Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 171 (2020) 1147–1156

Procedia Computer Science

www.elsevier.com/locate/procedia

Third International Conference on Computing and Network Communications (CoCoNet'19)

A secured data hiding using affine transformation in video steganography

Mritha Ramalingam[a,*], Nor Ashidi Mat Isa[b], R.Puviarasi[c]

[a,*] Faculty of Computing, Universiti Malaysia Pahang, Gambang 26300, Kuantan, Malaysia
[b] Universiti Sains Malaysia, Nibong Tebal 14300, Penang, Malaysia
[c] Saveetha School of Engineering, Saveetha Institute of Medical and Technical Science, Chennai 605102, India

Abstract

Network security is the most essential aspect of information technology among today's emerging digital technologies which demands secured communication of information. In this digital network, it is essential to secure the data from intruders and unauthorized receivers. Steganography plays a vital role in secure transmission of data. This paper proposes a steganography method to hide data using affine transformation technique. The secret data are embedded in the coefficients of integer wavelet transform of the video frames. While embedding, the pixel values are distributed using affine transformation. The proposed method has been tested on many input data and the performance is evaluated both quantitatively and qualitatively. The results indicate the enhanced capability of the proposed method that can ensure imperceptible distortions with minimum computational cost in terms of PSNR factor over the existing methods.

Keywords: Security; Affine transformation; Integer wavelet transform; Video steganography

1. Introduction

Recent digital economy depends on the information and communication technologies which enable the interactions using digitized information. In today's world, the digital communication [1, 2] faces the challenge of maintaining secure data transmission when exchanged over the Internet [3]. Therefore, it is vital to develop a system to ensure data security. This is achieved by using steganography techniques. Steganography technique overcomes the encryption algorithms [4] in secure data transfer by embedding the mere existence of data in the network communication.

Steganography is the art of disguising data inside a cover-medium, without degrading the perceptual quality of data [5]. In steganography, the digital multimedia data (text, image, audio, and video) [6] in which the secret data are embedded are referred to as cover-media and the cover-media containing hidden data are called as stego-media. The current digital media steganography refers to the capability to hide information secretly within text, image, audio, or video data, such that receivers cannot guess which steganography medium contains hidden data [7]. Many approaches have been developed in digital media steganography as the privacy of individuals has become increasingly essential. Security is defined as the detectability rate between cover and stego media. The un-detectability of steganography method depends on the embedding capacity and imperceptible distortions occur in stego-media due to data embedding [8]. However, the discrimination of various steganography techniques show a complex trade-off between quality and embedding capacity [9]. In addition to the practice of steganography methods in earlier periods, different

10.1016/j.procs.2020.04.123

research attempts with respect to steganography have been initiated in recent years. Moreover, as an alternative to existing solutions, present steganography techniques achieve better data secrecy when compared with conventional security techniques [10].

Hence, the objective of this paper is to demonstrate the new steganography method using affine transformations and integer wavelet transform (IWT) coefficients to ensure security with better imperceptibility and less computational cost.

Video steganography is a process of embedding data in videos to ensure secure communication. Recent video steganography techniques use transform domain to increase security [11]. The block diagram of a basic video steganography system is illustrated in Fig.1. The system represent a general data-hiding process at the sender site and de-steganography process for data extraction at the receiver site. At sender side, the data are hidden in the cover-video by using the data hiding algorithm to produce stego-video. The embedded data is extracted using data extraction algorithm and as a result, data and carrier video are the outputs at the receiver end.

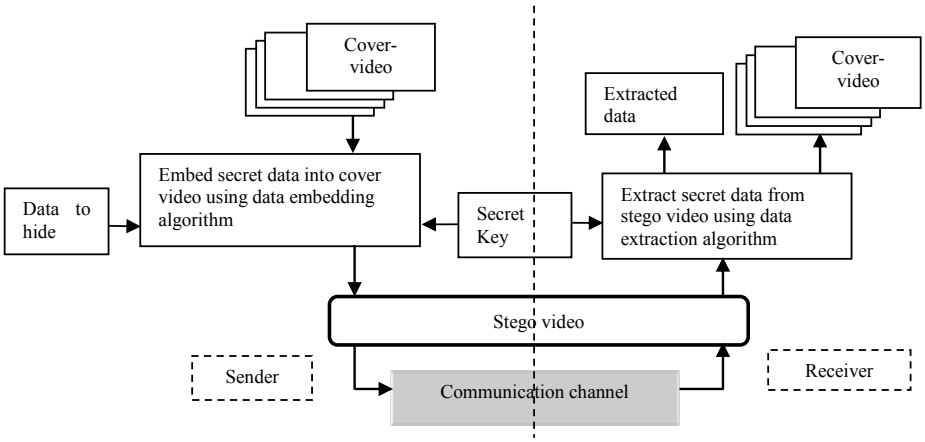

Fig. 1 Block diagram of basic video steganography system

The rest of this paper is organized into four sections. Section 2 discusses the related works. Section 3 explains the proposed method and the algorithms. Section 4 discusses the experimental results. Section 5 concludes the paper.

2. Related works

In recent years, video transmission has become increasingly popular and continue to flourish in the future, because of the fact that video provides good hiding space to perform steganography. In steganography, data are hidden in spatial, transform, compression domains of the carrier. The Least significant bit (LSB) is used widely as spatial domain-based method. LSB method hides the data by modifying the LSBs of cover-media with secret data bits. The advantages of hiding data in spatial domain are high embedding capacity and simple implementation. However, a major drawback is the data are vulnerable to various attacks making the system less secured. A spatial domain-based algorithm hid data on LSB replacement and matching stego-images [12, 13]. But there yielded a trade-off between image quality and embed capacity while using multimedia objects. Steganography based on Huffman Encoding (SHE) [14] was proven as more secured image steganography which used two 8 bit gray level images. Though improved security was proved, the method SHE addressed only to brute force attacks.

Transform domain techniques hide data by modifying the coefficients of the cover-media, then embedding the data into the transformed coefficients. Transform domain steganography techniques embed secret data in the transform space to provide high stability. Transform domain-based steganography provides higher security than spatial domain-based data hiding methods [15]. The transform domain includes Fourier, discrete cosine transform (DCT), and wavelet transforms. A discrete wavelet transform difference modulation (DWTDM) steganography technique that hides secret data in adjacent DWT coefficients is proved to be secure against various image-based attacks, such as noise addition [16].

In DWT, the wavelets use floating point coefficients. While performing data embedding in DWT, if any truncation to the floating point value of the image pixel may lead to any damage in image or loss of embedded data. In the wavelet domain, an image is divided into different sub-bands namely: low-low (LL), high-high (HH), low-high (LH) and high-low (HL) [17]. The Approximation coefficients called as LL sub-bands contains most crucial details of an image. So, embedding data in LL sub-band will decrease the image quality compared to other coefficients. Therefore, more data could be embedded in the coefficients of LH, HL and HH sub-bands. This generally enables the hiding of data in high-resolution bands which are less sensitive to Human Visual Systems (HVS). In integer wavelet transform (IWT), the integers are mapped to integers. The IWT were utilized to increase hiding capacity and enhanced image quality [18]. Besides that, there are steganography techniques which hid the data in LSB of the IWT

coefficients [19] and most significant bits (MSB) of the IWT coefficients of cover-media. Hiding in MSB of IWT coefficients ensure the better adaptation of HVS [20] resulting in better Peak-to-signal-noise (PSNR) values [21].

Meanwhile, a combination of IWT and LSB method were used to hide data in videos and shown improved security [22]. Several methods hid data in multiple group pictures and evaluated the consequences of the least distortion in the resulting video [23, 24]. A steganography technique hid an image into another image by using the matrix multiplication on max-algebra operations. This technique has achieved a better security for their secret images [25]. Additionally, the improved security in steganography was achieved by using affine transformation in the integer DCT coefficients of the stego-media [26].

A multivariate regression and flexible macro block (MRFB) ordering model hid data in compressed moving picture experts group (MPEG) videos provide high prediction accuracy and obtains better payload [27]. The major problems hindering the improvement of the performance of a transform domain-based video steganography scheme are high computational cost and lower time frequency. The method in [27] used flexible macroblock ordering (FMO) to allocate macroblocks to slice groups according to the message content. The rate of channel bit errors with computational complexity and packet losses is high because of the use of FMO. Therefore, the proposed compressed MPEG video against channel bit errors and packet losses require additional focus. However, a security threat was detected while retrieving the embedded data from the video file in the selected transform domain. However, the above existing methods were not optimal because of security and quality issues. Hence, a transform domain-based video steganography technique that could provide added security for the embedded data without affecting video quality should be developed.

The focus of this paper, the affine transformation is a method that maintains the collinearity in the carrier image. A specific view of an image scene is said to be an object. The reliability of an image will not be degraded by performing an affine transformation on an object [28-31]. The visual quality of images are influenced by performing affine transformation on images. Although the transform based steganography algorithms proved to have substantial embedding data rate with less distortion in the cover media, those methods did not achieve better imperceptibility to HVS. Hence an IWT based steganography method is proposed and discussed. Moreover, the proposed system utilizes these above mentioned advantages of IWT for better performance. Hence the data are embedded in the Diagonal coefficients called as HH sub-bands of the input cover-video frame in the proposed system.

3. The proposed system

The proposed system hides the secret data in videos by using affine transformation. In this method, secret data is hidden in the carrier file which is cover-video to result in stego-video. The transform domain of the cover-video is considered for hiding data using IWT coefficients. The pixel values are distributed by using the function of affine transformation. An affine transformation in a 2D space is expressed by Eq (1),

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix} \tag{1}$$

where (x, y) are pixel coordinates of an object in image; (x`, y`) are the pixel coordinates of transformed object [28]. After the images are transformed, the level of intensity of pixel is assigned using interpolation. The variables, a, b, c, d, e and f are transform coefficients. In Fig. 2, a simple affine transformation is applied to the image using a function called, interpolation [30]. An affine transformation of a video frame in a plane has an inverse that is also an affine transformation of the plane. In the transformation process, it is easy to check that the identity matrix, I is the only matrix with the property that if A is any m x n matrix, then it is given as in Eq.2

$$AI = IA = A \tag{2}$$

for each element x in matrix A. So the identity matrix has a special significance in the affine transformation.

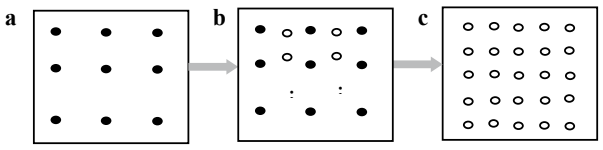

Fig. 2 Image Interpolation of Affine transformation: (a) Image: Original (b)Image Interpolation (c) Image after interpolation

An affine invariant is the invariance up to affine transformations. Affine invariant property of an image states that each movement alters the appearance of objects in image without affecting the relative geometry of the objects [30]. Affine Invariance provides good security in transmitting a visually imperceptible stego-image even with a large payload [30-32]. The proposed framework is discussed with the data embedding and extraction algorithms in the subsequent subsections.

3.1. Data embedding process

The process of data embedding algorithm is illustrated in Fig.3. The data is embedded in input cover-video frame to produce stego-video frame. The embedding process is described using the following algorithm.

Embedding algorithm: **Input**: Cover-video, Secret data; **Output**: Stego-video

1: Cover-video is partitioned into frames of equal size.

2: The cover-video frame (CVF) is split into blocks of size 8x8 pixels to categorize smooth and complex blocks for the secret data to be embedded efficiently and is formulated as given in Eq.3

$$CVF = (X_{i,j} 0 \leq i \leq R, 0 \leq j \leq C) \tag{3}$$

where 'R' ,'C' are number of rows and columns in cover image, $X_{i,j}$ denoting pixel intensities present in i, j.

3: The subsequent step in the embedding process is the pre-processing of secret data. Before embedding, the secret data are converted to binary values to facilitate further processing.

4: Each block of cover-video frame is segmented into 4x4 sized frames to obtain four sub-bands, namely, LL, HL, LH, and HH with 4x4 size.

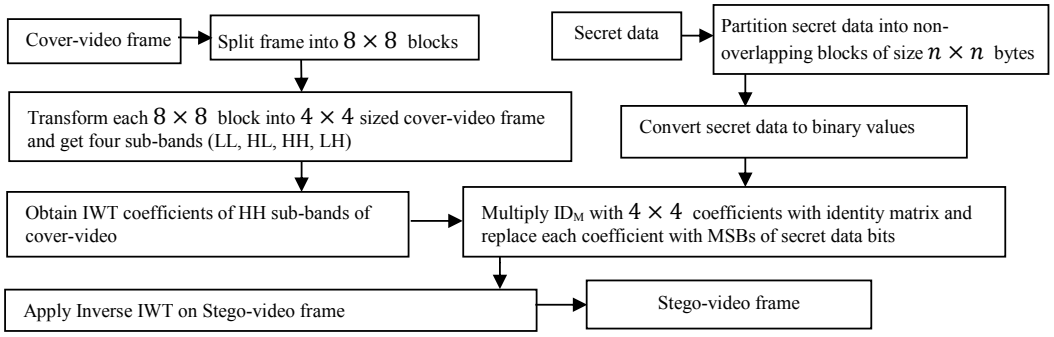

Fig. 3 Data embedding process

5: The IWT coefficients of HH sub-bands of each 4x4 video frame are identified. Four secret data bits (s1, s2, s3, s4) are considered at a time for embedding data. Data bits are embedded in the cover-video frame as follows:

Consider the identity matrix, ID = $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

Let ID_M be the identity matrix that has to be compared with 'Y' consisting of 4x4 matrix, such that,

$$ID_M = \{ ID_{ij}, i, j \in (1, 2, 3, 4)\} \tag{4}$$

From Eq. (4), the modification matrix, ID_M is obtained from ID using following conditions:

(a) If secret data bits are (0, 0, 0, 0), no change in ID occurs, such that

ID_M = $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

(b) If secret data bits are (1, 1, 0, 0), the first two rows of ID are interchanged.

$$ID_M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

(c) If secret data bits are (0, 1, 0, 0), the second row elements are replaced by using the first row elements; the first row elements remain unaltered. That is,

$$ID_M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

(d) If secret data bits are (1, 0, 0, 0), then the first row elements are replaced by using the second row elements; the second row elements remain unaltered. That is,

$$ID_M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

6: The multiplier process is applied on 4x4 HH sub-bands of the cover-video to multiply with the obtained ID_M resulting in the stego-video, that is, $ID_M \cdot Y=K$. The resultant stego-video values are stored in K.

Consider an example, let Y be 4x4 cover-video frame,

$$Y = \begin{pmatrix} 5 & 9 & 4 & 2 \\ 8 & 6 & 9 & 8 \\ 2 & 7 & 1 & 8 \\ 6 & 9 & 3 & 7 \end{pmatrix}$$

then, for each value of 'Y', the comparison with identity matrix ID_M is performed such that

$$\sum_{i,j=1}^{8} Y_{ij} \; where \; Y_{ij} = \begin{cases} \mathbf{1}, Y_{ij} = ID_{ij} \\ \mathbf{0}, otherwise \end{cases} \quad (5)$$

Based on Eq. (5), for the considered example, the multiplier is performed by using four cases:

Case (1): If secret data spot is (0, 0, 0, 0), then stego-video K is similar to the cover-video.

$$K = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 5 & 9 & 4 & 2 \\ 8 & 6 & 9 & 8 \\ 2 & 7 & 1 & 8 \\ 6 & 9 & 3 & 7 \end{pmatrix} = \begin{pmatrix} 5 & 9 & 4 & 2 \\ 8 & 6 & 9 & 8 \\ 2 & 7 & 1 & 8 \\ 6 & 9 & 3 & 7 \end{pmatrix}$$

Case (2): If secret data spot is (1, 1, 0, 0), in the resulting stego-video K the elements of first two rows of Y are interchanged.

$$K = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 5 & 9 & 4 & 2 \\ 8 & 6 & 9 & 8 \\ 2 & 7 & 1 & 8 \\ 6 & 9 & 3 & 7 \end{pmatrix} = \begin{pmatrix} 8 & 6 & 9 & 8 \\ 5 & 9 & 4 & 2 \\ 2 & 7 & 1 & 8 \\ 6 & 9 & 3 & 7 \end{pmatrix}$$

Case (3): If secret data spot is (0, 1, 0, 0), the resulting stego-video K will retain the elements of first row on the second row of Y.

$$K = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 5 & 9 & 4 & 2 \\ 8 & 6 & 9 & 8 \\ 2 & 7 & 1 & 8 \\ 6 & 9 & 3 & 7 \end{pmatrix} = \begin{pmatrix} 5 & 9 & 4 & 2 \\ 5 & 9 & 4 & 2 \\ 2 & 7 & 1 & 8 \\ 6 & 9 & 3 & 7 \end{pmatrix}$$

Case (4): If secret data spot is (1, 0, 0, 0), subsequently the stego-video K will have the first two rows similar to the second-row elements of Y.

$$K=\begin{pmatrix}0&1&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}5&9&4&2\\8&6&9&8\\2&7&1&8\\6&9&3&7\end{pmatrix}=\begin{pmatrix}8&6&9&8\\8&6&9&8\\2&7&1&8\\6&9&3&7\end{pmatrix}$$

7: Apply Inverse IWT on the resulting stego-video frame

8: Obtain the stego-video in spatial domain.

3.2. Data extraction process

The process of data embedding at the destination, the intended receiver of the secret data applies data extraction process to retrieve the embedded data from stego-video. This process is a reverse procedure of data embedding algorithm. The steps involved in data extraction process of proposed method is shown in Fig.4.

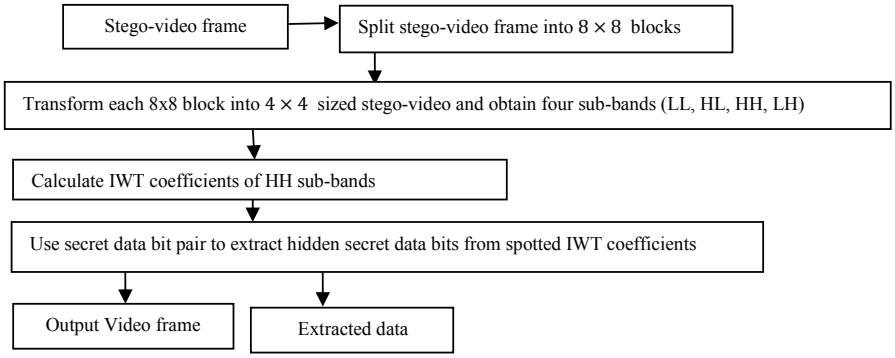

Fig. 4 Data extraction process

Extraction algorithm: **Input**: Stego-video; **Output**: Extracted data, Output video

1: Decompose stego-video into frames.
2: The stego-video frame is split into 8x8 blocks for further processing.
3: The IWT coefficients are obtained by decomposing 8x8 blocks into 4x4 blocks to obtain four sub-bands (LL, HL, HH, LH) in the transform domain
4: Secret data bit pair serves as a significant function in the extraction of the hidden data from each 4x4 stego-video block. Using secret data bit pair orientation, the embedded bits are extracted from stego-video in the following ways:
(a) If the first row r1 and the second row r2 of the matrix are identical, then two secret data bit pairs, (0,1) or (1,0), are hidden. While retrieving embedded data, the first element of bit pair in the secret data is used as a reference. If the data bit is 0, then embedded bits are (0,1) else, if data bit is 1 then embedded bits are (1,0).
(b) If r1 and r2 are not identical, two secret data bit pairs, (0,0) or (1,1) are hidden. If data bit is 0, then embedded bits are (0,0) else, if data bit is 1 then embedded bits are (1,1).
5: The resulting output is the embedded data and cover-video.

4. Results and Discussion

4.1. Experimental dataset and evaluation method

The proposed method was implemented in MATLAB to embed data in different video files. The dataset in Table 1 is employed from Internet Archive, a 501(c) (3) non-profit organization that provides researchers with permanent access to different formats of text, audio, digital images, and video files. The proposed method is tested using different video files as cover-videos quantitatively and qualitatively. Qualitative evaluation depends on human interpretation of the quality in resulting videos. Quantitative evaluation depends on mathematical evaluations of the resulting videos with the original video. The performance of proposed method is compared with that of three existing state-of-the-art methods, namely, the SHE [14] and DWTDM [16] and MRFB [27]. The

MRFB method was analyzed in terms of accuracy of data extraction, payload, distortion quality and compression overhead. On the other hand, the SHE method was proved to result in better security of stego image. Finally, the DWTDM method provided a steganography method for embedding data without producing major changes in the images. By considering the typical parameters in all the works, the performance results of proposed method is performed in terms of throughput (i.e. data extraction accuracy), computational cost and channel bit error rate.

Table 1. Dataset used to evaluate the performance

Cover-video					Secret data			
Test video sequence		Resolution	Number of frames	Size (KB)	ID	Name	Size (KB)	Resolution
ID	Name							
T1	flower.avi	1240×1180	5	247.1	S1	chrys.jpeg	27.4	32×64
T2	redrose.avi	2259×2325	10	350.9	S2	flower1.jpg	34.6	55×77
T3	car.avi	216×192	15	104.6	S3	image5.png	45.6	78×99
T4	skating.mp4	1380×960	20	380.3	S4	lotus.jpeg	73.3	85×110
T5	river.mpeg	390×355	25	52.44	S5	lily.jpg	78.6	25×32
T6	shape.avi	1420×1240	30	962.6	S6	img6.gif	81.3	152×80
T7	rock.wav	380×220	35	852.0	S7	child.jpeg	84.2	185×155
T8	rapidcar.avi	320×300	40	768	S8	sunset.jpg	85.3	245×23
T9	bin.mp3	235×155	45	10337	S9	power.ppt	88.2	230×220

The peak signal-to-noise ratio (PSNR) is to compute the low, medium, and average embedding capacity of secret data. PSNR value is used to measure the quality of the stego-video in proposed method, which is represented by Eq. (6).

$$\mathrm{PSNR} = 10\log10\left(\frac{L^2}{\mathrm{MSE}}\right) \tag{6}$$

where L is the peak signal level; and MSE is the mean square error, which is the pixel value of the cover-video after data hiding. MSE value is calculated using Eq. (7).

$$MSE = \frac{1}{H \times W}\sum_{i=1}^{H} \sum_{j=1}^{W}(C(i,j) - S(i,j))^2 \tag{7}$$

where $C(\mathrm{i},\mathrm{j})$ and $S(\mathrm{i},\mathrm{j})$ are pixel intensity values of cover and stego videos, respectively. The quality of videos is typically maintained at a better level with higher PSNR values, thus resulting in stego-video with few distortions that lead to high imperceptibility to HVS. Throughput is defined as the average rate of successful delivery of data over a communication channel. The throughput is obtained mathematically using Eq (8).

$$n = d \times t \tag{8}$$

where 'n' is the number of data bits hidden in the cover-video, 'a' is the rate at which data is transmitted, and 't' is the time taken to deliver the data over the communication channel.
Computational cost, C is defined as the time consumed by the sender to hide different data files of different size in the cover-video and is derived by using Eq (9).

$$C = M_x\, X(j,k) + M_y\, Y(j,k) + \frac{M_x + M_y}{M_x\, M_y} \tag{9}$$

where M_x and M_y are the time consumed in the data embedding process of the cover-video and the secret data, respectively. X(j, k) and Y(j, k) denote the average distortion (MSE value) computed over the cover-video and the secret data, respectively.

The channel bit error rate can be measured by using PSNR values, thus measuring the noise during data transfer between sender and receiver. Distortions refer to the alterations occurring in cover-videos by embedding secret data into the source videos. The security can be increased by selecting suitable coefficients in the wavelet domain for data embedding.

4.2. Quantitative analysis: throughput

Throughput is measured based on the embedding capacity and PSNR values of the secret data. For a test image, with the obtained PSNR value as the base, the throughput is evaluated using proposed method and three comparing methods. The experimental results in Table 2 shows the improved throughput of proposed method over existing methods.

Table 2. Performance comparison of proposed and other methods in terms of PSNR vs Throughput

		Throughput (kilobits/sec)			
Test video (T)	PSNR (dB)	**Proposed method**	MRFB	SHE	DWTDM
T1	9.84	**235**	225	218	200
T2	8.25	**335**	321	315	302
T3	10.06	**98**	95	91	85
T4	7.751	**372**	360	352	343
T5	10.33	**49**	47	44	40
T6	8.83	**954**	935	921	918
T7	7.58	**841**	832	825	818
T8	8.52	**759**	745	733	721
T9	8.05	**10320**	10290	10270	10263

The comparative variance of the proposed method is approximately 24% greater than that of MRFB, 45% to that of SHE and 76% higher than that of the DWTDM. Based on the above-mentioned observations, it is noted that embedding secret data in IWT coefficients of the proposed method produces better throughput compared to existing techniques.

4.3. Quantitative analysis: computational cost

The Computational cost is evaluated in milliseconds. The comparison of computational cost evaluated for hiding data of different sizes using proposed and existing methods is shown in Fig.5.

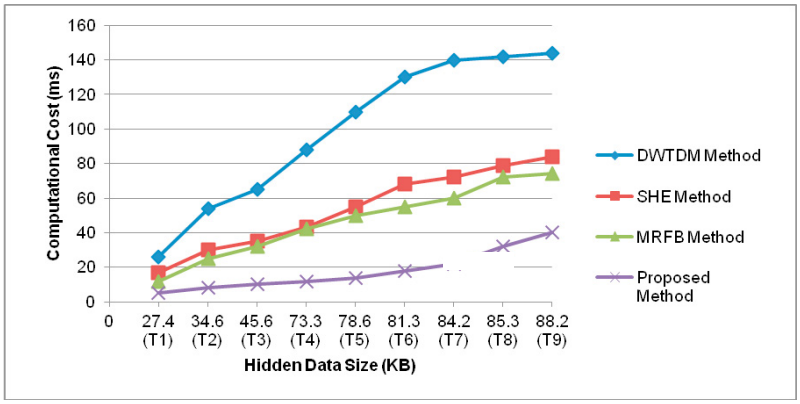

Fig. 5 Comparison of computational cost: proposed vs state-of-the-art methods

From Fig.5, the cost incurred to hid data using proposed method is significantly lower than that of existing state-of-the-art methods. The variance of computational cost in proposed method is approximately 50% to 75%, 60% to 80%, and 70% to 75% less than that of the MRFB, SHE, and DWTDM, respectively. Overall, the proposed method clearly outperforms the MRFB, SHE, and DWTDM methods in terms of computational cost.

4.4. Quantitative analysis: channel bit error rate

The channel bit error rate is measured in decibels (dB). The evaluated performance of proposed method in terms of channel bit error rate compared with existing methods is shown in Fig.6. The proposed method is proven to provide the optimal result, which is 60% to 75% less than that of the MRFB and DWTDM and 80% to 85% less than that of the SHE. The channel bit error rate of SHE method is the highest. Although the channel bit error rates of MRFB and DWTDM are less than that of SHE, the proposed method is proven to provide the optimal result. This condition ensures that the proposed method reduces the occurrence of noise in videos providing better imperceptibility. Thus, the method provides better security as the error rate of the method is comparatively lesser than state-of-the-art methods

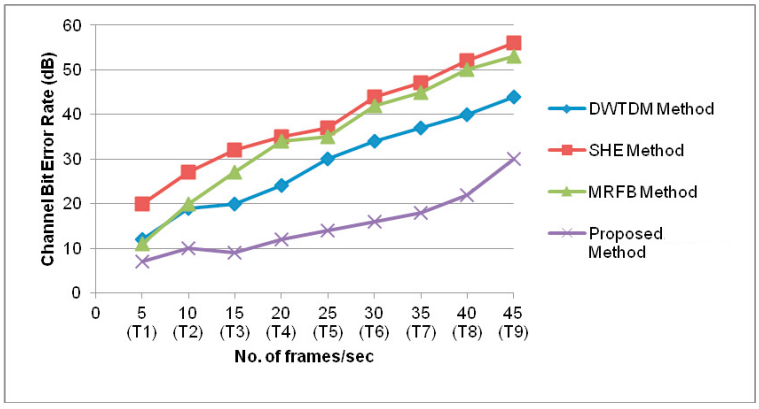

Fig. 6 Comparison of channel bit error rate using proposed and other methods

4.5. Quantitative analysis: Comparison of Noise Occurrence

The qualitative evaluation of proposed method is conducted involving human perception of the quality of the resulting videos. The qualitative results of noise occurrence in the resulting videos are shown in Fig.7.

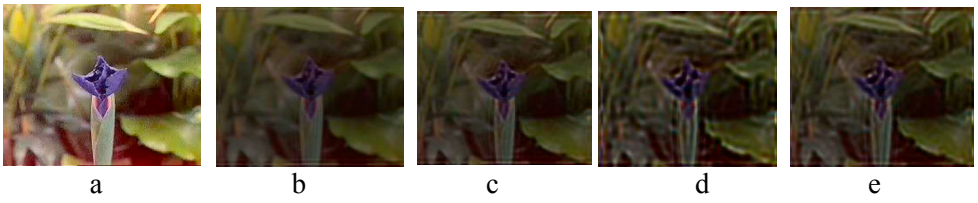

Fig. 7 Noise occurrence in T1: (a) original cover-video frame T1; (b) proposed method, (c) MRFB, (d) SHE, and (e) DWTDM.

The video frames in Fig.7 demonstrate the noise introduced in sample cover-video frame T1, Flower.jpg, by applying the proposed and comparing methods. The areas affected by noise reduce the functionalities of the video frames. By comparing the video frames in Fig.7 (b)-(e) with original cover-video frame in Fig.7 (a), the distortion or noise that has occurred in the resulting video frame by using SHE method in Fig.7 (d) is higher. In contrast, the noise occurred in the stego-video frame generated by the proposed method is comparatively less.

5. Conclusion

This paper discussed an IWT-based video steganography method to conceal the secret data. The method used affine transformations for steganography and proved to have less channel bit errors. By exploiting the features of superior consistency with the HVS of wavelet transform, the proposed method hide the data in IWT coefficients to achieve better imperceptibility and visual quality. To summarize, the proposed method minimizes the occurrence of noise in the resulting videos, and incurs low computational cost. Moreover, the hidden data in the proposed method are proven to be perceptually invisible and statistically undetectable, thereby resulting in a system with enhanced security

Acknowledgements

This work was supported by Universiti Malaysia Pahang, Malaysia as a research grant [Grant number: RDU170396]

References

[1] Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N., & Farouk, A. (2018). “Secure medical data transmission model for IoT-based healthcare systems”. *IEEE Access*, **6**, 20596-20608.

[2] Das, R., & Das, I. (2016). “Secure data transfer in IoT environment: adopting both cryptography and steganography techniques”. *IEEE Second International Conference on Research in Computational Intelligence and Communication Networks*, 296-301.

[3] Yin, J. H. J., Fen, G. M., Mughal, F., & Iranmanesh, V. (2015). "Internet of Things: Securing Data using Image Steganography". *IEEE International Conference on Artificial Intelligence, Modelling and Simulation*, 310-314.

[4] Zhou, S., Wei, Z., Wang, B., Zheng, X., Zhou, C., & Zhang, Q. (2016). "Encryption method based on a new secret key algorithm for color images". *AEU-International Journal of Electronics and Communications*, **70(1)**, 1-7.

[5] Anderson, R. J., & Petitcolas, F. (1998). "On the limits of steganography". *IEEE Journal on selected areas in communications*, **16(4)**, 474-481.

[6] Saha, B., & Sharma, S. (2012). "Steganographic techniques of data hiding using digital images". *Defence Science Journal*, **62(1)**, 11.

[7] Ziellnska, E., Mazurczyk, W., & Szczypiorski, K. (2014). "Trends in Steganography". *Communications of the ACM*, **57(3)**, 86-95.

[8] Zhang, W., & Li, S. (2004). "Security measurements of steganographic systems". *International Conference on Applied Cryptography and Network Security*. 194-204. Springer, Berlin, Heidelberg.

[9] Thanikaiselvan, V, Bansal T, Jain P & Shastri S (2016). "9/7 IWT Domain data hiding in image using adaptive and non-adaptive methods". *Indian Journal of Science and Technology*, **9(5)**.

[10] Wadhwa, A. (2014). "A survey on audio steganography techniques for digital data security". *International journal of advanced research in computer science and software engineering*, **4(4)**, 618-622.

[11] Zhang, H., Cao, Y., & Zhao, X. (2016). "Motion vector-based video steganography with preserved local optimality". *Multimedia Tools and Applications*, **75(21)**, 13503-13519.

[12] Shukla, A. K., Singh, A., Singh, B., & Kumar, A. (2018). "A secure and high-capacity data-hiding method using compression, encryption and optimized pixel value differencing". *IEEE Access*, **6**, 51130-51139.

[13] Quach, T. T. (2011). "Optimal cover estimation methods and steganographic payload location". *IEEE Transactions on Information Forensics and Security*, **6(4)**, 1214-1222.

[14] Das, R., & Tuithung, T. (2012, March). "A novel steganography method for image based on Huffman Encoding". *IEEE 3rd National Conference In Emerging Trends and Applications in Computer Science*, 14-18.

[15] Maniriho, P., & Ahmad, T. (2019). "Information hiding scheme for digital images using difference expansion and modulus function". *Journal of King Saud University-Computer and Information Sciences*, **31(3)**, 335-347.

[16] Bhattacharyya, S., & Sanyal, G. (2012). "A robust image steganography using DWT difference modulation (DWTDM)". *International Journal of Computer Network and Information Security*, **4(7)**, 27.

[17] S. Hemalatha, U. D. Acharya, A. Renuka, and P. R. Kamath. (2013). "A secure color image steganography in transform domain", *International Journal of Information Security*, **3(1)** 17–24.

[18] Jayasudha, S. (2013)."Integer wavelet transform based steganographic method using OPA algorithm". *International Journal of Engineering and Science*, **2(4)**, 31-35.

[19] Emad E, Safey A, Refaat A, Osama Z, Sayed E and Mohamed.E (2018). "A secure image steganography algorithm based on least significant bit and integer wavelet transform". *Journal of Systems Engineering and Electronics*, **29(3)**, 639-649.

[20] Aref M and Karim F, 2018. "An image steganography method based on integer wavelet transform". *Multimedia Tools and Applications*, **77(11)**, 13133-13144

[21] Hisham, S. I., Muhammad, A. N., Badshah, G., Johari, N. H., & Zain, J. M. (2017). "Numbering with spiral pattern to prove authenticity and integrity in medical images". *Pattern Analysis and Applications*, **20(4)**, 1129-1144.

[22] Ramalingam, M., & Isa, N. A. M. (2014). "Video steganography based on integer haar wavelet transforms for secured data transfer". *Indian Journal of Science and Technology*, **7(7)**, 897-904.

[23] Aly, H. A. (2011). "Data hiding in motion vectors of compressed video based on their associated prediction error". *IEEE transactions on information forensics and security*, **6(1)**, 14-18.

[24] Filler, T., Judas, J., & Fridrich, J. (2011). "Minimizing additive distortion in steganography using syndrome-trellis codes". *IEEE Transactions on Information Forensics and Security*, **6(3)**, 920-935.

[25] Song, X., Wang, S., & Niu, X. (2012). "An integer DCT and affine transformation based image steganography method". *IEEE Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 102-105.

[26] Kiswara A. S, Fatmawati, and Suprajitno H. (2018). "On Max-Plus Algebra and Its Application on Image Steganography", *The Scientific World Journal*, vol. 2018, Article ID 6718653, 9 pages. https://doi.org/10.1155/2018/6718653

[27] Shanableh, T. (2012). "Data hiding in MPEG video files using multivariate regression and flexible macroblock ordering". *IEEE transactions on information forensics and security*, **7(2)**, 455-464.

[28] Yang, Z., & Cohen, F. S. (1999). "Image registration and object recognition using affine invariants and convex hulls". *IEEE Transactions on Image Processing*, **8(7)**, 934-946.

[29] Ben-Arie, J., & Wang, Z. (1998). "Pictorial recognition of objects employing affine invariance in the frequency domain". *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **20(6)**, 604-618.

[30] Lee, Y. K., & Chen, L. H. (2002). "Object-based image steganography using affine transformation". *International journal of pattern recognition and artificial intelligence*, **16(06)**, 681-696.

[31] Wang, S., Song, X., & Niu, X. (2012). "An affine transformation based image steganography approach". *International journal of digital content technology and its applications*, **6(1)**, 14-85.

[32] Younus Z.S and Hussain M.K. (2019) "Image steganography using exploiting modification direction for compressed encrypted data", *Journal of King Saud University - Computer and Information Sciences*, https://doi.org/10.1016/j.jksuci.2019.04.008