows good results on natural video as natural video have large areas of uniformity and sharply define border. For audio video steganography in which BPCT algorithm is used for hiding the secret information inside the selected frames of video and LSB technique to conceal the secret data into audio which improve the embedding capacity and provide more security. In future it can be applied on online video transition from source to destination with different attacks to increase the hidden data security.

REFERENCES

- [1] Manasi Subhedar and V.H. Mankar, "Current Status and Key Issues in Image Steganography: A Survey", *Computer Science Review*, Vol. 13-14, pp. 95-113, 2014.
- [2] Mennatallah M. Sadek, Amal S Khalifa and Mostafa G.M Mostafa, "Video Steganography: a Comprehensive Review", *Multimedia Tools Application*, Vol. 74, No. 17, pp. 7063-7094, 2015.
- [3] George Abboud, Jeffrey Marean and Roman Yampolskiy, "Steganography and Visual Cryptography in Computer Forensics", Proceedings of IEEE 5th International Workshop on Systematic Approaches to Digital Forensic Engineering, pp. 25-32, 2010.
- [4] SghaierGuizani and Nidal Nasser, "An Audio /Video Crypto Adaptive Optical Steganography Technique", Proceedings of IEEE 8th International Conference on Wireless Communication and Mobile Computing, pp. 1057-1061, 2012.
- [5] Smita Bansod, Vanita Mane and R. Ragha, "Modified BPCS Steganography using Hybrid Cryptography for Improving Data Embedding Capacity", *Proceedings of IEEE International Conference on Communication, Information and Computing Techniques*, pp. 1-5, 2012.
- [6] Souvik Bhattacharyya and Aparajita Khan, "Pixel Mapping Method based Bit Plane Complexity Segmentation Steganography", *Proceedings of IEEE World Congress on Information and Communication Technique*, pp. 36-41, 2011.
- [7] Peipei Shi, Zhaohui Li and Tao Zhang, "Technique of Improved Steganography Text based on Chaos and BPCS", *Proceedings of IEEE 2nd International Conference on Advanced Computer Control*, pp. 232-236, 2010.
- [8] Rosane English, "Comparison of High Capacity Steganography Techniques", Proceedings of 2nd IEEE International Conference on Soft Computing and Pattern Recognition, pp. 448-453, 2010.
- [9] Sunil K. Moon and Rajeshree D. Raut, "Analysis of Secured Video Steganography using Computer Forensic Technique for Enhanced Data Security", *Proceedings of IEEE 2nd International Conference on Image Information Processing*, pp. 660-665, 2013.
- [10] Hamdy M. Kelash, Osama F. Abdel Waheb, Osama A. Elshakankiry and Hala S.EI Sayed, "Hiding Data in Video Sequence using Steganography Algorithms", *Proceedings*

of International Conference on ICT Convergence, pp. 353-358, 2013.

- [11] Jidagam Venkata Kartik and B Venkateswara Reddy, "Authentication of Secret Information in Image Steganography", *International Journal of Latest Trends in Engineering and Technology*, Vol. 14, No. 6, pp. 97-104, 2013.
- [12] G. Swain and S. Lenka, "LSB Array based Image Steganography Technique By Exploring the Four Least Significant Bits", *Global Trends in Information System and Software Application*, Vol. 270, pp. 479-488, 2012.
- [13] S.F. Mare, M. Vladutiu and L. Prodan, "Decreasing change Impact using smart LSB Pixel Mapping and Data Rearrangement", *Proceedings of IEEE 11th International Conference on Computer and Information Technology*, pp. 269-276, 2011.

- [14] Anant M. Bagade and Sanjay N.Talbar, "A High Quality Steganography Musing Morphing", *Journal of International Process System*, Vol. 10, No. 2, pp. 256-270,2014.
- [15] Geeta Kasana, Kulbir Singh and Stavanger Singh Bhatia, "Data Hiding Algorithm for Images using Discrete Wavelet Transform and Arnold Transform", *Journal of Information Processing System*, Vol. 13, No. 5, pp. 1331-1344, 2015.
- [16] F. Arab, M. Shahidan and S. Abdullah, "A Robust Video Watermarking Technique for the Tamper Detection of Surveillance System", *Multimedia Tools and Application*, Vol. 75, No. 18, pp. 10855-10865, 2016.
- [17] Hung-Min Sun, Chi-Yao Weng, Chin-Feng Lee and Cheng-Hsing Yang, "Anti-Forensics with Steganographic Data Embedding in Digital Images", *IEEE Journal on Selected Areas in Communications*, Vol. 29, No. 7, pp. 1392-1403, 2011.