Integrated Approach for Text Hiding through Video using Steagnography and Visual Cryptography

Sabyasachi Samanta
Haldia Institute of Technology, Haldia, WB, INDIA
E-mail id: sabyasachi.smnt@gmail.com

Saurabh Dutta
Dr. B. C. Roy Engineering College, Durgapur, WB, INDIA
E-mail id: saurabh.dutta@bcrec.org

Gautam Sanyal
National Institute of Technology, Durgapur, WB, INDIA
E-mail id: nitgsanyal@gmail.com

Abstract- Video steganography is a practice to hide information into carrier image files of video. Employment of the video steganography is more appropriate than the other carriers, not only for its magnitude but also the choice to pick the arbitrary image file(s). In this paper, we have worked on with a combination of encryption, steganography and visual cryptography. Initially, we have encrypted the data bits using one sorting based encryption technique. Then embedded that cipher text to some targeted frames of the video and also to some suitable nonlinear pixel positions of that image frames. Both of the encryption and embedding process have done by using distinct secret key. Next, some video shares have generated using color components of image and also key shares correspondingly. At the time of decryption, the video and key shares need to reschedule with proper order that make possible to retrieve hidden data bits from stego-video. The computational time for the decryption process is fewer than the other predictable video steganography methodologies. Without investigate all of the enclosures, cipher text are collected simply from the selected frame, pixel and bit positions which is selected by the secret key. Finally, the cipher text is decrypted by sorting based decryption algorithm.

Key words: Information Security, Nonlinear Pixel Position (NPP), Encryption, Video Steganography, Visual Cryptography

1. INTRODUCTION

Encryption is a process to alter plaintext into the cipher text and decryption is reverse of it. Video steganography is a very significant field of digital steganography [1][2]. The visual cryptography uses secret sharing scheme based on {k, n} threshold frame, a secret image will be hidden in n transparencies, and require k or more (≥k) transparencies to reconstruct the secret image [3][4][5].

At this time, we have embedded the data bits about the random video frames, pixel and bit positions. The text taken from the keyboard or special characters encoded into its ASCII-8 binary equivalent. Then the data bits are encrypted through Sorting Algorithm based Encryption (SAE) method. Using the Nonlinear Pixel Position (NPP) method arbitrary positions are selected in entire image (video frame). The arbitrary frame positions are selected using the key. The ASCII value of neighbor key characters has multiplied and modulus division performed to total frames, to select frame positions. At the time of embedding, data bits are taken and rooted to selected frames at nonlinear pixel positions through the key and stego-image is generated. After that, we have formed different video and key shares using components of video based on visual cryptography as in Table 1. Cascading the above newly developed schemes, an integrated security scheme for video has been developed.

In our work, we have targeted any one of last four significant bit of each R, G and B of any selected random pixel positions in video frame. The replacement of all the bits have done in nonlinear pixel and bit positions, in any one of last four significant bit of R,G and B at selected pixels about the entire image using the private key. We have altered only any one bit of last four significant bits. If any bit generated from text become similar to the targeted bit of image then there will be no alteration.

Table 1: Image and Video Share Formation

Image/key Shares	**Image Shares**			**Key Shares**		
	IM_R	**IM_G**	**IM_B**	**K_1**	**K_2**	**K_3**
Share1	A	P	P	A	P	P
Share2	P	A	P	P	A	P
Share3	P	P	A	P	P	A

2.RELATED WORKS

In this section we have discussed various video steganographic data hiding methodologies.

R. Balaji et. al. [6] proposed a secure data communication using video steganography that produces a index/directory for the secret information. That index is itself positioned in a frame of the video itself. With the help of this index, the frames which contain the secret information are originated. As index is placed in video ,it lessens the computational time taken for the elimination process.

Mrudul Dixit et. al.[7] proposed a video steganography method to secret data and is replaced at the LSB positions of pixels of the carrier video frame. It becomes very difficult for an attacker to guess that data is hidden in the video.

Kunal Hossain et. al. [8] proposed a method of image, audio and video steganography by converting the media type into a dissimilar form. Each frame of the video is considered as a single RGB image. Later, the frames are transformed into relevant number of sound files.

Yugeshwari Kakde et. al.[9] proposed an algorithm for audio-video steganography. They proposed an algorithm for hiding image in selected video sequence is an image-hiding technique based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) and random LSB audio steganography method for hiding secret text information inside audio of the audio-video file, which reduce embedding distortion of the host audio.

Nirmalya Kar et. al. [10] proposed a chaos-based video steganography. They proposed the method based on Non-Linear Feedback Shift Register and Tinkerbell 2D chaotic map. The major work using chaotic map was restricted to image steganography. Those significant restrictions were to increase payload. In their work, 2D chaotic map and NLFSR are used to develop a video steganography mechanism where data will be embedded in the segregated frames. This will increase the data hiding limit exponentially. Also, embedding position of each frame will be different from others frames which will increase the overall security of the proposed mechanism.

A. Munasinghe et. al. [11] proposed a video steganography by changing the LSB of each byte of the carrier file. The limitation for this development is that the library avifill32.dll can only be used for uncompressed AVI files.

Pooja Yadav et. al. [12] also proposed a secure video steganography with encryption based on LSB technique. Each frame of secret video was broken into individual components then converted into 8-bit binary values, and encrypted using XOR with secret key and encrypted frames will be hidden in the LSB of each frames using sequential encoding of cover video.

3. THE SCHEME

This section represents an innovative algorithm for "Integrated Approach for Text Hiding through Video using Steagnography and Visual Cryptography" technique. Section 3.1 includes the three algorithms 3.1.1, 3.1.2 & 3.1.3 for encryption and section 3.2 describes the decryption of it.

3.1 Encryption of data bits about the video and formation of video shares

3.1.1 Create an encrypted array using SAE

Step I: Calculate the message length (M_l). Convert the length into its equivalent 8-bit binary and store it to encryption array (Earr[]).

Step II: Take a key (K) with length 8 and split its alphanumeric characters (K_c).

Step III: Insertion sorting techniques is applied to sort the key characters in ascending order based on ASCII-8 value.

Step IV: Transform each character of plaintext into its ASCII-8 equivalent.

Step V: Depending on key character positions, ASCII value of message is transposed or replaced.

Step VI: Calculate the total (T) of ASCII-8 value for key characters and perform n=T%8.

Step VII: If the reminder is odd then the ascending order and n^{th} bit left shift operation is performed. Otherwise, the descending order and right shift operation is performed. If reminder is zero, then in ascending order and no bit shifting.

Step VIII: Store the binary values encoded from characters to Earr[], LSB to MSB.

Step IX: Repeat Step IV to Step VIII for i=1 to $M_{l.}$

Step X: Stop.

3.1.2 Stego frame formation using NPP

A. Selection of the nonlinear pixel positions of selected video frame

Step I: Arbitrary frames are selected using key.

Step II: Total number of required pixels (p) are calculated by p= (ceil (bit /3)).

Step III: Compute F(x, y) = K^p [i.e. pow (k, p)].

Step IV: The values up to "e" are accumulated onto file from the exponential long double values.

Step V: Obtain most three significant digits to $Earr_x$[p], next three digits to array $Earr_y$ [p] and last significant digit to $Earr_z$[p].

Step VI: Repeat Step V for all of the values.

Step VII: Stop.

B. Replacement of array elements to pixel

Step I: Pixel positions are selected (as x=$Earr_x$[p] and y=$Earr_y$[p]) into frame by comparing the value of x and y with the value of w and h. If (x >(w-1)) or (y >(h-1)) then P (x, y) = P (0+(x %(w-1)), (0 +(y %(h-1))). Otherwise, set P (x, y) = (x, y).

Step II: To select the bit position (b) of selected pixel, set z =$Earr_z$[p].

i) If (z%4=0) then b=1^{st} LSB

ii) If (z%4=1) then b=2^{nd} LSB

iii) If (z%4=2) then b=3^{rd} LSB

Otherwise, b=4^{th} LSB of each R, G & B component.

Step III: Repeat Step I to Step II for i=1 to p.

Step IV: Stop**.**

3.1.3 Creation of video and key shares

Step I: Create the video shares (VS_0- VS_2) with presence (P) or absence (A) of Red (V_R), Green (V_G) and Blue (V_B) components respectively.

Step II: Also the key shares (KS_0-KS_2) are with presence (P) or absence (A) of key components (K_1, K_2 and K_3).

Step III: Stop.

3.2 Decryption of the data bits from the stego-video

Step I: Take any two video and key shares to reform the stego-video and key.

Step II: To get the pixel and bit position in R, G & B of selected pixels go through 3.1.2.A and Algorithm 3.1.2.B.

Step III: Retrieving data bits from the selected bit position of selected pixels, store it to decrypted array from Darr[1] to Darr[bit].

Step IV: Taking data values from the decrypted array Darr[], LSB as Darr[8*i+1] and MSB as Darr[8*(i+1))] respectively. Repeat Step III to Step IV to decrypt the data bits and convert to its equivalent ASCII-8 character. Store the character to an array Msg[len].

Step V: Apply insertion sorting techniques for the key digits/characters in ascending order based on ASCII-8 value of Darr[].

Step VI: Place the array bits based on sorted key character positions (as in 3.1.1. Step V and VI) and replace the data bits as per original key characters and store to message array (Marr[]).

Step VII: Repeat Step V to Step VI for Darr[].

Step VIII: Finally place the characters one by one assemble the original message.

Step IX: Stop.

4. IMPLEMENTATION AND EXPERIMENTAL RESULT

In this section, we have considered a separate plaintext (P) as: “IMAGE”.

Table 2: Encryption Table for SAE Method

	Digit/Character Position							
	0	1	2	3	4	5	6	7
Key Characters	6	3	A	7	5	B	8	9
ASCII-8 value	54	51	65	55	53	66	56	57
After Insertion Sort	51	53	54	55	56	57	65	66
ASCII Characters	3	5	6	7	8	9	A	B
ASCII-8 Binary of Message character ‘N’	0	1	0	0	1	1	1	0
After Transposition	1	1	0	0	1	0	0	1
After Left Shift	1	0	0	1	0	0	1	1

Table 3: Binary Value after Encryption Using SAE Method

Character	Equivalent ASCII-8 Binary Value	Binary Value after Encryption
I	01001001	10001001
M	01001101	10001011
A	01000001	00001001
G	01000111	00011010
E	01000101	00001010

Let the key (K) =63A75C.

Number of effected pixel required for data (p) = [ceil (90/3)] =30.

Here we have taken a very short duration (tribal dance) video that contains 117 frames.

The frame size= 640 X 480 (w x h).

Here we have targeted only one arbitrary frame. For our total data 30 pixel positions are required. Calculate total (t) =54+51+65+55+53+67=345.

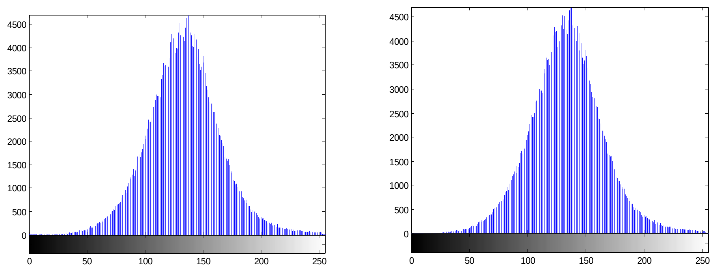
Frame position = [(54x51) % 117] = 63.

Table 4: Selected Pixel Position for NPP-1 Bit

(Key, i)	Value	Pixel Position	Bit Position	Array Data
345,1	3450000E-04	(89,128)	LSB	Earr[1] Earr[2] Earr[3]
:	:	:	:	:
345,30	2533486E 222	(125,92)	3rd LSB	Earr[88] Earr[89] Earr[90]

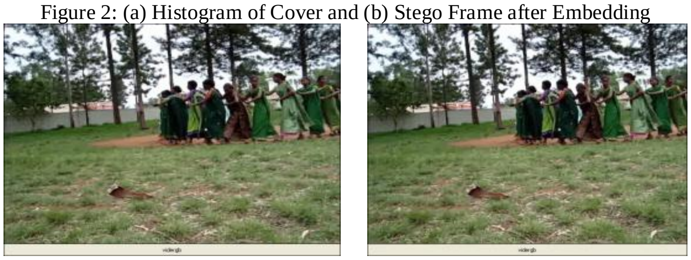
(a) (b)

Figure 1: (a) Cover and (b) Stego Frame after Embedding



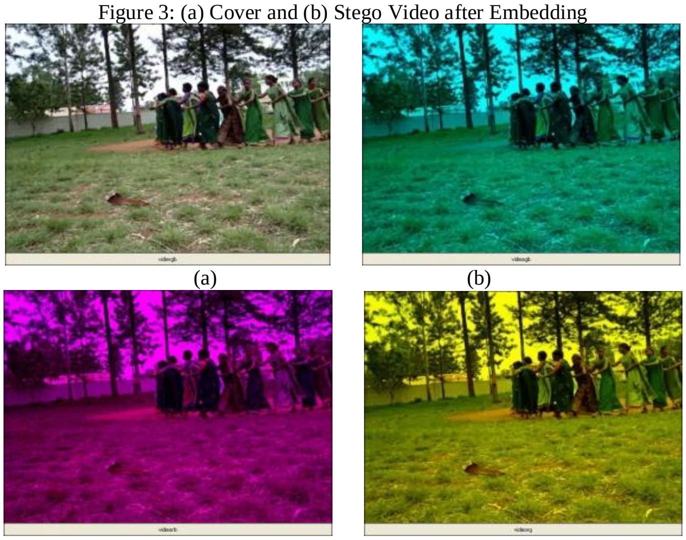
(a) (b)

Figure 2: (a) Histogram of Cover and (b) Stego Frame after Embedding



(a) (b)

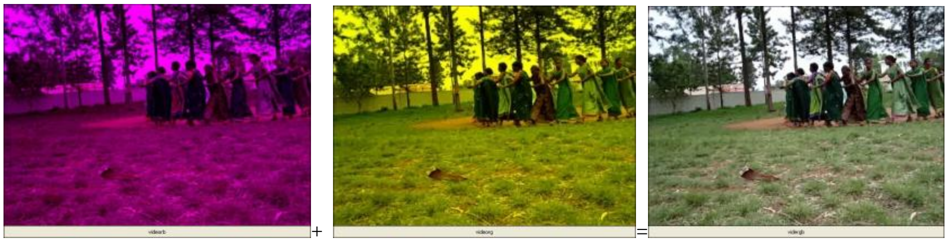
Figure 3: (a) Cover and (b) Stego Video after Embedding



(a) (b)

(c) (d)

Figure 4: (a) The original video, (b) (c) and (d) video shares



(a) (b) ©

Figure 5: Orignal video formation

Table 5: Comparison of Proposed and other Methodologies

Method Name	Video File Name	Resolution	Frame Rate	Total Number of Frames	MSE	PSNR	Payload (Kb)
HLSB[13]	Drop.avi	256*240	30	182	0.34	44.34	2.66
LSB Poly[14]	Drop.avi	256*240	30	182	0.42	48.56	1
MSLB [15]	Globe.avi	320*240	30	107	0.295	53.43	13.3
HES[16]	Globe.avi	320*240	30	107	0.46	51.43	13.3
Proposed Method	Tribal_Dance.mpg	640 x 480	30	117	0.036	55.29	4

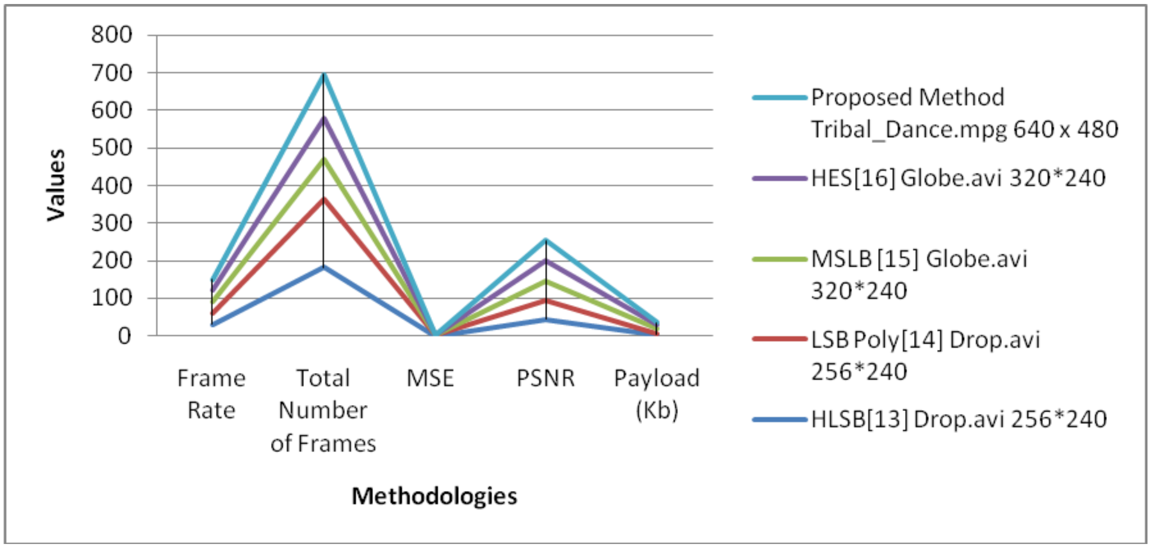


Figure 6: Graphical Comparison of Proposed and other Methodologies

5. ANALYSIS

Here we have proposed a novel video share based security approach. A stego-video has been produced by employing an encryption technique and then the video shares using color components. Use of any compression technique may produce the length of array less and then strength of encryption will be higher than present. As well the amount of resulting pixel will be less. We have targeted random frame, pixel and bit positions depending on key value. Limited number of frames is selected depending on key value, without considering all of the enclosures. So for at the time of decryption, without investigate all of the enclosures, data bits are collected only from the selected frame, pixel and bit positions. That’s why the computational time for the decryption process is fewer than the conventional process. Also video and key shares have generated based on color components and key characters simultaneously. We have used six alphanumeric characters. More over someone may use only numerical digits/characters with more/less length. As well may generate more subset of key. In this work we have targeted only three frames. Anybody may target any number of frame(s) of the video. The data bits are placed any four LSB position. Anybody may place less or more number of bits in any pixel position (LSB to MSB) to each of R, G and B color components. The number of targeted pixels proportionally varies to size of text. If the video size becomes large and size of text becomes less then it will be quite harder to differentiate the encrypted video from the original video. Figure 6 represents the graphical comparison of proposed and other well-known methodologies[17]. The result shows an improvement in terms of imperceptibility, robustness and embedding capacity in video steganography domain than the other methodologies [Ms. Pooja Vilas Shinde et. al.].

6. CONCLUSION

We have used private key cryptographic technique to place the data bits (from both text and size of text) in arbitrary pixel positions about the video and also have generated random frame and pixel positions depending on key. After that video and key subsets have generated from stego-video and key. Moreover, it produces the similar video using this method to see in naked eye. After that the resultant video shares are totally different from the stego-video. At the time of decryption only a proper combination of video and key subsets may produce the original stego-video and key from which, data can be extracted with least amount time. After all, it will be quite impossible to find out the information from the stego-video.

REFERENCES

[1] Jafar Mansouri and Morteza Khademi, "An Adaptive Method for Compressed Video Steganography Using Temporal and Spatial Features of the Video Signal", ICEE, Iranian Conference on Electrical Engineering, pp. 575-579, 2009

[2] Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt, "Skin Tone Based Steganography in Video Files Exploiting the Ycbcr Colour Space", ICME, pp.905-908, 2008

[3] Mritha Ramalingam, " Stego Machine – Video Steganography using Modified LSB Algorithm", World Academy of Science, Engineering and Technology, Vol: 50, pp.443-446, 2011

[4] Yu-Chi Chen, Gwoboa Horng and Du-Shiau Tsai, "Comment on Cheating Prevention In Visual Cryptography", IEEE Transactions on Image Processing, Vol. 21, No. 7, July, pp.3319-3323,2012

[5] In Koo Kang, Gonzalo R. Arce and Heung-Kyu Lee, "Color Extended Visual Cryptography Using Error Diffusion. IEEE Transactions on Image Processing", Vol. 20, No. 1, January, pp. 132-145, 2011

[6] R. Balaji and G. Naveen, "Secure Data Transmission Using Video Steganography", IEEE International Conference On Electro/Information Technology, 15-17 May, Mankato, MN, USA, 2011

[7] Mrudul Dixit, Nikita Bhide, Sanika Khankhoje and Rajashwini Ukarande, "Video Steganography", International Conference on Pervasive Computing (ICPC), 8-10 Jan. 2015, Pune, India, 2015

[8] Kunal Hossain and Ranjan Parekh, "An Approach Towards Image, Audio and Video Steganography", International Conference on Research in Computational Intelligence and

Communication Networks (ICRCICN), 23-25 Sept., Kolkata, India, 2016

[9] Yugeshwari Kakde, Priyanka Gonnade and Prashant Dahiwale, "Audio-Video steganography", International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 19-20 March, Coimbatore, India, 2015

[10] Nirmalya Kar, Md A A A. Aman, Kaushik Mandal and Baby Bhattacharya, "Chaos-Based Video Steganography", 8th International Conference on Information Technology (ICIT), 17-18 May, Amman, Jordan, 2017

[11] A. Munasinghe, Anuja Dharmaratne and Kasun De Zoysa, "Video Steganography", International Conference on Advances in ICT for Emerging Regions (ICTer), pp. 056 – 059, Colombo, Sri Lanka, 2013

[12] Pooja Yadav, Nishchol Mishra and Sanjeev Sharma, "A Secure Video Steganography with Encryption Based on LSB Technique", International Conference on Computational Intelligence and Computing Research, 26-28 Dec., Enathi, India, 2013

[13] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta, "Hash based Least Significant Bit Technique for Video Steganography (HLSB)", International Journal of Security, Privacy and Trust Management (IJSPTM), Volume 1, No 2, pp. 1-11,2012

[14] A. Swathi and S.A.K Jilani, "Video Steganography by LSB Substitution Using Different Polynomial", International Journal of Computational Engineering Research (ijceronline.com), Volume 2, Issue 5, pp. 1620-1623,2012

[15] Mritha Ramalingam, "Stego Machine-Video Steganography using Modified LSB Algorith" World Academy of Science, Engineering and Technology, Volume 5, pp. 425-428, 2011

[16] Ashawq T. Hashim, Dr. Yossra H. Ali & Susan S. Ghazoul, "Developed Method of Information Hiding in Video AVI File Based on Hybrid Encryption and Steganograph", Engg. and Tech. Journal, Volume 29, No.2, pp. 359-364,2011

[17] Ms. Pooja Vilas Shinde and Tasneem Bano Rehman, "A Survey: Video Steganography techniques", International Journal of Engineering Research and General Science, ISSN 2091-2730, Volume 3, Issue 3, pp. 1457-1464, 2015

Sabyasachi Samanta is working as Assistant Professor at Dept. of IT, Haldia Institute of Technology Haldia, WB, and India. He has received Ph. D at National Institute of Technology, Durgapur, WB, India. His main research interest includes watermarking, steganography and cryptography.

Saurabh Dutta is a professor in Dr. B. C. Roy Engineering College. He holds a Ph. D Degree in Coputer Science. His research domain is information security and cryptology.

Gautam Sanyal is a member of the IEEE. He has received his B.E and M. Tech degree from National Institute of Technology (NIT), Durgapur, India. He has received Ph.D. (Engg.) from Jadavpur University, Kolkata, India, in the area of Robot Vision. His research interests include Natural Language Processing, Stochastic modeling of network traffic, High Performance Computing, Computer Vision. He is presently working as a Professor in the department of Computer Science and Engineering at National Institute of Technology, Durgapur, India.