I.J. Image, Graphics and Signal Processing, **2020, 1, 10-17**
Published Online February 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2020.01.02

Secure Data Transmission in Video Format Based on LSB and Huffman Coding

Shwe Sin Myat Than
University of Computer Studies, Hpa-an, Myanmar
Email: ssmyatthan@gmail.com

Received: 26 July 2019; Accepted: 23 August 2019; Published: 08 February 2020

Abstract—The growth of needing to transmit bit amount of data through the internet in secure format encourage the research for steganography technique, especially in video file. Stenographic technics in video format gives many advantages to transportation of important data because video files are a part of people's daily life and the attackers can't notice easily. The high embedding capacity of video file improves the popularity of video steganography among the various media types. Therefore, the simplest form but with many advantage of (Least significant bit) LSB, that is enforced with the high compression method of Huffman chunk coding method is proposed in this paper to embed data in video file in multi-step cryptography embedding schemes. The intension is to get more secure nature of the system and to get more embedding capacity system. The experiments are carried out with various sizes of video files and text file sizes are used to show the effectiveness of the proposed methods. The results manifest superior performance for proposed algorithm with the performance parameters like Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Bit Error Rate (BER) are calculated to test the quality of stego video.

***Index Terms*—**Bit Data, Cryptography, Huffman Chunk Coding, LSB (Least significant bit), Video Steganography

I. Introduction

Currently, the video files are used due to increasing internet technologies to share data in various fields such as business processes, medical records, broadcast information, banking information, and military intelligence. Due to increasing demand for digital communication in various environments, a confidential approach is utilized to protect the secret data from attacks. The two techniques such as steganography, cryptography are utilized to achieve secret communication in worldwide.

Steganography is an essential technique for hiding information in secure format where the important content is concealed in carrier cover media file without a distortion of its presence. The various types of steganography techniques block diagram is shown in figure 1. Fundamentally, steganography mechanisms have six types: image steganography, audio steganography, video steganography, text steganography, DNA steganography and protocol steganography [1, 2].

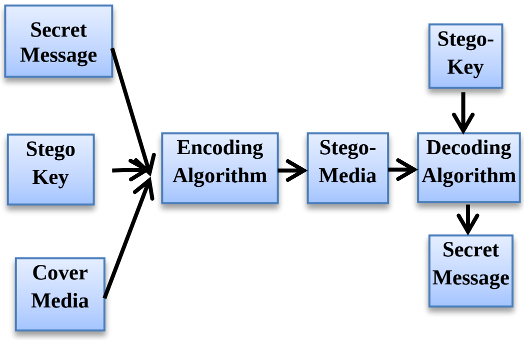


Fig.1. General Block Diagram for Steganography technique

Between the different types of stego techniques, this paper concentrates on video transmission using steganography. The purpose of video steganography is to achieve the goal of secret communication and send the secret information to the target side safely through insecure environment. Video file is a combination of various types of frames and the constituting of these frames forms a video file in a fixed rate. These separate frames are vital building block for the video file as well as for video encryption process. Various types of media file format such as text, image, audio and video can be inserted along with the frames by using various techniques as shown in the Fig. 2 [3, 4].

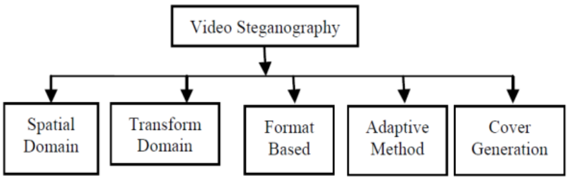


Fig.2. Video Steganography Types

Among the various algorithms in Video Steganography, Least Significant Bit (LSB) substitution is the most frequently used algorithm for data embedding in Spatial Domain types. In most applications, the LSB substitution method can be found as the complement of another method because it has the weakness nature where embedded message can be easily find by the attackers [5]. Therefore this system is proposed triple embedding mechanism to increase the transmission of secret data using video steganography based on LSB and Huffman Chunk Coding method.

The presentation form of the remaining part of the paper is as follows. Section II illustrates the literature reviews for video steganography works and the researches that used the methods LSB and Huffman Coding. Section III describes the methodology that used in the proposed system. Section IV presents about the proposed work. Section V discusses about the performance measurement that used for this system. Section VI is for the results that are collected when the system is experimented. Section VII is the end section and it concludes the paper.

II. Related Work

Video Steganography is a relatively new popular and attractive steganographic medium in today world. There are many proposed works in the previous time for hiding data in video file to encode secrete information in various domains. This paper concentrate on spatial domain and review for that domain have been done in categorization for each media.

The works for encoding text in a video file based on LSB technique have been done in papers [6, 7]. The women engineers from India [6] have done data security technique in which secret data is embedded in cover video. LSB replacement method of data hiding has been implemented and tested for video steganography. They showed the results that describe LSB technique is robust and requires less computation time and there are no bit errors for the received message. The authors from [7] also propose a new method for video steganography for text data based on LSB technique by using Randomization and Parallelization. They embedded the secret information in random frames using FSR to take less computation time in steganography process. They recommend that their algorithm technique encodes high volume of data and can also use for other media information as further extension. The authors in [8] analyzed video steganography techniques and the method of Least Significant Bit, LSB. They also emphasize on the LSB method of video steganography with the different parameter such as PSNR, MSE and RMSE. They describe the text message hiding process of LSB in cover video.

The mechanism for transmission secret image in a video file can be seen in prposed papers [9, 10]. The research for image in video steganography scheme with a combination of LSB substitution and additional AES encryption to apply on the Android platform is proposed in [9]. The researchers used MP4 video as the media cover and JPEG image as the inputs to be the embedded secret message. They show the result for both the stego-video and the decrypted image file quality. The authors in [10] also introduced the video steganography based on human vision ROI with face detection algorithm to increases capacity rate of the information embedding. Their proposed research is intended for images of medical system. For each of the frame in video file, index values are collected based on motion and calculate the variation range, then the interested region of human is selected according to this value. Although the credential information is inserted as different level in different regions, they get the high PSNR value and little amount of MSE.

The research for embedding secret audio file in a video file has been proposed in paper [11]. The writers developed a generalized algorithm to embed an audio file within a digital video format using the simple LSB technique. To conceal the audio data inside a video file, the random number sequence is generated to serves as a cryptographic technique. The results show the nature result of audio encryption, a low MSE value over 4 is obtained along with a high PSNR of 101.7709 for the video frame after embedding the audio samples.

The investigation approaches for encrypting video file into a cover video file can be seen in works [12, 13]. The secured system of video steganography using LSB technique is done in paper [12]. They proposed a novel video steganography system that has the capability of security and high capacity, based on the image steganography of LSB to hide a video behind a video. Their system is designed based on the simple LSB method with addition of symmetric encryption and sequential encoding to get the improve security level of the steganography system. The researchers in [13] also proposed the new technique of video steganography by improving LSB technique. They implemented cover frame pixel randomization, de-randomization and data embedding technique to maintain the quality of the secret video file and prevented it from being accessed by impostors while communication through internet. The levels of security are getting from Prime Factorization Method applied on cover or stego-video frames though scrambling and de- scrambling its pixels. In their proposed approach data embedding is done by a new method called Spiral LSB method. They deal with embedding the confidential video within a cover video without degrading the quality of the cover video.

Many experience researchers declare that although the simple LSB based steganographic technology has some advantages, the weakness of its strategy should not be neglected. Therefore, they proposed the new methods in different way as the extension of LSB. The researchers in [14] and [15] also proposed LSB method with the use of Huffman coding in different ways in image steganography. The authors in [14], proposed the steganography method in image by using LSB and Huffman coding on gray level image. They compared the results of LSB simple and the combination of LSB and Huffman methods, and recommend that the combination of LSB and Huffman method is better than single LSB method to hide text into image. The authors in [15] continue research works for image steganography using Least Significant Bit (LSB) technique with Huffman Coding to reduce the amount of data bits to be inserted into the cover carrier in order to achieve efficient image steganography. They recommend that more efficient steganography can be implemented in terms of compression ratio by using the hybrid method in image steganography.

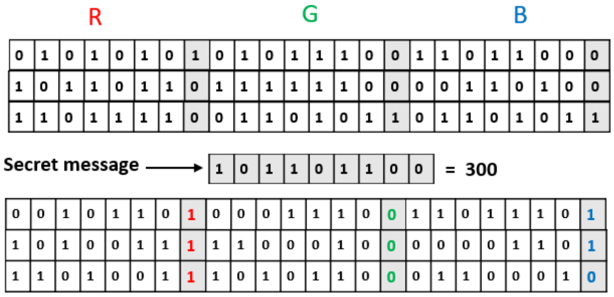
From the review process of the previous works, a statement can be seen clearly that there is nothing done in video steganography with the combination of LSB and Huffman coding methods.

III. Background Methodology

This system used the combination of Least Significant Bit, LSB and Huffman coding methods with the use of multi-step embedding ideas.

A. *Least Significant Bit (LSB)*

The bits of the secret text message can be changed with the 8th bit of the LSB in an image. With the RGB pixel in an image with the bit depth of 24, 3 bits can be stored within each pixel by altering a bit each of RGB components as they are each represented by a byte. An image of 800x600 pixel size can store a total of 180,000 bytes (1,440,000 bits) of secret inserted text. The LSB portion of the cover image is utilized to embed information. Fig.3 is a simple example of hiding the number 300 into the first 8 bytes, where only 5 bits are required to be changed in the embedded secret information. Therefore, embedding a secret message with the maximum carrier size requires altering only half of the image bits. Each primary color consists of about 256 potential intensities. There are minor variations in the intensity of the colors when the LSB is changed unrecognizably. The normal human eyes cannot realize these variations due to its insensitivity to color progression; so, the secret information is successfully inserted into the images [2, 16 and 17].



			R									G									B		
0	1	0	1	0	1	0	1	0	1	0	1	1	1	0	0	1	1	0	1	1	0	0	0
1	0	1	1	0	1	1	0	1	1	1	1	1	1	0	0	0	0	1	1	0	1	0	0
1	1	0	1	1	1	1	0	0	1	1	0	1	0	1	1	0	1	1	0	1	0	1	1

Secret message →

1	0	1	1	0	1	1	0	0

= 300

0	0	1	0	1	1	0	1	0	0	0	1	1	1	0	0	1	1	0	1	1	1	0	1
1	0	1	0	0	1	1	1	1	1	0	0	0	1	0	0	0	0	0	0	1	1	0	1
1	1	0	1	0	0	1	1	1	0	1	0	1	1	0	0	0	1	1	0	0	0	1	0

Fig.3. Example pixel substitution of LSB method

B. *Huffman Chunk Coding*

Huffman coding [18] is the less of losing data method in compression algorithms based on the frequency number of the occurrence of a data item. The idea behind the method is to allocate variable-length of codes for the input characters based on their frequencies number of equivalent characters. The most frequent character gets the shortest code and the least character gets the longest code. This idea improves the compression rate. The produced codes are prefix codes, i.e. the code allocate to a character is not prefix of the code allocated to any other characters. Huffman Tree is built from input characters and then all the codes are assigned for all characters by navigating the Huffman Tree.

After Huffman tree has been build, a codeword can be get. This codeword links with each symbol in the Huffman code dictionary. Huffman coding needs this dictionary information of the data being encoded to be used when decoding process of that data [19].

C. *Combination of the LSB and Huffman Coding*

The combination of LSB and Huffman Coding method is the serial integration. Firstly the secret text is encoded in an artificial image created by zero function using LSB method. The substitution can be done any bit among the 8 bits. The substituted text is then coded using Huffman method. Finally the codeword of Huffman method is encoded again in each frames of the cover video using LSB method with a secret file.

IV. Propose System DesiGN

A secure video steganography method for data transmission based on LSB approach is presented. To overcome the weakness or disadvantages of LSB techniques, Huffman coding method is served as the additional method in data hiding process. The principle of LSB is that, the data is inserted in an existing bits of the video frame, no additional bytes is added. Huffman coding method is used as the data compression technique to get the high capacity embedding mechanism. The Huffman algorithm is easy to implement and produces lossless compression and it saves more capacity in the size of the message. Furthermore, to get the security and robustness in data transmission process, only the cipher text is embedded and uses the confidence key technique. The proposed video steganography mechanism consists of two stages such as

- Embedding Process at the Sender Side
- Decryption Process at the Receiver Side

A. *Embedding Process at the Sender Side*

Fig.4 illustrates the process of proposed video steganography framework at the sender side. The brief process steps are as follow;

1. Input secret text file to make transmission
2. Enter the no of LSB bits to be substituted
3. Encode text with LSB insertion
4. Encode LSB cipher text with Huffman Chunk coding
5. Input video file as the cover media to transmit
6. Separate frames from cover media
7. Input key file for encoding video process to get security
8. Hide Huffman chunk coding text in each LSB of frames of cover video file, that starts from the initial frame and it will be continued until the message is fully embedded

9. Output the stego video file

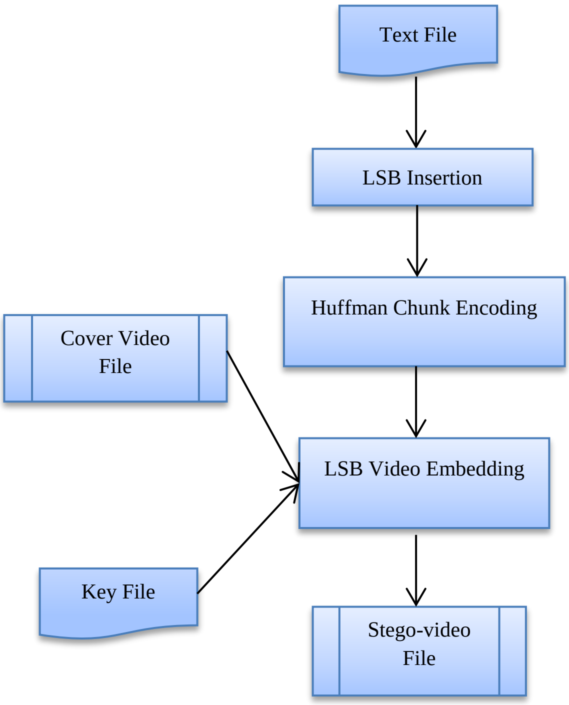


Fig.4. Proposed Blog Diagram for Video encryption at Sender Side

B. Decryption Process at the Receiver Side

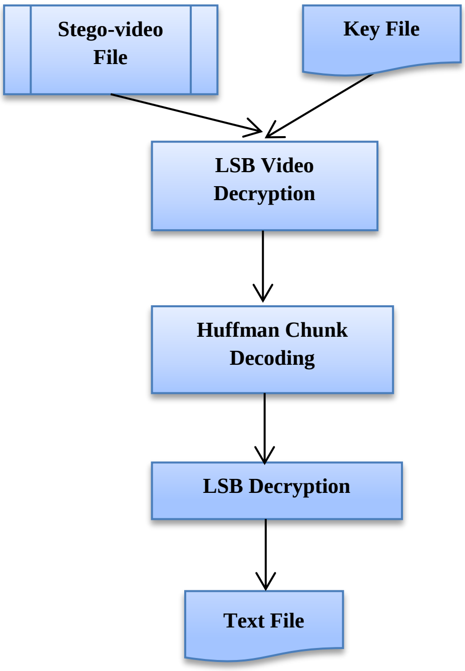


Fig.5. Proposed Blog Diagram for Video decryption at Receiver Side

Fig.5 illustrates the process of proposed video steganography framework at the receiver side. The brief process steps are as follow;

1. Input stego video file to make decryption
2. Enter the private key file that is the agreement with the sender
3. Separate frames of stego video file
4. Decode frames with LSB decryption method to get transmission text
5. Decode receive text with Huffman Chunk coding
6. Decode Huffman recover text with LSB decryption
7. Receive the transmitted text

V. Performance Measure

A. PSNR and MSE

The primary difficulty in video steganography is to handle the visual transparency that is the distortion should be fairly small in the stego video. Visual imperceptibility is also known as the imperceptibility factor that depends on the similarity between the stego carrier image and the original carrier image. A video file is also signified using the authenticity factor also which lies between the resemblance of the extracted secret text and the original secret text. The authenticity factor parameters which lie between the resemblance of the extracted secret text and the original secret text can be computed with the help of the quantitative index such as mean square error (MSE) and peak signal to noise ratio (PSNR). For the video files, the MSE and PSNR values are calculated using the below formulas [20].

$$MSE = \frac{1}{MN}\sum_{n=1}^{M}\sum_{m=1}^{N}[\bar{g}(n,m) - g(n,m)]^2 \quad (1)$$

$$PSNR = -10\ \log_{10}\frac{MSE}{s^2} \quad (2)$$

where $\bar{g}(n,m)$ is the stego carrier image and $g(n,m)$ is the original carrier image. M and N represent the width and height of the image, S is the maximum pixel value.

B. BER

BER, the number of bit errors rate, is the number of decrypted bits of a data stream over a communication channel that has been changed due to noise, interference, distortion or bit synchronization errors. Here, the distortion because of video steganographic technique.

$$BER(w,w') = \frac{100}{N}.\sum_{n=1}^{N} XOR\left(w(n), w'(n)\right) \quad (3)$$

where *w* is desired bit and w' is retrieved bit [21]

VI. Experimental Results

For testing the proposed video steganography algorithm, the four text file and 3 video file s are set up. The detail descriptions of these file are described below in Table 1 and 2. All the movie and text file size are vary to emphasize the detail experimental results.

Table 1. Movie data description

Movie Name	Size (kb)	Frame Size	No: of Frames	Frame Rate	Data Rate (kbps)	Bit Rate (kbps)
Moana.mp4	63.9	300x220	26	30	409	98
Stitch.mp4	172	320x240	54	30	562	131
Brave.mp4	81.2	640x360	27	30	1061	125

Table 2. Text data Description

Text File Name	Size (kb)	No: of Characters
hpa_an1.txt	1.95	2000
hpa_an2.txt	3.90	4000
hpa_an3.txt	5.85	6000
hpa_an4.txt	7.81	8000

Firstly the smallest window size of Moana movie file is tested for all the different text file size and the important factors of the PSNR and MSE of the video steganography technique is calculated and depicted in Table 3. Moreover this paper also concentrates on the bit error rate, so the experiments are carried out for that parameter. But the bit error rates are not changed for the various size of text file.

Table 3. Experimental results for Moana (300x220) video file for various text file size

Text file name	PSNR	MSE	BER for video
1	38.7484	8.65125	37.50
2	38.7601	8.65125	37.50
3	38.78265	8.6066	37.50
4	38.8225	8.52775	37.50

Then the experiments are continued for the rest of the video files of different window size with these same text files. The detail results for important measurements of small frame size 360x240 and big size 640x360 are shown in Table 4 and 5 respectively.

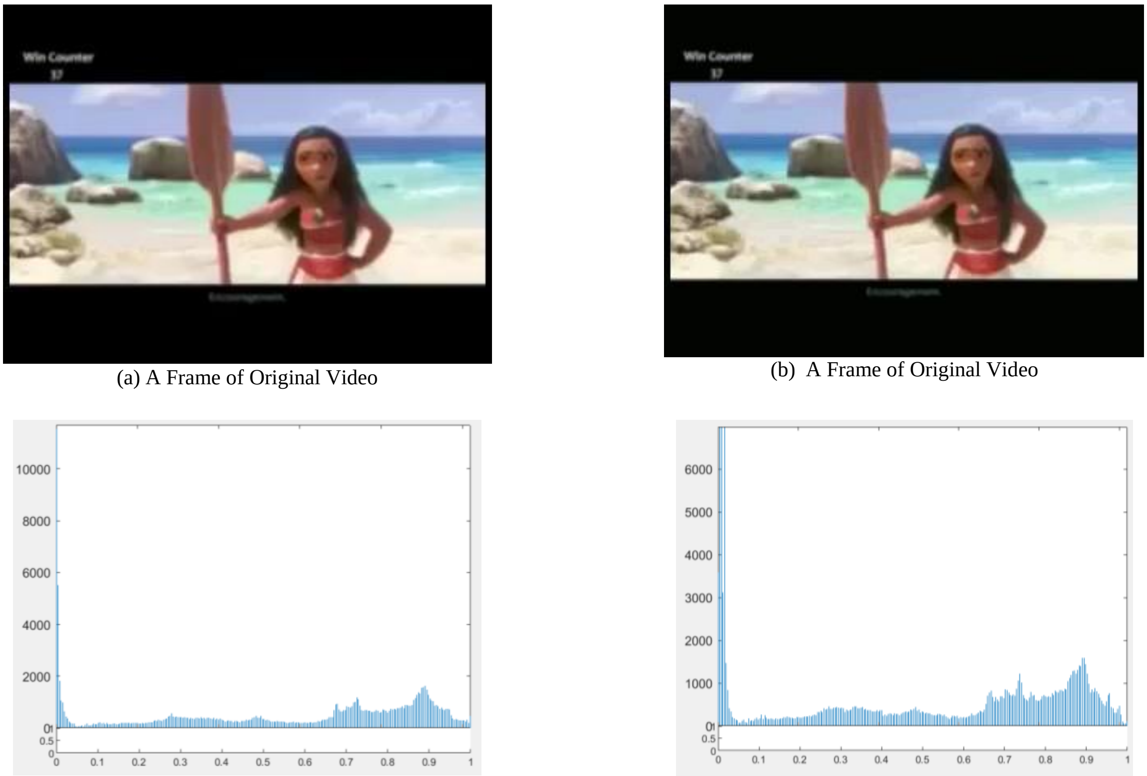
Table 4. Experimental results for Stitch (360x280) video file for various text file size

Text file name	PSNR	MSE	BER for video
1	38.54395	9.1986	37.50
2	38.57605	9.1209	37.50
3	38.60595	9.05975	37.50
4	38.61125	9.05255	37.50

Table 5. Experimental results for Brave (640x360) video file for various text file size

Text file name	PSNR	MSE	BER for video
1	42.0022	4.1007	37.50
2	42.0204	4.0836	37.50
3	42.0294	4.0752	37.50
4	42.0434	4.0620	37.50

The histogram of the original frame and stego frame of the video are selected to compare the human vision distortion as shown in the following figures.



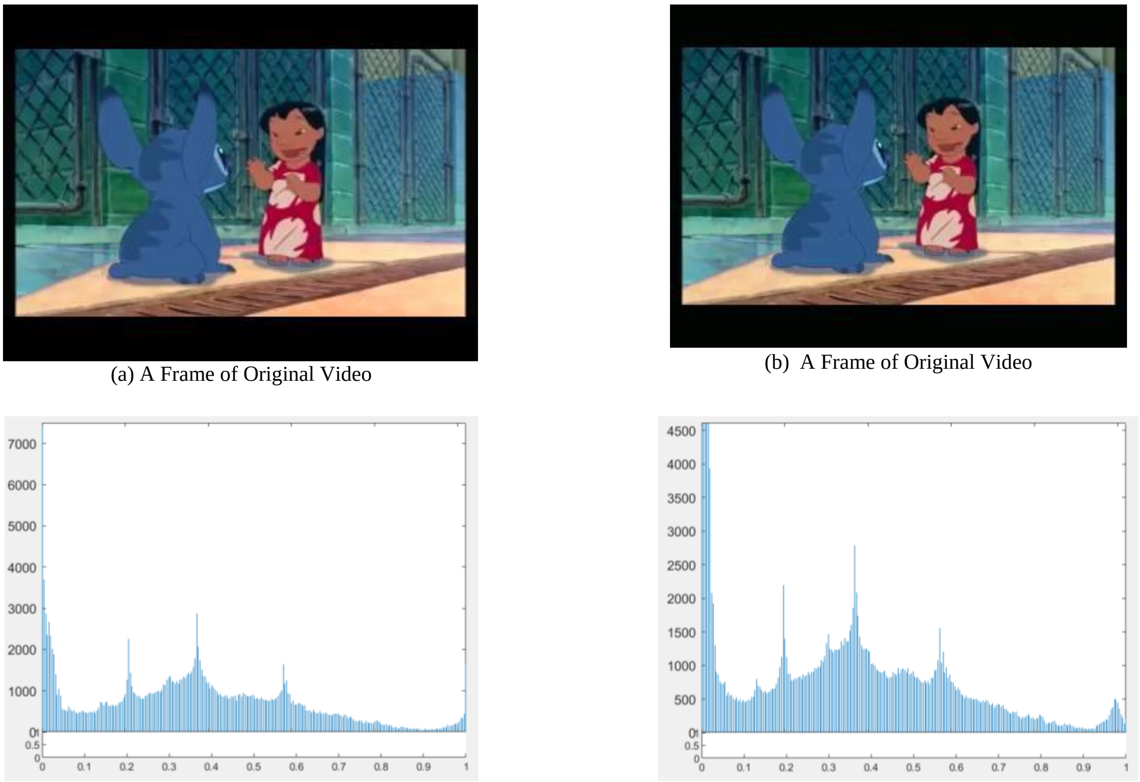
(a) A Frame of Original Video

(b) A Frame of Original Video

(c) Histogram of Original Frame

(d) Histogram of Stego Frame

Fig.6. The selected original frame and stego frame from Moana.mp4 file for the visual comparison in histogram



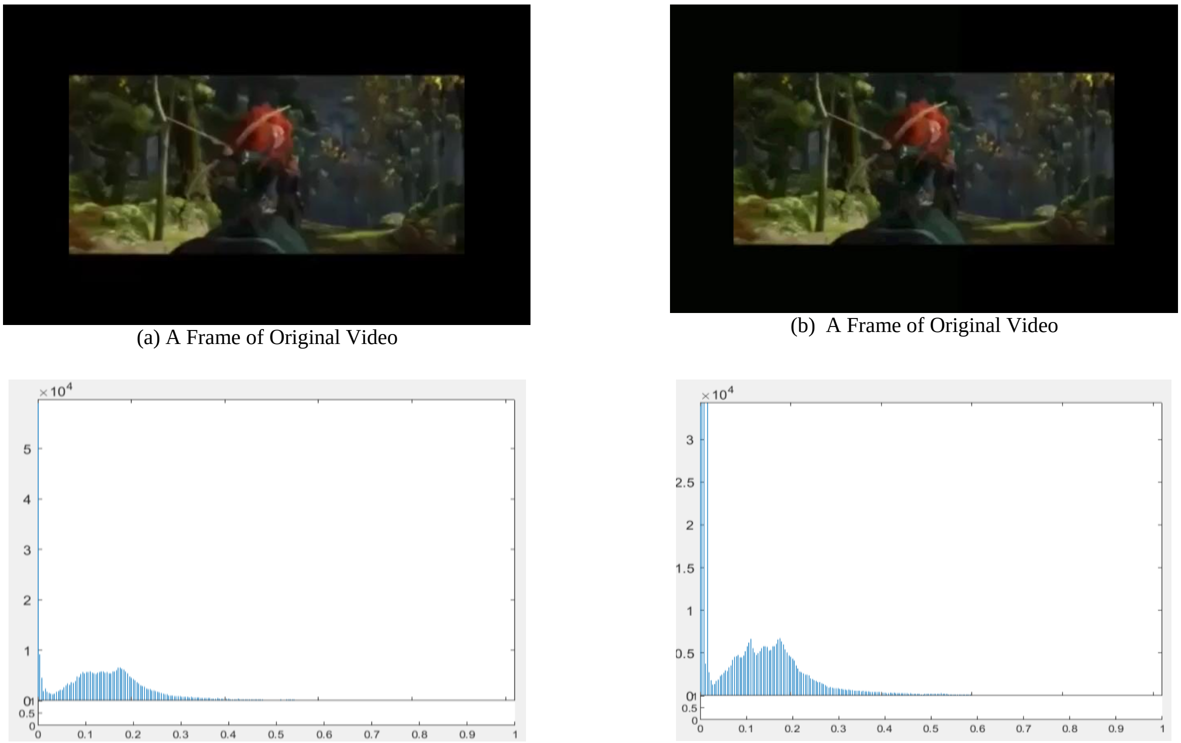
(a) A Frame of Original Video

(b) A Frame of Original Video

(c) Histogram of Original Frame

(d) Histogram of Stego Frame

Fig.7. The selected original frame and stego frame from stitch.mp4 for the visual comparison in histogram



(a) A Frame of Original Video

(b) A Frame of Original Video

(c) Histogram of Original Frame

(d) Histogram of Stego Frame

Fig.8. The selected original frame and stego frame from brave.mp4 for the visual comparison in histogram

A frame is extracted from the original video and histogram of this frame is depicted and shown as the Fig 6, 7 and 8. Then the same frame number is extracted from the stego video frame after embedding with the proposed methods and histogram of that frame is extracted again. The pictures of the histogram results show that there is a little difference between the original and the stego video files, therefore the human can't notice easily there has been a secret message.

VII. Conclusion

This paper proposed a 3 embedding process for mp4 video file to transmission in secure format in open area. From the base of the results, the larger the size of the text to carry, the greater the PSNR value will be get and the BER is no change. The valuable point of this embedding capacity can serve the advantages for the nowadays bit data era. The proposed system has the ability to withstand large embedding capacity without distortion in video quality that is served from the Huffman and LSB technique. The system is consistent, platform independent and the stego video achieved same output file contents as the file input. However, this steganography system needs as the further extension to emphasize to reduce the size of the output stego file. As this system used the mp4 file type as the input to resist the compression and AVI format is used as the stego output to avoid data loss.

References

[1] K. Rajalakshmi and K. Mahesh, "Robust secure video steganography using reversible patch-wise code-based embedding", Springer Science+Business Media, LLC, part of Springer Nature 2018

[2] Mohammed Mahdi Hashim, Mohd Shafry Mohd Rahim, Fadil Abass Johi , Mustafa Sabah Taha, Hassan Salman Hamad, "Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats", International Journal of Engineering & Technology, 3505-3514, 7 (4) (2018)

[3] K. Rajalakshmi and Dr. K. Mahesh, "Video Steganography Based on Embedding THE Video Using PCF Technique", International Conference on Information , Communication & Embedded Systems (ICICES 2017)

[4] Abhinav Thakur, Harbinder Singh and Shikha Sharda, "Different Techniques of Image and Video Steganography: A Review", International Journal of Electronics and Electrical Engineering, Volume-2, Issue-2, 2015

[5] M. Bashardoost, G. B. Sulong, and P. Gerami, "Enhanced LSB image Steganography method by using knight Tour algorithm, Vigenere Encryption and LZW compression", IJCSI International Journal of Computer Science Issues, Vol.10, No.2, pp.221-227, 2013

[6] M. Dixit, N. Bhide, S. Khankhoje, R. Ukarande, "Video Steganography", 2015 International Conference on Pervasive Computing (ICPC -2015), Pune, India, 8-10 January 2015.

[7] Sudeepa K B, Raju K, Ranjan Jumar H S and Ganesh Aithal, "A New Approach for Video Steganography Based on Randomization and Parallelization", International Conference on Information Security and Privacy (ICISP2015), 11-12 December, 2015, Nagpur, India, Procedia Computer Science 78, 483 – 490 (2016)

[8] Anamika Saini, Kamaldeep Joshi, Kirti Sharma and Rainu Nandal, , "An Analysis of LSB Technique in Video Steganography using PSNR and MSE", International Journal of Advanced Research in Computer Science, Volume 8, No. 5, May – June 2017

[9] P. A. S. L. E. Ningsih, G. M. A. Sasmita and N. M. I. M. Mandenni, "MP4 Video Steganography using Least Significant Bit (LSB) Substitution and Advanced Encryption Standard (AES)", Journal of Theoretical and Applied Information Technology, Vol.95. No 21, November 15, 2017.

[10] S. Balu, C. Nelson Kennedy Babu and K. Amudha, "Secure and efficient data transmission by video steganography in medical imaging system", Springer Science+Business Media, LLC, part of Springer Nature 2018.

[11] S. Gosalia, S. Shetty and Revathi A.S, "Embedding Audio inside a Digital Video Using LSB Steganography", 2016 International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi , India, 16-18 March, 2016.

[12] Pooja Yadav1, Nishchol Mishra2, Sanjeev Sharma3, "A Secure Video Steganography with Encryption Based on LSB Technique", 2013 IEEE International Conference on Computational Intelligence and Computing Research, Madurai, India. 26-28 December 2013.

[13] V. K. Jha, S. Roy, S. Mukherjee and G. Sanyal, "Video Steganography technique using Factorization and Spiral LSB methods", 2017 International Conference on Computer, Communications and Electronics (Comptelix), Manipal University Jaipur, Malaviya National Institute of Technology Jaipur & IRISWORLD, July 01-02, 2017

[14] Wa'el Ibrahim A. Al-Mazaydeh, " Image Steganography using LSB and LSB+Huffman Code", International Journal of Computer Applications (0975 – 8887) Volume 99– No.5, August 2014

[15] H. T. Khan, H. Saleem, " Improved Image Steganography Algorithm using Huffman Codes", International Journal of Computer Applications (0975 – 8887) Volume 147 – No.12, August 2016

[16] Li, B., Li, Z., Zhou, S., Tan, S., & Zhang, X. (2018). "New stegoanalytic features for spatial image steganography based on derivative filters and threshold LBP operator". IEEE Transactions on In-formation Forensics and Security, 13(5), 1242-1257. https://doi.org/10.1109/TIFS.2017.2780805.

[17] Zhang, Y., Qin, C., Zhang, W., Liu, F., & Luo, X., "On the fault-tolerant performance for a class of robust image steganography",Signal Processing, 146, 99-111. 8-10 January 2018, https://doi.org/10.1016/j.sigpro.2018.01.011.

[18] S. Mahato, D. A. Khan and D. K. Yadav, "A modified approach to data hiding in Microsoft Word documents by change-tracking technique", Journal of King Saud University – Computer and Information Sciences (2017)

[19] matlab documentation, https://uk.mathworks.com/help/comm/ug/huffman-coding-1.html, last view at July, 2019

[20] R. Singh et al. (eds.), "A Highly Secure Video Steganography Inside DWT Domain Hinged on BCD Codes", Intelligent Communication, Control and Devices, Advances in Intelligent Systems and Computing 624, Springer Nature Singapore Pte Ltd. 2018, https://doi.org/10.1007/978-981-10-5903-2_74

[21] "Bit error rate", https://en.wikipedia.org/wiki/Bit_error_rate, last view at July, 2019

Author's Profile

Shwe Sin Myat Than received the Bachelor of Computer Science (B.C.Sc.) degrees from the Computer University, Hpa-An, Myanmar in 2004. She graduated from Computer University, Thaton, with a Master of Applied Science (M.A.Sc.) in Computer Technology, in 2011. She is interested in Cryptography, Multimedia, Computer Vision and Image Processing. She works as a Lecturer at Faculty of IT Support and Maintenance in University of Computer Studies, Hpa-an, Myanmar.

How to cite this paper: Shwe Sin Myat Than, " Secure Data Transmission in Video Format Based on LSB and Huffman Coding", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.12, No.1, pp. 10-17, 2020.DOI: 10.5815/ijigsp.2020.01.02