Lightweight and Optimized Multi-Layer Data Hiding using Video Steganography Paper

Samar kamil[1], Masri Ayob Authors[2]
CAIT, Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia,
Bangi, Selangor, Malaysia

Siti Norul Huda Sheikh Abdullah[3]
Cyber Security, Faculty of Information Science and Technology
Universiti Kebangsaan Malaysia,
Bangi, Selangor, Malaysia

Zulkifli Ahmad[4]
School of Language Studies and Linguistics, Faculty of Social Sciences and Humanities
Universiti Kebangsaan Malaysia,
Bangi, Selangor, Malaysia

***Abstract*—The ever-escalating attacks on the internet network are due to rapid technological growth. In order to surmount such challenges, multi-layer security algorithms were developed by hybridizing cryptography and steganography techniques. Consequently, the overall memory size became enormous while hybridizing these techniques. On the other side, the least significant bit (LSB) and modified LSB replacing approaches could provide the variability as detected by steganalysis technique, most found to be susceptible to attack too due to numerous reasons. To overcome these issues, in this paper a lightweight and optimized data hiding algorithm is proposed which consume less memory, provide less variability, and robust against histogram attacks. The proposed steganography system was achieved in two stages. First, data was encrypted using lightweight BORON cipher that only consumed less memory as compared to conventional algorithm such as 3DES, AES. Second, the encrypted data was hidden in the complemented or non-complemented form to obtain minimal variability. The performance of the proposed technique was evaluated in terms of avalanche effect, visual quality, embedding capacity and peak signal to noise ratio (PSNR). The results revealed that the lightweight BORON cipher could produce approximate same avalanche effect as the AES algorithm produced. Furthermore, the value of PSNR had shown much improvement in comparison to optimization algorithm GA.**

Keywords*—Video steganography; least significant bit technique; optimized data hiding; cloud computing; boron cipher

I. INTRODUCTION

Nowadays, the internet is the most used medium to access desired information. However, the internet misused activities or cybercrimes such as security breaches [1-19] are also increasing exponentially. In order to overcome these attacks, cryptography and steganography algorithms are used. In cryptography algorithms, secret data are scrambled but the encrypted output stream leaves clues to attackers. On the other hand, steganography algorithms conceal the visibility of secret messages by hiding them in cover media. Unfortunately, this technique could also be compromised by using statistical tests. Therefore, to overcome these issues and to provide multi-layer data security, hybridizing cryptography with steganography algorithms could strengthen data security.

In cryptography algorithm, secret data bits were altered in such a way that only trusted persons who have the key to the file can have access to the data. This technique is classified as private and public. In privateclass, same key is used for encryption and decryption purposes whereas in public class, different keys are used for encryption and decryption procedures [2].

In steganography algorithm, symmetric as well as asymmetric algorithms are gaining more popularity now. The most preferred encryption algorithm for steganography are 3DES, AES, Blowfish, RSA (Rivest, Adi Shamir and Leonard Adleman), and ECC (Elliptic Curve Cryptography) [3-7-20]. These algorithms provide more efficient security but they require large number of resources. Therefore, lightweight ciphers are studied such as BORON cipher [16] for encryption purpose as shown in Table 1. The table is show that the lightweight cipher consume minimum area for s-boxes as compared to other the conventional ciphers but increase the computation time for encryption due to the large number of rounds

TABLE I. COMPARATIVE OF ENCRYPTION ALGORITHM

Algorithm	Block Size (bits)	Key Size (bits)	Number of Rounds	Number of S-boxes
Data Encryption Standard (3DES)	64	3Keys-56	16	4-64 entry S-box
Advanced Encryption Standard (AES)	128	128/192/256	10/12/14	256 Entry S-Box (Each position 8-bit long)
BLOWFISH	64	32-448	16	4-256 entry S-Box
BORON (Lightweight Cipher)	64	80/128	25	16 entry s-box (Each position 4-bit long)

TABLE II. MULTIMEDIA FILES AND THEIR CHARACTERISTICS

Multi-Media Files	Characteristics
Text	Line/Word Shifting Encoding
Protocol	Packet Payload and Packet Header
Audio	Phase Coding, Spread spectrum, Low-Bit Encoding
Image	Image Pixels
Video	Frame and Audio

In steganography, choosing multimedia file for data embedding has played an important role. The multimedia files include text, protocol, audio, image, and the video [3-18]. Various characteristics of these multimedia files have been used for data hiding as shown in Table 2. Images and videos are more popular in comparison to other media because they contain higher number of pixels information and could conceal secret information in a more organized manner. Further, the steganography embedding domain has also an important parameter for data embedding. The embedding domain is classified into spatial and transform domain. In spatial domain, cover media data/pixels are used to conceal information. In transform domain, cover media is changed into other signal/form for data hiding procedure. In this paper, video files and the spatial domain are used for data embedding.

In steganography, LSB and its variant are the most techniques used for data hiding due to its implementation simplicity, low complexity, and high embedding capacity [4-5-17]. The replacement of cover media LSB bits with secret data bits has resolved the visual quality problem. For reduction of variability in cover pixels, a number of techniques such as LSB matching [6-7], optimization technique GA, PSO [8-10-21-22], and optimal position to match with secret data bits [11] have been used in the past

When suitable match is not found, the algorithm hides the secret data in LSB bits. Hence, the visual quality is maintained.

In this paper, lightweight and optimized multi-layer data hiding technique is designed for video steganography. In videos, number of frames are available which improve data hiding capacity and security. The proposed technique is improve visual quality, enhanced security by hiding secret data bits in random frames in less execution time. In this proposed technique, BORON cipher is used for secret data encryption procedure. The encrypted secret data bits incomplemented or non-complemented form are determined and matched with cover frame LSB bits. The matched combination index is determined and based on index information where the encrypted data is decrypted at the receiver side. Next, the proposed technique analysis is conducted to show the security level of the lightweight cipher and the visual quality of frames after the data hidingprocedure. Finally, a counter measure technique is proposed to resolve any issues pertaining to the result of the analysis as defined in table 3.

TABLE III. ISSUES AND COUNTER MEASURE

Issues	Counter Measure
Multi-layer security algorithms are increased overall area.	Preferred Lightweight Cipher which consume less area
Steganography LSB replacing techniques is provide maximum variability and easy to break.	Optimized data hiding is done in complemented or non-complement form.

The rest of the paper is organized as follow: Section II defined related works regarding secret data encryption and optimized data hiding techniques. Section III illustrates the proposed technique in details. Section IV presents the experimental results and Section V states the conclusion of the work.

II. RELATED WORK

In this section, the cryptography algorithms, spatial domain and optimal match data hiding techniques are studied.

Yadav, et al. [19] used a key named XOR operation for data encryption. Next, they used sequential encoding and LSB techniques for data embedding and data hiding subsequently. Even though the encryption process required less time as compared to 3DES, AES and Blowfish but it is still considered relatively easy to break. **Apau, *et al.* [6],** designed multilayer security in spatial domain using RSA, Huffman coding, and LSB technique. In their work, secret data are encrypted using asymmetric algorithm namely RSA. Firstly, the data are compressed using lossless technique specifically Huffman code. Next, Huffman code compression lossless technique provides cover data size reduction without causing any data loss. Finally, the secret data are then hidden using LSB technique. Although RSA algorithm provides effective encryption as well as authentication, its security are dependent on large key size thus and consumes huge amount of time for encryption process. **Ramakrishna Hedge and Jagadeesha S [7],** employed ECC and optimization in their work. Their method uses data encryption via ECC (Elliptic Curve Cryptography) algorithm and its data embedment is in the form of H.264 videos. They deployed artificial bee colony (ABC) algorithm to reduce variability and to find the best position in the data embedding procedure. They also took advantage of ECC technique due to its smaller key size and less storage requirement. Hence, the technique succeeds in improving overall processing speed for data encryption. **Mstafa, et al. [5]** improve embedding capacity and robustness of security system against attacks by hybridizing spatial domain of various LSB techniques (1-bit, 2-bit, 3-bit, 4-bit LSB) with hamming codes (15, 11). In their experimental setup, they have four stages. In the first stage, secret messages are pre-processed using hamming algorithm. In the second stage, Region-of-Interest (ROI) is detected from the cover videos for data embedding procedure. In the third stage, data embedding is performed using various LSB techniques. In the fourth stage, data extraction from stego video is achieved. Their result shows that they have high embedding capacity and enhanced visual quality.

In order to reduce variability, Mielikanien [6] used LSB matching technique for data hiding. In LSB matching technique, if secret bits do not match with the cover bits, then ± 1 is randomly added in the corresponding pixels. The LSB match technique provides better visual quality and similar embedding capacity as compared to LSB replacement technique. However, the LSB matching technique deals with given pixel/pixel pair without considering the difference between the pixel and its neighbour [7]. Dasgupta et al. [8] split the data bits into 3:3:2 ratio to improve embedding capacity and create less variability as compared to other ratio. They used genetic algorithm to search optimal position in video steganography. Moreover, they used optimization algorithms such as GA [9] and PSO [10] to find optimal matches for data embedding procedure. However, these algorithms search optimal matches in cover pixels using a number of iterations that cause an increase in computational time. Next, [11], used a technique which search cover pixel bits 0 to 7 to find optimal matches for secret data bits. When optimal matches are found, the index position will be determined. Otherwise, the data bits will be hidden in the LSB position. The secret data bits and index information are hidden in the stego media. The index position varies 0 to 7 and 3 bits of pixel is used to hide the index information and to provide high variability (maximum variability $2^3=8$). In order to reduce variability, in which data is embedding in complemented or non-complemented form provide zero variability for embedding secret data. Further, hide to their index only 2 bits are required which provide maximum variability $2^2=4$.

Their contribution for data encryption preferred 3DES, AES, Blowfish, RSA, and ECC algorithms. Even though, these algorithms provide efficient security, they consume large number of resources in terms of memory space. In order to overcome these issues, lightweight ciphers are introduced to provide the same level of security and consume less memory space. On the other hand, techniques that use optimal match search do provide better visual quality but they increase the computational time, index information bits, and unable to distinguish the difference between pixels and its neighbours [6, 8-10,18].

Therefore, in this paper after considering all these parameters and issues, proposed complemented or non-complemented form technique for data hiding procedure. This data hiding procedure embeds the secret data in the LSB bits of the pixel either in complemented or non-complemented form. It provides zero variability, high embedding capacity and enhanced security level.

III. Proposed Technique

In this section, the proposed technique block diagrams and its components are explained. The block diagram of data hiding technique is shown in Fig 1.

The secret data is encrypted using BORON cipher. Next, the video frames, encrypted secret data, and Look-up Table are input parameters for data hiding procedure. The Look-up Table shows the number of times taken to determine complemented or non-complemented secret data to find complete matches with cover pixel bits. In this proposed technique, about half of the frame contains encrypted secret data and another half contained index information which counts the number of times to achieve the complemented form of data bits.

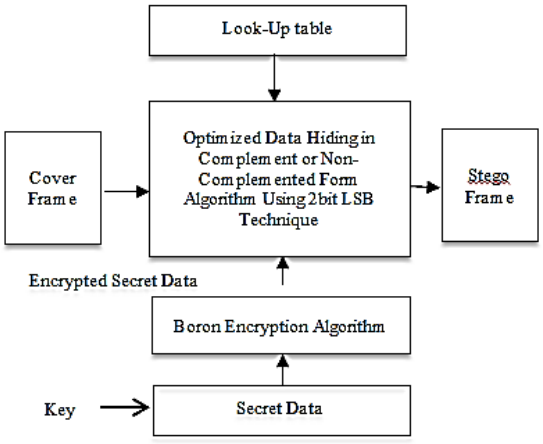


Fig. 1. Block Diagram for Data Hiding Technique.

The extraction process block diagram is in Fig. 2. In the extraction process, the Stego Frame and Look-up Table (index information regarding complemented or non- complemented data bits to the cover bits) serve as inputs to the Data Extraction algorithm. The Data Extraction algorithm will then extract original Secret Data. The detail description of block diagram components is explained below.

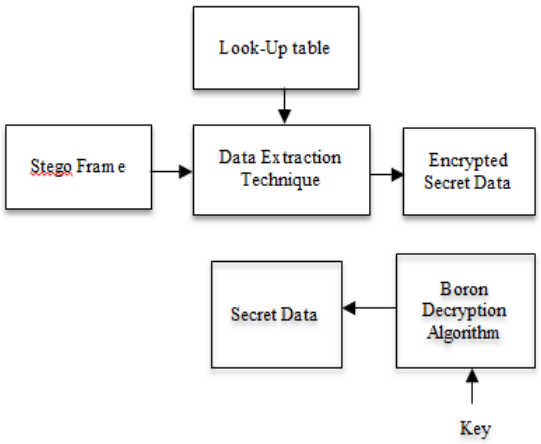


Fig. 2. Block Diagram for Data Extraction.

A. Secret Message Encryption using Lightweight Boron Cipher

The BORON cipher is a lightweight block cipher. It is based on substitution-permutation network. This cipher has 64-bit block size, two key variant of size 80 and 128 bit, and total 25 rounds [16]. The lightweight algorithm has block size 64 bit and process in 4-bit chunk. Therefore, 24 = 16 is the combination required in the s-box. On the other side, In the conventional technique, the block size is 128 bit and process the data in 8-bit and 28= 256 combination is required in the s-box implementation which increase memory requirement. The encryption pseudo code for the BORON cipher is explained in Figure 3.

Encryption Algorithm
For m is 0 to 24 rounds
{XOR Operation(State, Key)
S-Box Layer(State)
Block Shuffle(State)
Left Circular Shift (State)
XOR Operation (state)
Key Scheduling (Key)}
XOR Operation (State, Key)

Key Scheduling Algorithm
For 80-bit Key
Left Circular shift(Key, 13)
S-Box Layer(Key_{0-3})
XOR Operation ($Key_{63-59}, Round\_Counter$)
For 128-bit Key
Left Circular shift(Key, 13)
S-Box Layer(Key_{0-7})
XOR Operation ($Key_{63-59}, Round\_Counter$)

Fig. 3. Pseudo-Code for BORON Cipher.

Furthermore, the lightweight Boron cipher has large number of rounds such as 25 as compared to AES which has 10 rounds for encryption. Therefore, the time required to encrypt data using BORON cipher is higher than AES. To improve the computational time of encryption to the algorithm, optimization algorithms such as loop-unrolling is preferred [16].

B. Encrypted Secret Message Complemented or Non-Complemented Form

The encrypted secret message pixels are broken into 2-bit using logical operations. The encrypted secret bits complemented or non-complemented matrix is formed as shown in Table 4. Table 4 shows that indexes are defined according to the number of times taken to form complements. For example, the 0th index shows no complement is taken, 1st index shows first bit of the encrypted secret bit is complemented. In the 2nd index, the second bit of the encrypted secret bit is complemented. In the 3rd index, both of the encrypted secret bits are complemented.

TABLE IV. LOOKUP TABLE

0th Index	**1st Index**	**2nd Index**	**3rd Index**
00	01	10	11
01	00	11	10
10	11	00	01
11	10	01	00

TABLE V. DATA HIDING TECHNIQUE

Cover Pixels	10010100	11110000	11001100	10010001
Stego Pixels	10010100	11110000	11001100	10010001
Index	2	1	2	1

C. Optimized Data Hiding of Encrypted Data

For the optimized data hiding, LSB 2 bits of the cover pixel are extracted and compared with the encrypted secret bits. The index information determines where the encrypted secret bits matches with cover bits are shown in Table 5

For example

The encrypted data bits: 10 01 10 00

The 10 pixels of the encrypted secret bit is compared with cover pixel bit 00. Based on the matches bits in the Look-up Table, index 2 is stored and zero variability in stego pixels.

In figure 4 the algorithm for the proposed technique is given

Transmitter Side
1.Read the video and extract the frames.
2. Read the secret data, key and encryption using BORON Cipher.
3. Read the encrypted secret messages and divide them into chunks. Each chunk size is 2bit.
4. For data embedding, the cover 2 LSB bits are compared to the encrypted secret 2 bits which are based on the Look-up Table the matches are found an index values are determined.
5. The indexes are hidden in the cover frame using 2 bit LSB technique.
6. The performance analysis is conducted using various parameters such as embedding capacity, PSNR, SM, BER.
7. The stego frames are combined together to form stego video.
Receiver Side
1. Read the stego video and extract the frames.
2. Determine pixels in which indexed bits are hidden.
3. The index information is compared with stego 2 LSB bits and is based on the Look-up Table matches to determine encrypted secret messages.
4. The encrypted secret messages and key input to BORON decryption module enable the retrievement of the secret messages.

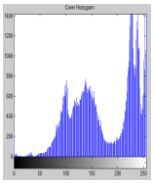
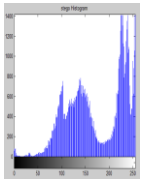
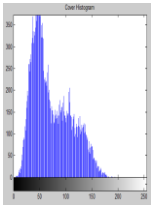
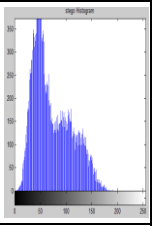
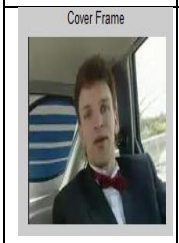
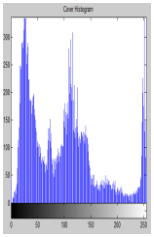
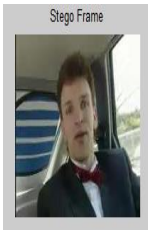
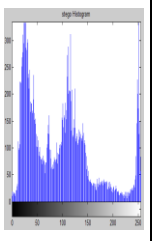
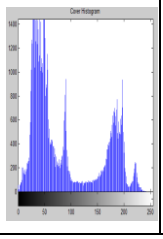
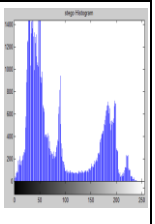
Fig. 4. Algorithm for the Proposed Technique.

IV. EXPERIMENTAL RESULTS

In the experimental setup, various video sequences which includes: Foreman (352×288), Salesman, Car Phone 176×144) and an akiyo video (352×264) are taken [12]. The MATLAB version 8.1.0.604 (R2013a) is used for coding purposes. In Table 6, first frames of all the videos, visual effect between the cover and stego frames are shown after performing the data hiding process. The results show that the histogram looked similar between the cover and stego frames

The performance analysis of the proposed technique is done based on parameters avalanche effect, invisibility, embedding capacity, and robustness against attacks. The parameters are explained below:

TABLE VI. VISUAL COMPARATIVE ANALYSIS BETWEEN COVER AND STEGO FRAME

Cover Frame	Cover Histogram	Stego Frame	Stego Histogram
			
			
			
			

1) Avalanche effect: This parameter is defined the strength of the encryption algorithm. In the ideal scenario, 50% change in the ciphertext required while changing in the one bit of the key. For the BORON cipher, on standard dataset test vector avalanche effect is determined using equation (1) and found that it is provides 50% as shown in table 7.

$$Avalanche\ Effect = \frac{Number\ of\ bits\ Changed}{Block\ Size} \quad (1)$$

TABLE VII. AVALANCHE EFFECT

Plaintext (In Hex Value)	Key	Number of bits changed
0000 0000 0000 0000	0000 0000 0000 0000 0000	32
	0001 0000 0000 00 0	

2) Embedding capacity: The embedding capacity depends on how much information bits are embedded in the cover frame [13]. It is calculated using equation (2)

$$EC = \frac{Total\ Number\ of\ Bits\ Embedded}{Size\ of\ the\ Cover\ Frame}(\text{bpp}) \quad (2)$$

Here, bpp represents bits per pixel

A. Peak Signal to Noise Ratio (PSNR)

The invisibility of the proposed technique is measured based on the visual quality. The PSNR parameter is used to measure the distortion in stego frame after data embedding [14]. The decibel unit is used to measure PSNR. It is calculated by using equation (3-4).

$$PSNR = 10 \times \log_{10} \frac{255 \times 255}{MSE} \quad (3)$$

Here,

$$MSE = \frac{1}{J \times K} \sum_{m=1}^{J} \sum_{n=1}^{K} (X_{m,n} - Y_{m,n})^2 \quad (4)$$

Here, J, and K defines as the row and column of the frame. The X and Y represent the cover and stego frame.

B. Normalized Cross-Correlation (NCC)

The closeness or similarity between cover and stego frame is determined using this parameter. The value lies between -1 to 1. In the ideal case, NCC value 1 is required. It is measured using equation (5)

$$NCC = \frac{\sum_{J=1}^{M} \sum_{K=1}^{N} C(J,K) \times S(J,K)}{\sum_{J=1}^{M} \sum_{K=1}^{N} C(J,K)^2} \quad (5)$$

3) Average difference: This parameter is given an actual difference between cover and stego frames as mentioned in equation (6)

$$verage\ Difference = \sum_{m=1}^{J} \sum_{n=1}^{K} \frac{(C(i,j) - S(i,j))}{JXK} \quad (6)$$

Here, J and K represent the row and column of the frame. The average difference varies in the interval from -255 to 255.

4) Maximum difference (MD): The maximum difference parameter measures the magnitude difference between cover and stego frame. Its value varies from 0 to 255 and determined using equation (7).

$$MD = Max|(C(J,K) - S(J,K))| \quad (7)$$

Here, C and S represented the cover and stego frame. J and K total number of rows and column.

5) Normalized absolute error (NAE): This parameter is measured by the absolute error between cover and stego frames. It is determined using equation (8).

$$NAE = \frac{\sum_{J=1}^{M} \sum_{K=1}^{N} |C(J,K) - S(J,K)|}{\sum_{J=1}^{M} \sum_{K=1}^{N} |S(J,K)|} \quad (8)$$

The performance analysis for the propsed technique is show in table 8

6) Similarity index measure (SIM): The similarity index measure (SIM) parameter is used to evaluate the performance of the proposed technique by determining how much information has been extracted after attacking process [15] as mentioned in equation (9).

$$IM = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} J(i,j) K(i,j)}{\sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} J^2(i,j)} \sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} K^2(i,j)}} \quad (9)$$

TABLE VIII. PERFORMANCE ANALYSIS FOR THE PROPOSED TECHNIQUE

Parameters	Videos			
	Foreman	Salesman	Carphone	Akiyo
Embedding Capacity	1	1	1	1
$PSNR_{Average}$(dB)	50.18	50.19	50.24	50.22
Normalized Cross Correlation	0.999	0.999	0.996	1
Average Difference	0.31	0.31	0.30	0.31
Maximum Difference	3	3	3	3
Normalized Absolute Error	$1.78X10^{-3}$	$4.24X10^{-3}$	$3.15X10^{-3}$	$3.54X10^{-3}$

7) The bit error rate (BER): BER is used to measure how much bits are changing between original and extracted secret message after attacking process. Below is the respective equation (10),

$$BER = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} J(i,j) \oplus K(i,j)}{M \times N} X100\% \quad (10)$$

Here, J and K represent the original and extracted secret message and M and N represent the size of the secret message.

In the ideal scenario, SIM 1 and BER 0 are required. The various attacks on the proposed technique for video 1 is shown in Table 9. The table shows that SIM and BER are acceptable for salt & pepper attack and highly influenced for other attacks.

TABLE IX. VARIOUS ATTACK ON THE PROPOSED TECHNIQUE

Attacks	SIM	BER%
Salt & Pepper attack (D=0.1)	0.954	76
Median Filtering	0.834	341
Sharpening	0.816	395
Histogram Equalization	0.78	392
Gaussian attack (mean=0, Variance=0.1)	0.82	402

V. COMPARATIVE ANALYSIS WITH EXISTING TECHNIQUE

The video frames are basically a collection of the images. Also, in the literature number of optimization algorithm results available for the images. Therefore, the proposed technique is run on standard dataset images and compared with existing technique which prefer GA algorithm for optimized datahiding [11]. The most preferred performance parameters such as PSNR and embedding capacity are determined and compared in table (10-12). The proposed technique has better embedding capacity and approximate same PSNR as compared to existing techniques. Because, the index in the proposed technique for searching optimal combination varies from 0 to 4(00 to 11) where in the existing techniques such as GA the index position varies from 0 to 7 for searching optimal position. If matches are not found then the data will be hidden in the LSB.

TABLE X. COMPARISON OF THE PROPOSED TECHNIQUE WITH EXISTING TECHNIQUE BASED ON PSNR VALUE

Cover Image (.jpg)	Shah, P.D. and Bichkar [11] PSNR (dB)	Proposed Technique PSNR (dB)
Baboon	54.43	50.21
Lena	52.33	50.62
Barbara	53.80	50.25
Cameraman	52.36	50.01

TABLE XI. COMPARISON OF THE PROPOSED TECHNIQUE WITH EXISTING TECHNIQUE BASED ON EMBEDDING CAPACITY

Parameter	Shah, P.D. and Bichkar [11]	Proposed Technique
Embedding Capacity for Secret Message	Quarter part of the cover image	half part of the cover image

TABLE XII. T-TEST: PAIRED TWO SAMPLE FOR MEANS FOR THE PROPOSED AND SHAH & BICHKAR [11] TECHNIQUES

Parameters	Shah & Bichkar[11]	Proposed Method
Mean	53.23	50.27
Variance	1.11	0.065
P(T<=t) one-tail	0.001	
P(T<=t) two-tail	0.013	

Referring to Table 12, we assume that null hypothesis is no significant difference between the proposed and Shah & Bichkar [11] methods. Since the p – value of both one (0.001) and two tail (0.13) are less than ($p<0.05$), we reject the null hypothesis and conclude that there is a significant difference between the proposed and Shah & Bichkar [11] methods

VI. CONCLUSION

In this paper, a multi-layer data hiding technique is proposed for video steganography. The videos have large number of frames which improve embedding capacity and security. In the multi-layer data hiding techniques, conventional encryption algorithms are used for data encryption which consumes large memory for data encryption. To overcome this issue, lightweight algorithms are studied which consume less memory but influence on the computation time. To reduce computation time software optimization technique loop-unrolling is used. Furthermore, optimal match techniques increase computational time and provide small variability when optimal matches are not found. In order to overcome this issue complemented or non-complemented technique is proposed which provide less computational time and zero variability for secret data. The proposed technique is applied on standard dataset videos and is found to perform better in terms of avalanche effect, PSNR, Embedding Capacity, Normalized Cross Correlation, Average Difference, Maximum Difference, Normalized Absolute Error. In addition, from the analysis of SIM and BER, the spatial domain is found to be highly influenced by noise. Hence, in the future, the proposed technique is hybridized with error correction code. Furthermore, the comparative analysis shows that the proposed technique is much better in comparison to

existing techniques [11]. In the future, to improve the robustness of proposed technique, the technique is hybrid with error correction codes.

ACKNOWLEDGMENT

This work was supported by UniversitiKebangsaan Malaysia grant Dana Impak Perdana (DIP-2014-039) and AP 2017-005/2 for supporting this project.

REFERENCES

[1] Sebastian Neuner, Artemios G. Voyiatzis, Martin Schmiedecker, Stefan Brunthaler, Stefan Katzenbeisser, and Edgar R. Weippl, "Time is on my side: Steganography in filesystem media," *Digital Investigation*, vol. 18, pp.576-586, 2016.

[2] Mamta Jain, Saroj Kumar Lenka, Sunil Kumar Vsistha, "Adaptive circular queue image steganography with RSA crypto-system," *Perspective in Science*, vol. 8, pp. 417-420, 2016.

[3] Mehdi Hussain, Ainuddin Wahid Abdul Wahab, Yamani Idna Bin Idris, "Image Steganography in spatial domain: A survey," *Signal Processing: Image Communication*, vol. 65, pp. 46-66, 2018.

[4] Khan Muhammad, Jamil Ahmad, Seungmin Rho, Sung Wook Baik, "Image Steganography for authenticity of visual contents in social networks," *Multimedia Tools and Application*, vol. 76, pp. 18985-19004, 2017.

[5] Mstafa, Ramadhan J., and Khaled M. Elleithy "A video steganography algorithm based on Kanade Lucas Tomasi Tracking algorithm and error correcting codes," *Multimedia Tools and Application*, vol. 75, pp. 10311-10333, 2016.

[6] J. Mielikainen, "LSB matching revisited," *IEEE signal processing letter*, vol. 13, issue 5, 2006.

[7] Luo, W., Huang, F. and Huang, J., "Edge adaptive image steganography based on LSB matching revisited," *IEEE transactions on information forensics and security*, vol.5, issue 2, pp.201-214, 2010.

[8] Dasgupta, K., Mondal, J.K. and Dutta, P., "Optimized video steganography using genetic algorithm (GA)". *Procedia Technology*, vol. 10, pp.131-137, 2013.

[9] Wang, S., Yang, B. and Niu, X., "A secure steganography method based on genetic algorithm," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, issue 1, pp.28-35, 2010.

[10] Li, X. and Wang, J.,"A steganographic method based upon JPEG and particle swarm optimization algorithm," *Information Sciences*, vol. 177, issue 15, pp.3099-3109, 2007.

[11] Shah, P.D. and Bichkar, R.S., "A Secure Spatial Domain Image Steganography Using Genetic Algorithm and Linear Congruential Generator" *In International Conference on Intelligent Computing and Applications*, pp. 119-129. Springer, Singapore, 2018.

[12] http://trace.eas.asu.edu/yuv/index.html

[13] Sadek, M.M., Khalifa, A.S. and Mostafa, M.G., "Robust video steganography algorithm using adaptive skin-tone detection," *Multimedia Tools and Applications*, vol. 76, issue 2, pp.3065-3085, 2017.

[14] Kumar, V. and Kumar, D., "A modified DWT-based image steganography techniques", *Multimedia Tools and Applications*, vol. 77, issue 11, pp.130279-130308, 2017.

[15] He Yingliang, Yang Gaobo, Zhu Ningbo, "A real-time dual watermarking algorithm of H.264/AVC video stream for Video-on-Demand service," *International Journal of Electronics and Communication*, vol. 66, pp. 305-312, 2012.

[16] Bansod, Gaurav, Narayan Pisharoty, and Abhijit Patil, 'BORON : An Ultra-Lightweight and Low Power Encryption Design for Pervasive Computing', Frontier of Information Technology & Electronic Engineering, 18 (2017), 317–31

[17] Majeed, Mohammed Abdul, and Rossilawati Sulaiman, "An Improved Lsb Image Steganography Technique Using Bit-Inverse In 24 Bit Colour," Journal of Theortical and Applied Information Technology, 2016

[18] Ali, Ahmed Hussain, Mohd Rosmadi Mokhtar, And Loay E George, "Enhancing The Hiding Capacity Of Audio Steganography Based On Block Mapping Enhancing The Hiding Capacity Of Audio," Journal of Theoretical & Applied Information Technology, vol.95, no.7, 2017.

[19] Ali, Ahmed Hussain, And Loayedwar George, "A Review On Audio Steganography Techniques," Research Journal of Applied Sciences, Engineering and Technology, vol.12, No. 2, pp. 154-162. 2016

[20] Othman, I O R, And Tructure In, "Key Exchange In Elliptic Curve Cryptography Based On The Decomposition Problem," Sains Malaysiana, vol. 41, pp. 907–10, 2012.

[21] Hussein, Wasim Abdulqawi, And Shahnorbanun Sahran, 'An Improved Bees Algorithm For Real Parameter Optimization', Int J Adv Comput Sci Appl, vol. 6, pp. 23-39, 2015.

[22] Abdul, Rafidah, Aziz Masri, Ayob Zalinda, Othman Zulkifli, And Nasser R Sabar, 'An Adaptive Guided Variable Neighborhood Search Based On Honey-Bee Mating Optimization Algorithm For The Course Timetabling Problem', Soft Computing, 2016.