http://www.ftsm.ukm.my/apjitm
Asia-Pacific Journal of Information Technology and Multimedia
Jurnal Teknologi Maklumat dan Multimedia Asia-Pasifik
Vol. 7 No. 2-2, December 2018: 53 – 62
e-ISSN: 2289-2192

CHALLENGES IN MULTI-LAYER DATA SECURITY FOR VIDEO STEGANOGRAPHY REVISITED

SAMAR KAMIL
MASRI AYOB
SITI NORUL HUDA SHEIKHABDULLAH
ZULKIFLI AHMAD

ABSTRACT

The steganography is prone to number of attacks such as geomatical, salt & pepper, gaussian, median filtering, attacks. To overcome these problems, the cryptography and error correction codes are comes in the pictures and hybrid with steganography algorithms. The cryptography algorithms add one layer of security on steganography algorithms and error correction codes improves the robustness of steganography algorithms. On the other side, the hybridization of the algorithms, increase memory complexity and increase computation time for data embedding. Thus, in this paper a review on multi-layer algorithms for video steganography is done. This paper comprehensively reviews the steganography, spatial and frequency domain techniques hybrid with cryptography and error correction techniques. In-depth analysis on published literatures revealed that the spatial domain techniques require shorter computation time for data embedding and provide higher data hiding capacity than frequency domain methods. Performance of such techniques was evaluated in terms of visual quality and robustness parameters. Present challenges and future trends towards the improvement of the multi-layer data security in video steganography are discussed to provide the taxonomy for further navigation.

Keywords**:** cryptography, error correction codes, video steganography, data hiding, Security.

INTRODUCTION

Presently, internet is the most exploited means to access the desired information from anywhere on the globe where vast amount of sensitive and private data can be exchanged freely and instantly. However, an exponential escalation in the internet maltreatments or cybercrime including adversaries' attacks, unauthorized access, and security threats became the major challenges to the internet provider towards secured data transmission (Bharathi, & Kiran, 2017). To surmount such defy, cryptography and steganography algorithms have been introduced. The cryptography algorithms scramble the data and the resultant encrypted output stream preserves the data security against possible attacks. The cryptography algorithms security is dependent on number of parameters such as algorithm structure, number of rounds. These parameters optimization will required for improving the performance of cryptography algorithms. Conversely, the steganography algorithms that hide the visibility of sensitive data within the cover media are easy to break using statistical tools (such as neighbor pixel analysis, histogram analysis). To overcome these limitations and to provide multi-layer data security, unification in the cryptography and steganography algorithms have been proposed. Meanwhile, the error correction code (ECC) has been hybridized with steganography algorithm to achieve a multi-layer data security system robust against varied attacks and noise factor.

Figure 1 presents the block diagram of a typical complete multi-layer security system, wherein the original data is first read and then encrypted using cryptography algorithms to generate the cipher data. Next, the cipher data is processed using ECC. Simultaneously, the cover video is read, and its frames/audio is extracted. Finally, various steganography techniques are applied on the frames/audio to generate the stego-video at the transmitting end. Despite much research an accurate and robust video steganography technique effective for multi-layer data security is far from being achieved.

In this view, this paper presents communication assesses the performance of various state-of-the-art techniques used in video steganography, cryptography, ECC, and data hiding domains. Further, a detailed analysis disclosed that spatial domain techniques provide higher capacity with less computational complexity for data hiding compared to frequency domain systems, but more susceptible to attack such as geometrical attacks (rotation, cropping, equalization, compression). Next, the most preferred performance parameters in steganography are evaluated. In the last, based on the literature survey future research directions are defined.

This paper is organized as follows: Section 2 reviews the relevant literatures related to cryptography, ECC, and steganography. Section 3 emphasizes diverse multi-layer data security algorithms. Section 4 analyzes the performance of these techniques in terms of diverse parameters. Section 5 concludes the paper with future trends in cryptography, ECC, and video steganography for privacy preserved data communication in cloud computing.

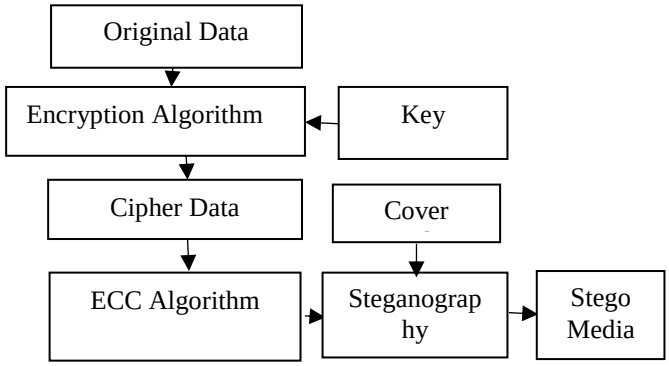

FIGURE 1. Schematic Diagram Displaying The Typical Architecture Of Multi-Layer Data Security System.

RELATED WORK

This section briefly describes the salient features of cryptography, error correction codes, and video steganography prior to extensive understanding on the area of multi-layer data security.

CRYPTOGRAPHY ALGORITHMS

The purpose of cryptography algorithms is to alter the data in such a way only the trusted users having access of the keys can read the transmitted data. The cryptography techniques are classified into private and public. Private cryptography uses the same key for encryption and decryption processes. Conversely, public cryptography uses different keys for encryption and decryption processes (Shim, 2016). Of late, symmetric and asymmetric algorithms in steganography became popular. For steganography the most preferred encryption approaches are triple data encryption standard (3DES), advanced encryption standard (AES introduced by NIST), Blowfish, RSA (Rivest, Adi Shamir and Leonard Adleman), and ELCC (Elliptic Curve Cryptography) (Padmavathi, & Kumari, 2013). Table 1 depicts the comparative analyses of varied symmetric block ciphers. The DES cipher being substitution permutation

network based was proposed in the initial phase of encryption however it can easily be broken owing to small key size. Thus, its variant 3DES was proposed which used 3 keys. Meanwhile, the Rijndael encryption algorithm exhibited best security performance because of large block size with three key variants which has been applied in e-commerce and mobile network. Blowfish algorithm is Feistel network based and has the same structure for encryption/decryption purposes with reduced hardware sizes. Furthermore, large s-boxes mediated high memory consumption limits the applications of Blowfish algorithm despite its robust security and high efficiency.

TABLE 1. Comparative Analysis of Symmetric Encryption Algorithms.

Algorithm	Block Size (bits)	Key Size (bits)	Number of Rounds	Number of S-boxes
3DES	64	3 Keys-56	16	4-64 entry S-box
AES	128	128/192/256	10/12/14	256 Entry S-Box
Blowfish	64	32-448	16	4-256 entry S-Box

Table 2 outlines the comparative analyses of diverse asymmetric block ciphers. Despite the requirement of large key size and prolonged computation time the RSA cipher has widely been implemented due to its simple operations (mathematics based on factorization). Elliptic Curve Cryptography key encryption technique has been gaining momentum due to shorter computation time, smaller key size, and comparable security level to other approaches (Hegde, & Jagadeesha, 2016).

TABLE 2. Comparative Analysis of Asymmetric Encryption Algorithms.

Algorithm	Mathematics	Key Size	Complexity	Applications
RSA	Factorization based	1024/2048/3072 /7680/15360	High	Encryption/Authentication
ELCC	Elliptic Curve based	160/224/256 /384/521	Low as compared to RSA	Encryption/Authentication /To create secure channel

ERROR CORRECTION CODES

Generally, error correction codes are applied on the cipher data to make it robust against any attacks. In ECC, parity bits are added with data bits to correct the errors at the receiver side. Hamming code and BCH (Bose, Chaudhuri, and Hocquenghem) code are the most referred steganography processes (Mstafa, & Elleithy, 2016). Table 3 presents the comparative analyses of various error correction codes.

TABLE 3. Comparative Analysis of Various Error Correction Codes.

Algorithm	Description	Advantages	Disadvantages
Hamming Code BCH	Hamming codes and BCH codes add some extra redundant bits known as parity bits with data bits to recover original data bits in the noisy or attack environment	Simple operations Correct Multiple bit Error	Detect and correct single bit error Degree of complexity of BCH code is higher than Hamming codes

In steganography, sensitive data is embedded in cover media to make it imperceptible. Such cover formats include text, image, audio, and video files. Amongst all, image is the most widely used cover format for data hiding because it contains large number of pixels with minimal visual impact. Lately, the concept of cover media in video steganography became prospective due to its improved data hiding capacity and enhanced security (Xu, Ping, & Zhang, 2006). Video steganography are broadly classified as compressed and uncompressed types. In the compression type of video steganography, the data embedding frames are selected based on the motion, intra/inter frame prediction. On the other side, in the uncompressed domain, all frames are selected and used for data embedding. Figure 2 displays the details classification of video steganography techniques into various sub-categories.

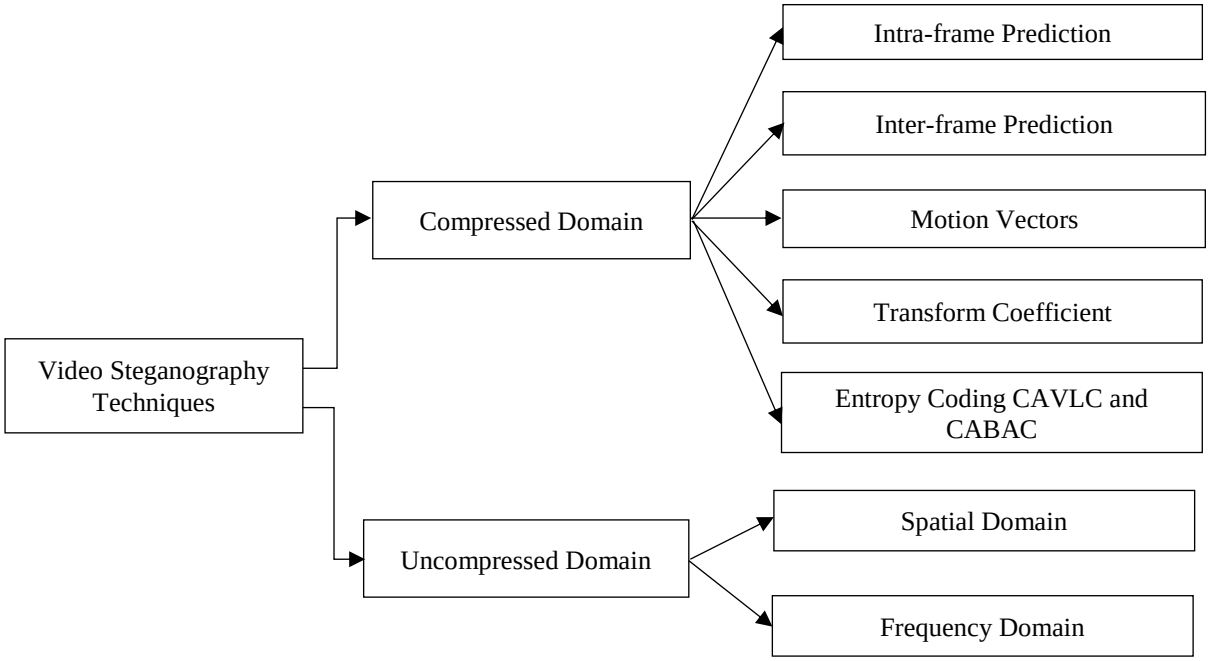

FIGURE 2. Detail Classification of Video Steganography Techniques

Table 4 and Table 5 outline the comparative analyses of various video steganography techniques in the compressed domain and uncompressed domain respectively.

TABLE 4. Comparative Analysis of Video Steganography Techniques In The Compressed Domain (Mstafa, & Elleithy, 2017)

Technique	Advantages	Disadvantages
Intra-frame Prediction Inter-frame Prediction	Moderate complexity Low computation cost	Low embedding capacity
Motion Vectors	Moderate complexity and embedding capacity	Influence on the video quality
Transform Coefficient Entropy Coding CAVLC and CABAC	Low complexity and high embedding capacity	Distorted the quality of stego media

TABLE 5. Comparative Analysis Of Video Steganography Techniques In The Uncompressed Domain (Al-Dmour, & Al-Ani, 2016)

Domain	Advantages	Disadvantages
Spatial	No need of pre-processing Less computation time High capacity	Highly affected by noise factor
Frequency	Less affected by noise More secure	Pre-processing required Complex in nature Less capacity as compared to spatial domain techniques

LSB TECHNIQUE

Cover videos being the most used technique for data hiding needs further explanations. Amongst all, least significant bit (LSB) technique is majorly preferred for data embedding in video steganography (El Safy, Zayed, El Dessouki, 2009). Wherein the LSB in the cover media is replaced by the message bit to provide minimum variability. Table 6 explains the basic design of LSB technique in terms of cover frame pixels, secret data bits and the stego frame pixels. First, the cover frames of each pixel are represented in 8 bits. Next, the cover pixels LSB bits are transformed into "0" using logical operation. Finally, the secret data bits are hidden in the cover LSB bits and maximum 1-bit variability is produced in each pixel.

TABLE 6. Architecture of LSB Technique.

Cover Frame Pixels		Secret Data Bits		Stego Frame Pixels	
10101100	00110011	1	0	10101101	00110010
11110000	00000001	0	1	11110000	00000001
10110001	11111001	0	0	10110000	11111000
10101011	00110011	1	0	10101011	00110010

MODIFIED LSB TECHNIQUE

In the modified LSB technique, the secret 2-4 bits per pixel in the cover frame is concealed. This improves the data hiding capacity and enlarges the variability exponentially as summarized in Table 7. For instance, 2 bits of secret data per pixel are hidden in 2-bit technique. Thus, only 4 pixels are required in place of 8 pixels in modified LSB technique to hide 1 byte of secret data. Conversely, in 2-bit technique maximum 4-bit variability is produced compared to 1 bit in LSB technique.

TABLE 7. Implementation of Modified LSB Technique for 2, 3 Or 4 Bit.

Technique	2-bit	3-bit	4-bit
Maximum variability	4	8	16
Pixels required to hide one byte	4	3	2

MULTI- LAYER DATA SECURITY ALGORITHMS FOR VIDEO STEGANOGRAPHY

Over the years, intensive research efforts have been dedicated in video steganography to improve the data security and robustness which involved the hybridization of cryptography

and ECC (Apau & Twum, 2017). Thus, it is customary to analyze the data security of multi-layer algorithms in video steganography in terms of their notable benefits and shortcomings.

Apau and Twum (2017) designed a multi-layer data security system in the spatial domain using the RSA, the Huffman coding, and the LSB technique. In the proposed system, data was encrypted using the asymmetric algorithm namely RSA. First, the data was compressed using lossless technique so called the Huffman code. Then, the Huffman code compression lossless technique was used to reduce the data size without any data loss. Finally, the data was hidden using the LSB technique. Although RSA algorithm provided an effective encryption with authentication however the security was achieved at the cost of large key size and too much time consumption for the encryption process. Hedge and Jagadeesha (2016) applied ELCC and optimization for data encryption wherein the data was embedded in the form of H.264 videos. Furthermore, artificial bee colony (ABC) algorithm was utilized to reduce the variability and find the best position in the data embedding step. It was acknowledged that ECC was advantageous in improving the overall processing speed for data encryption due to its smaller key size and less storage space requirement.

Mstafa and Elleithy (2016) proposed four stage algorithms for multi-layer data security in video steganography. In the first stage, the secret message was pre-processed using Hamming codes. Second stage determined the region of interest (ROI) in the frames before performing the data embedment. Besides, Viola-Jones object detection algorithm was applied to detect facial ROI. Third stage involved the construction of adaptive data embedding via 1-bit, 2-bit, 3-bit, and 4-bit LSB techniques. Lastly, the data was extracted from the RGB planes. Despite the robustness of the technique against attacks and high capacity the number of stages elongated the computation time and the Hamming code could detect only single bit errors. Liu, Li, Ma, and Liu (2013) encoded the original data using BCH scheme and embedded the data in H.264 videos. Furthermore, DCT transform was applied and processed the coefficient in 4X4 block to embed the data. The authenticity of the proposed technique was validated by applying on diverse standard video datasets (QCIF Format (176×144)-Bridgefar, Claire, Grandma, Container, Mother-daughter, Akiyo, Foreman, Hall, Carphone, Bridge-close, News, Mobiles, Salesman, and Coastguard). The developed technique provided high visual quality and robustness against attacks but required complex pre-processing in the initial phase.

Zhang, Zhang, Yang, Guo, and Liu (2017) devised a technique based on three steps. First step dealt with the splitting of secret message into n pieces using Shamir's secret sharing technique. Then, the Hamming algorithm was applied onto the secret shares. Finally, the cover video was transformed into frequency domain via DCT technique wherein the data was embedded in the DCT coefficient in zigzag manner. The proposed technique provided good invisibility, robustness, and anti-steganalysis ability wherein message bits were influenced by attacks insignificantly. The standard videos dataset format QCIF (Grandma, Carphone, Container, Miss America, and Soccer) and CIF format (Stefan, Foreman, News, Paris, and Mobile) were utilized for validating the developed technique.

Mstafa and Elleithy (2016) introduced an encryption scheme using secret keys where Hamming and BCH codes were applied for secret data encoding. Next, the obtained secret data was embedded in the discrete cosine transform (DCT) coefficients. Standard video dataset format CIF (Akiyo, Bus, Coastguard, Container, Foreman, and Soccer) was utilized. However, large number of cover media frequency domain conversion was employed for data embedding. Proposed scheme achieved high embedding capacity and excellent peak-signal to noise ratio (PSNR) to resist various attacks.

Ramalingam and Isa (2016) developed an encryption technique for data hiding in the video pre-processing wherein DCT was applied to detect scene change frames in the videos before data embedding. Later, DWT technique was applied to normalize the data embedding

frame. The main purpose of normalization was to reduce the distortion so that the maximum value of the DTC coefficients remained in the desired limit during the fusion process. Non-standard video dataset format avi (Vehicle, Person, Plot, Sample, Bulb, Sine Wave, Athletic, and Conversation) was used. The proposed technique could reduce the distortion appreciably and provide the data embedding in the random frames.

Shanableh (2012) used matrix encoding to hide the data in MPEG videos. The raw videos data were encoded using multi-layer signal to noise ratio. Besides, the quantization scales were applied to embed the data bits via matrix encoding wherein the coding parameters were stored within the encoding process. Finally, the video was encoded using modulated quantization scales and coding parameters. The technique was further improved by doubling the payload without affecting the bit rate or coding quality of the video. The proposed technique revealed less degraded video quality but required prolonged time for encoding process (such as matrix encoding, modulated quantization scale and coding). The performance of the scheme was tested by applying on standard videos dataset format MPEG-2 (Coastguard, Container, Flowergarden, Foreman, Mobile, and Hall Monitor).

Mumthas and Lijiya (2017) developed two layers encryption scheme using RSA, DNA and Huffman encoding. First, the video data was transformed using DCT technique and data was embedded using the DCT coefficients. Despite the presence of tri-tier security provision the proposed technique consumed extensive computation time to perform the required large number of pre-processing step. Meanwhile, Yadav, Mishra and Sharma (2013) introduced a data encryption technique using XOR key operation. They used sequential encoding and LSB techniques for data embedding and data hiding, respectively. Even though the encryption process consumed less time for computation compared to 3DES, AES and Blowfish based technique but the security was weak against adversaries' attacks.

PERFORMANCE ANALYSIS PARAMETERS

The performance of various video steganography techniques is analyzed using diverse parameters as discussed underneath.

VISUAL QUALITY

In the steganography, the mean square error (MSE) and PSNR are determined to ensure the visual quality after the data hiding.

MEAN SQUARE ERROR

The mean square error reflects the normalized error/difference between cover and stego video, which is expressed as:

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(Cover\ Frame - Stego\ Frame)^2}{M \times N}, \quad (1)$$

where M and N define the video dimensions.

PEAK SIGNAL TO NOISE RATIO

The PSNR parameter is used to determine the tolerance of stego video error so that the existence of the data cannot be identified. In steganography, PSNR value above 30 dB is acceptable and is defined as:

$$PSNR = 10\, log_{10} \frac{Max^2}{MSE}\ , \quad (2)$$

where Max is the highest pixel value in the video frame.

EMBEDDING CAPACITY

Usually, the video cover media consisted of several frames for data hiding wherein the data embedding capacity (EC) varies depending on the technique/domain used. Embedding capacity of the cover media can be can be written as:

$$EC = \frac{Size\ of\ Original\ Message}{Video\ Size} \times 100\% , \quad (3)$$

where M and N define the video dimensions.

ROBUSTNESS

Robustness measures the ability of embedding messages to remain unaltered even if the stego-media undergoes several transformations such as scaling or filtering. In the steganography, similarity index is determined to check its robustness.

Similarity Index (SIM)
The similarity between original and modified message is defined as:

$$SIM = \frac{\sum_{i=1}^{a}\sum_{j=1}^{b}[M(i,j) \times M^*(i,j)]}{\sqrt{\sum_{i=1}^{a}\sum_{j=1}^{b} M(i,j)^2} \times \sqrt{\sum_{i=1}^{a}\sum_{j=1}^{b} M^*(i,j)^2}} , \quad (4)$$

where M and $M^*$is the original and obtained messages; a and b parameters are the size of the hidden message.

Bit Error Rate (BER)
The BER measures the number of altering bit's position via the relation:

$$BER = \frac{\sum_{m=1}^{a}\sum_{n=1}^{b}[S(m,n) \oplus S'(m,n)]}{a \times b} \times 100\% , \quad (5)$$

where S and $S'$is the original and obtained messages.

CONCLUSION AND FURTHER OUTLOOK

This article reviewed the multi-layer data security issues present in various state-of-the-art video steganography techniques. The security performance of the existing steganography techniques against attacks were discussed in terms of diverse measures. The data security and robustness of cryptography and steganography techniques involved error correction codes. The robustness of the video steganography techniques were tested on diverse datasets. It was demonstrated that improve security and robustness is decided by the hybridization of cryptography, steganography, and error correction techniques. It was established that the existing conventional cryptography algorithms have large block size and data bits are processed in 8-bit chunk. Thus, 2^8=256 combination is required in the s-box that increased memory sizes. This issue could be overcome using lightweight cryptography algorithms. In which block size is reduced from 128 to 64 bit and data bits are processed in 4-bit chunk.

Thus, in the s-box only 16 entries look-up table required as compared to conventional algorithms 256 entries. Furthermore, in the LSB and MLSB data hiding technique, the cover LSB bits are replaced with data bits which increase variability and more prone to statistical attacks such as histogram analysis. Thus, to overcome this issue, optimization algorithms is needed to be explore which search optimal data hiding position in the cover pixel. These criteria improve the data security and provide better visual quality in the video steganography algorithms.

ACKNOWLEDGMENT

This work was supported by Universiti Kebangsaan Malaysia grant Dana Impak Perdana (DIP-2014-039) and AP.

REFERENCES

Al-Dmour, H., & Al-Ani, A. 2016. A steganography embedding method based on edge identification and XOR coding. *Expert systems with Applications*, 46: 293-306.

Apau, R., B., J., & Twum, F. 2016. Enhancing Data Security using Video Steganography, RSA and Huffman Code Algorithms with LSB Insertion. *International Journal of Computer Applications*, 143(4): 28-36.

Bharathi, D. A., & Kiran, S. M. 2017. High-Security Data Hiding in Videos using Multi-Frame, Image Cropping, and Lsb Algorithm. Ijariit, 3(3): 693-698.

Bhitre, P., & Sayankar, M. R. 2018. Audio and Video Steganography using Blowfish and 4 LSB Technique. International *Journal on Future Revolution in Computer Science & Communication Engineering*, 4(6), 51-54.

El Safy, R. O., Zayed, H. H., & El Dessouki, A. 2009. An adaptive steganographic technique based on integer wavelet transform. *International Conference on Networking and Media Convergence* (ICNM), 111-117.

He, Y., Yang, G., & Zhu, N. 2012. A real-time dual watermarking algorithm of H. 264/AVC video stream for Video-on-Demand service. *AEU-International Journal of Electronics and Communications*, 66(4): 305-312.

Hegde, R., & Jagadeesha, S. 2016. An optimal modified matrix encoding technique for secret writing in MPEG video using ECC. *Computer Standards & Interfaces*, 48: 173-182.

Lan, T. H., & Tewfik, A. H. 2006 A novel high-capacity data-embedding system. *IEEE Transactions on Image Processing*, 15(8), 2431-2440.

Liu, Y., Li, Z., Ma, X., & Liu, J. 2013. A robust data hiding algorithm for H. 264/AVC video streams. *Journal of Systems and Software*, 86(8), 2174-2183.

Mstafa, R. J., & Elleithy, K. M. 2016. A novel video steganography algorithm in DCT domain based on hamming and BCH codes. *IEEE 37th Sarnoff Symposium*, 208-213.

Mstafa, R., & Elleithy, K. 2015. A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes. *Multimedia Tools and Applications*, 75(17): 10311-10333.

Mstafa, R. J., & Elleithy, K. M. 2017. Compressed and raw video steganography techniques: a comprehensive survey and analysis. Multimedia Tools and Applications, 76(20), 21749-21786.

Mumthas, S., & Lijiya, A. 2017. Transform Domain Video Steganography Using RSA, Random DNA Encryption and Huffman Encoding. *Procedia Computer Science*, 115: 660-666.

Padmavathi, B., & Kumari, S. R. 2013. A survey on performance analysis of DES, AES and RSA algorithm along with LSB substitution. *International International Journal of Science and Research* (IJSR) India, 2(4), 170-174.

Ramalingam, M., & Isa, N. A. M. 2016. A data-hiding technique using scene-change detection for video steganography. *Computers & Electrical Engineering*, 54: 423-434.

Shanableh, T. 2012. Matrix encoding for data hiding using multilayer video coding and transcoding solutions. *Signal Processing: Image Communication*, 27(9), 1025-1034.
Shim, K. A. 2016. A survey of public-key cryptographic primitives in wireless sensor networks. IEEE Communications Surveys & Tutorials, 18(1): 577-601.
Xu, C., Ping, X., & Zhang, T. 2006. Steganography in compressed video stream. *First International Conference on Innovative Computing, Information and Control (ICICIC)*, 1: 269-272.
Yadav, P., Mishra, N., & Sharma, S. 2013. A secure video steganography with encryption based on LSB technique. IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 1-5.
Zhang, Y., Zhang, M., Yang, X., Guo, D., & Liu, L. 2017. Novel video steganography algorithm based on secret sharing and error-correcting code for H.264/AVC. Tsinghua Science and Technology, 22(2): 198-209.

Samar Kamil
Masri Ayob
Siti Norul Huda Sheikh Abdullah
Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia
p88051@siswa.ukm.edu.my, masri@ukm.edu.my, snhsabdullah@ukm.edu.my

Zulkifli Ahmad
School of Language Studies and Linguistics,
Faculty of Social Sciences and Humanities,
Universiti Kebangsaan Malaysia
duzeb@ukm.edu.my

Received: 28 December 2018
Accepted: 31 December 2018
Published: 15 January 2019