Video steganography based on DCT psychovisual and object motion

Muhammad Fuad, Ferda Ernawan
Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang, Malaysia

ABSTRACT

Steganography is a technique of concealing the message in multimedia data. Multimedia data, such as videos are often compressed to reduce the storage for limited bandwidth. The video provides additional hidden-space in the object motion of image sequences. This research proposes a video steganography scheme based on object motion and DCT-psychovisual for concealing the message. The proposed hiding technique embeds a secret message along the object motion of the video frames. Motion analysis is used to determine the embedding regions. The proposed scheme selects six DCT coefficients in the middle frequency using DCT-psychovisual effects of hiding messages. A message is embedded by modifying middle DCT coefficients using the proposed algorithm. The middle frequencies have a large hiding capacity and it relatively does not give significant effect to the video reconstruction. The performance of the proposed video steganography is evaluated in terms of video quality and robustness against MPEG compression. The experimental results produce minimum distortion of the video quality. Our scheme produces a robust of hiding messages against MPEG-4 compression with average NC value of 0.94. The proposed video steganography achieves less perceptual distortion to human eyes and it's resistant against reducing video storage.

This is an open access article under the CC BY-SA license.

Keywords:
DCT psychovisual threshold
Hiding data
Hiding technique
Object motion
Video steganography

1. INTRODUCTION

With the rapid growth of internet technology, hiding data techniques become popular in current communication. Steganography technique is one of hiding data techniques for secret communications. For example, a user embed a secret data and send to the receiver, then only a receiver who has a key can extract the secret message [1]. Multimedia data such as digital video has become popular for both online and offline environments. Video is the best medium for hiding data due to hiding capacity and it also provides large redundancy of sequence images than other digital multimedia, such as audio, text and image. Due to higher redundancy in the consecutive frames of a video, video data can be a better medium for steganography compared to other digital media [2]. Data-hiding techniques in video files grow widely in the recent years for secured communication, ownership and copyright protection. Data-hiding steganography technique for video files is more secure due to the relative complexity of video compared to audio and image files [3]. Therefore, video steganography technique becomes important for communication. Video file provides a large data and it requires large processing transmission. Due to the huge amount of data,
videos are often compressed to reduce the storage and the transmission payload at the expense of lower quality for bandwidth related issues. Due to limited bandwidth, videos are usually compressed to reduce the storage before transferring the video data. The videos provide additional hidden-space in scene change; those hidden-spaces are highly imperceptible to human visual systems. The existing video steganography schemes do not resistant under video compression. The hiding message was destroyed by the quantization process in video compression [4]. Therefore, it is quite challenging to develop video steganography technique that can resistant under video compression and maintain the quality of video close to the original video.

Many steganography techniques presented data hiding scheme by randomly selected frames of videos. They do not sufficiently consider the bit error of hidden data. Concealed message by randomly selected frames may produce some distortions in the stego-videos. In order to manage the video quality, there exists a number the data-hiding techniques that conceal message among scene changes. A video steganography technique based on scene-change provides better security and less distortion in the quality of the video. The scheme in [5] implements least significant of bits (LSB) for concealing the messages which are easy to be removed against compression methods. Furthermore, this scheme does not sufficiently consider the optimal bits of the hidden data. Scene-change redundancies have not been revealed like the redundancy model that has been investigated in audio steganography [6]. The field of audio steganography has made a significant progress in identifying the redundant part of audio to conceal a secret-message while reducing the distortion of the stego-audio. Unlike the audio steganography, the scene-change process in videos has not been fully investigated in video steganography system.

This paper proposes DCT psychovisual effect and object motion for concealing message in video data. The proposed video steganography uses discrete cosine transform (DCT) due to compact transform and easy to be implemented. The message is concealed in the selected DCT coefficients that do not give significant effect on the quality of video. The proposed scheme provides a good level of video quality and it can resistant against compression technique.

2. RELATED WORK

Steganography is an art of hiding confidential information to secure communication [7]. Steganography techniques have been developed in spatial and frequency domains to hide the secret data/message. In the spatial domain, data are concealed in the pixels of cover-media [8]. For example, Hong and Chen [9] focused on increasing the capacity of hiding-data. Their scheme produces lower distortion for various payloads and is claimed to be secured under different types of detection techniques (steganalysis techniques). However, this approach is highly vulnerable to steganalysis under compression [10]. The hidden data may be lost because of quantization process in the compression technique.

Steganography can be performed in the frequency-transformed domains that generally provide lower imperceptibility in addition to robustness against compression. The most-used transforms include DCT, discrete wavelet transforms (DWT), redundant discrete wavelet transform (RDWT), integer wavelet transforms (IWT) and Tchebichef moments. Each transform has its own advantage e.g., Tchebichef moments result in the reduced accumulation of the numerical errors [11]. Tchebichef moments have energy compactness properties of the large image blocks. RDWT transform is able to produce high quality in the reconstruction of the images than other transforms [12], while it requires large computational time.

Unlike digital watermarking technique in which the robustness against attacks is the main objective, the basic features expected from steganography are high imperceptibility [13], large hiding capacity for secret-message, and security [14]. A video has a large number of image frame, it is a quite large amount of redundant data [15] and statistical complexity [16]. Therefore, video data is suitable for steganography. Since videos are often compressed to reduce the storage before transmission, the steganography technique for a video should withstand compression methods.

Steganography technique based on edge detection of images was studied in 2016 by Al-Dmour and Al-Ani [17]. The author claimed that their approach provides less degradation in image quality compared to smooth areas. However, this scheme has a limited capacity for data hiding. Idbeaa et al. [18] presented a steganography technique for embedding message in Intra and Inter frames (I, B, and P frames). Their schemes can achieve negligible degradation of PSNR values with minimum bit rates. While their scheme do not sufficiently consider the number of bits of hidden data. The less security and low quality of stego-videos are the major issues of many existing steganographic methods.

In 2015, Ramalingam et al. [19] presented a technique for fast retrieval of hidden data using enhanced hidden Markov model in video steganography. The proposed steganography technique provides rendering payload to increase the absolute visual quality. However, steganography technique may produce some distortions on the extracted secret message when the stego-video was compressed by compression

 Bulletin of Electr Eng & Inf, Vol. 9, No. 3, June 2020 : 1015 – 1023
techniques. The quality of the extracted hidden data needs to be improved when the cover-medium is compressed.

A steganography technique scheme for data hiding on randomly selected frames of videos was experimentally developed by Sudeepa et al. [20] in 2016 and by Kar et al. [21] in 2018. In the technique, the embedding process on randomly selected frames was constrained by how much bit error to be minimized. In [20] and [21], the authors do not consider the hidden space between image frames. Consecutive frames in a video have large redundancies that can be potentially used to hide the secret message. These redundant spaces are the best embedding locations, while it can be removed by compression method if we do not consider the optimal bits of hidden data.

There exist a number of scene-detection algorithms for video steganography which uses discrete cosine transform during video parsing. A data hiding scheme using the scene-change during video sequences was presented by Ramalingam and Isa in [5]. They utilized DCT and DWT to enhance the hidden-data security and the video quality. However, the capacity and the quality of the cover-medium of steganography scheme adopted in their paper need to be improved. Furthermore, the embedding process was constrained by how many bits of secret message are embedded and the embedding locations in the frame during the scene change were not investigated to determine whether they can withstand the compression. Thus, improving robustness against video compression and preserving video quality must be investigated in video steganography. Video steganography typically focuses on how to embed hidden data in the video without being seen by the human visual system. While, due to efficiency of transferring data most of videos are being compressed.

3. RESEARCH METHOD

3.1. Object motion 1

Object Motion can be detected by the motion vector of P and B frames [22]. The motion vector which has a large magnitude indicates faster moving pixels of the macro-blocks. It is potential to hide a message along the motion vectors that can produce minimum distortion. The concealing message in the slightly movement can introduce some distortion of the images. The object motion detection is described in the Algorithm 1.

Algorithm 1: Object motion detection

| Input: | I-Frame, B-Frame, and P-Frame |
| Output: | x and y coordinates of object motion |

Step 1: Select P and B frames to determine motion vector
Step 2: Calculate predicted motion value based on the difference between current and previous image frames
Step 3: Calculate the magnitude of motion vector $MV$ as defined by:
$$|MV(i)|=\sqrt{H(i)^2+V(i)^2}$$
where $H(i)$ and $V(i)$ represent the horizontal components and the vertical component of the motion vector in the i-th of blocks.
Step 4: Select block motions of 8×8 pixels where motion value $MV(i) <= 7$
Step 5: Save x and y coordinates of selected block motions.

3.2. Psychovisual threshold

Human visual system (HVS) cannot detect rapidly changing in normal viewing condition [23]. HVS is not equally sensitive to all visual image information and detect irrelevant image information (e.g. psychovisual redundancy) [24]. Psychovisual experiments have examined the visibility threshold of the HVS. Psychovisual threshold represents a possible threshold where HVS cannot detect a change or degradation of the image. If the frequency coefficients are lower than the psychovisual threshold, the image information can be discarded by HVS. Psychovisual threshold has been introduced in image compression [25] and digital watermarking [26] for prescribing quantization values and determining the embedding locations, respectively. This paper proposes a new embedding technique in video data that can embed the optimal number of bits of the secret message considering psychovisual effect and is resistant to compression. The selected blocks based on motion vector are transformed by 8×8 DCT. Furthermore, the transformed DCT coefficients are arranged in a zig-zag order as shown in Figure 1.

Referring to psychovisual threshold in [26], six coefficients in the frequency order between 4 and 5 are chosen for hiding data due to significantly less effect to the errors reconstruction. These coefficients provide minimum distortion against quantization tables [25] and it is potential concealing the message without visual image distortion. The authors assume that those coefficients provide minimum distortion against compressed video. This experiment uses two thresholds $f$ and $s$, these thresholds are used to scale the selected coefficient pairs. Thresholds $f$ and $s$ are set based on Algorithm 2.

Video steganography based on DCT psychovisual... (Muhammad Fuad)
where \( T \) represents a threshold value which obtained from a trade-off between the imperceptibility and robustness under video compression. Threshold \( T \) is evaluated by structural SIMilarity (SSIM) index [27] and normalized-cross correlation (NC) values [28]. This experiment proposes \( T \) of 20 for scaling DCT coefficients.

4. PROPOSED SCHEME

The proposed concealing message is shown in Figure 2. The proposed hiding technique is evaluated by imperceptibility measurement. The proposed hiding and extracting techniques are discussed in Algorithms 3 and 4 respectively. The proposed hiding and extracting schemes.

Algorithm 3: Hiding technique

Input: Selected video frame; thresholds (\( f \) and \( s \))

Step 1: Select blocks that have object motion.

Step 2: Selected blocks are transformed by 8×8 DCT.

Step 3: Select DCT coefficients based on psychovisual effect and re-arrange it into a vector \( D \).

Step 4: Hiding data algorithm is defined by:

\[
S=1;
\]

for \( u=0 \) to \( 2 \)

if \( S<=\)length(frame)

if frame(S)=1 then if(\(|D(2u)|<|D (2u+1)|\)) then

\[
C = D (2u);
\]

\[
D (2u) = D (2u+1) + s;
\]

\[
D (2u+1) = C;
\]

else

\[
D (2u) = D (2u) + f;
\]

\[
D (2u+1) = D(2u+1);
\]

end (if)
Video steganography based on DCT psychovisual.

Algorithm 4: Extracting Technique

Input: Stego-video; x and y coordinates of the selected blocks based on object motion;
Step 1: x and y coordinates of object motion are used to select concealed message region.
Step 2: Each selected block is transformed by 8x8 DCT.
Step 3: Select DCT coefficients based on psychovisual effect and re-arrange it into a vector D.
Step 4: Selected DCT coefficients D are computed by the following rule:

\[
\text{if } D(k) < D(k+1) \text{ for } k = 0, 2, 4 \text{ then } \\
\text{message_bit} = 1; \\
\text{else } \\
\text{message_bit} = 0.
\]
Step 5: Each message bit is arranged to recover the message.

Output: Message recovery

Our scheme is evaluated by imperceptibility measurement and compressed video. The mean peak signal-to-noise ratio (MPSNR) is measured to evaluate the quality of video data. The MPSNR is defined by:
\[ MPSNR(x, y) = \frac{1}{S} \sum_{j=1}^{S} PSNR(x_j, y_j) \]  

(1)

where \( S \) represents the sequence number of image frames and PSNR can be defined by [29]:

\[ PSNR = 10 \log_{10} \left( \frac{255^2}{\text{MNR}} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (f(i, j, k) - g(i, j, k))^2 \right) \]  

(2)

for \( M, N \) denotes the row and column sizes, \( R \) represents number of color channels. The distortion of the stego-video is measured by Mean Absolute Reconstruction Error (MARE), it can be defined by:

\[ MARE(x, y) = \frac{1}{S} \sum_{j=1}^{S} ARE(x_j, y_j) \cdot ARE = \frac{1}{\text{MNR}} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \sum_{k=0}^{R-1} (f(i, j, k) - g(i, j, k)) \]  

(3)

where \( S \) represents the sequence number of image frames. The minimum MARE value means that the quality of stego-video is closer to the original video. The quality of extracting hidden data is also evaluated by Mean bit error rate (MBER) and mean normalized-cross correlation (MNC). MBER and MNC are defined by:

\[ MNC = \frac{1}{S} \sum_{j=1}^{S} NC(j), \quad NC = \frac{\sum_{i=0}^{D} H(i) \cdot H'(i)}{\sqrt{\sum_{i=0}^{D} H(i)^2 \sum_{i=0}^{D} H'(i)^2}} \]  

(4)

\[ MBER = \frac{1}{S} \sum_{j=1}^{S} BER(j), \quad BER = \frac{\sum_{i=0}^{D} H(i) \oplus H'(i)}{D} \]  

(5)

where \( D \) denotes the length of message bits, \( H(i) \) is the original message, \( H'(i) \) is the extracted message and \( \oplus \) indicates the OR operation.

5. EXPERIMENTAL RESULTS

The experimental results of the proposed hiding technique in video steganography demonstrate the statistical imperceptibility of stego-video and the embedding capacity of the proposed scheme. This experiment uses five videos [30] to test the proposed algorithm. All the video sequences are uncompressed format. Five videos are identified as akiyo, xylophone, foreman, soccer and football as shown in Figure 3.

![Figure 3](image-url)  

(a) Akiyo, (b) Xylophone, (c) Foreman, (d) Soccer, (e) Football

This experiment evaluates hiding capacity with various amounts of message bits toward the quality of stego-video and the robustness of hidden data against video compression. Table 1 shows the experimental
results of the proposed scheme in terms of MPSNR and MARE. The proposed scheme is tested under various amounts of hidden data. The MPSNR values of the proposed scheme are shown in Figure 4.

Table 1. Comparison of mean absolute reconstruction error from the proposed scheme

| Video   | Frame | Motion | 800 bits | 3200 bits | 4800 bits |
|---------|-------|--------|----------|-----------|-----------|
| Akiyo   | 300   | 1742   | 0.0042   | 0.0149    | 0.0321    |
| Xylophone | 140   | 1067   | 0.0076   | 0.0310    | 0.0935    |
| Foreman | 300   | 779    | 0.0023   | 0.0105    | 0.0336    |
| Soccer  | 260   | 802    | 0.0037   | 0.0140    | 0.2829    |
| Football| 600   | 898    | 0.0069   | 0.0136    | 0.0307    |
| Coastguard | 1199 | 587    | 0.0008   | 0.0032    | 0.0099    |
| Mobile  | 300   | 586    | 0.0063   | 0.0231    | 0.0679    |
| Waterfall | 260   | 585    | 0.0040   | 0.0157    | 0.0486    |
| Flower  | 250   | 553    | 0.0021   | 0.0074    | 0.0211    |
| Bus     | 150   | 578    | 0.0060   | 0.0240    | 0.0824    |

Figure 4. MPSNR value obtained from Akiyo, Foreman, Carphone, and Bus

Embedding with minimum hidden data produces a good quality of stego-video. Meanwhile, embedding large hidden data produces slightly small distortion of stego-video. Referring to Table 1, the proposed scheme produces slightly pixel distortion, the quality of stego-video is closer to the original video data. Our scheme maintains the visual quality with the PSNR value of 50 dB. The embedding capacity of hidden data depends on the number of detecting motion in the video data. The proposed scheme does not suitable for videos which have minimum object motion. The robustness evaluation of the proposed steganography scheme against video compression is listed in Table 2.

Table 2. Comparison of BER and NC values of the proposed method against video compression

| Video   | Frame | Motion | MBER  | MNC   |
|---------|-------|--------|-------|-------|
| Akiyo   | 300   | 1742   | 0.3075| 0.8930|
| Xylophone | 140   | 1067   | 0.1575| 0.9180|
| Foreman | 300   | 779    | 0.2925| 0.8994|
| Soccer  | 260   | 802    | 0.0700| 0.9520|
| Football| 600   | 898    | 0.0975| 0.9400|
| Coastguard | 1199 | 587    | 0.0988| 0.9531|
| Mobile  | 300   | 586    | 0.0462| 0.9621|
| Waterfall | 260   | 585    | 0.0988| 0.9531|
| Flower  | 250   | 553    | 0.0462| 0.9621|
| Bus     | 150   | 578    | 0.1313| 0.9173|

Video steganography based on DCT psychovisual... (Muhammad Fuad)
The proposed scheme is designed to be robust against the video compression method. Videos have been widely transferred with compressed data due to limited transfer bandwidth. The proposed embedding technique based on DCT-psychovisual produces potentially resistant of the hidden data against compressed video. Our technique demonstrates it is hiding capacity and robustness against MPEG compression.

6. CONCLUSION

This paper proposes a new hiding technique based on DCT psychovisuval for concealing the message in the object motion among the scene change. This space can be utilized to conceal the secret-message which is imperceptible to the human visual system. The selected frames based on object motion are embedded using a new embedding algorithm based on psychovisual threshold. The message is concealed by examining the certain DCT coefficients in the middle frequencies using a certain proposed rules. The experimental results show that our data-hiding technique enhances the quality of video with hidden data and attains robustness of the concealed message. The proposed scheme achieves high imperceptibility of the stego-video. The proposed hiding technique for concealing secret-message provides robustness withstand video compression.

ACKNOWLEDGEMENTS

This work was supported by Fundamental Research Grant Scheme (FRGS) No. RDU190117 and Postgraduate Research Grants Scheme (PGRS) No.1903890 from Universiti Malaysia Pahang, Malaysia.

REFERENCES

[1] A. Kamel, et al., “Automatic security policy enforcement in computer systems,” Computer and Security,” vol. 73, pp. 156-171, 2018.
[2] N. Zarmehi and M. A. Akhace, “Digital video steganalysis toward spread spectrum data hiding,” IET Image Processing,” vol. 10, no. 1, pp. 001-008, 2016.
[3] K. Dasgupta, et al., “Optimized video steganography using Genetic Algorithm (GA),” Procedia Technology, vol. 10, pp. 131-137, 2013.
[4] M. Liśkiewicz, et al., “Security levels in steganography insecurity does not imply detectability,” Theoretical Computer Science, vol. 692, pp. 25-45, 2017.
[5] M. Ramalingam and N. A. M. Isa, “A data-hiding technique using scene-change detection for video steganography,” Computer and Electrical Engineering, vol. 54, pp. 423-434, 2016.
[6] H. Ghasemzadeh, et al., “Audio steganalysis based on reserved psychoacoustic model of human hearing,” Digital Signal Processing, vol. 51, pp. 133-141, 2016.
[7] M. Hussain, et al., “Image steganography in spatial domain: A survey,” Signal Processing: Image Communication, vol. 65, pp. 46-66, 2018.
[8] N. N. El-Emam and M. Al-Diabat, “A novel algorithm for colour image steganography using a new intelligent technique based on three phases,” Applied Soft Computing, vol. 37, pp. 830-846, 2015.
[9] W. Hong and T.S. Chen, “A novel data embedding method using adaptive pixel pair matching,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 1, pp. 176-184, 2012.
[10] H. Zhang, et al., “A steganalytic approach to detect motion vector modification using near-perfect estimation for local optimality,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 2, pp. 465-478, 2017.
[11] F. Erwanaw, et al., “An efficient image compression technique using thelenamefet allocation,” Optik-International Journal for Light and Electron Optics, vol. 148, pp. 106-119, 2017.
[12] L. Gao, et al., “Reversible watermarking in medical Image using RDWT and sub-sample,” International Journal of Digital Crime and Forensics, vol. 7, no. 4, pp.1-18, 2015.
[13] M. Hashemzadeh, “Hiding information in videos using motion clues of feature points,” Computers and Electrical Engineering, vol. 68, pp. 14-25, 2018.
[14] R. J. Mstafula, et al., “A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC,” IEEE Access, vol. 5, pp. 5354-5365, 2018.
[15] M. M. Sadek, et al., “Robust video steganography algorithm using adaptive skin-tone detection,” Multimedia Tools and Applications, vol. 76, no. 2, pp. 3065-3085, 2017.
[16] M. Dalal and M. Juneja, “Video steganography techniques in spatial domain-A survey,” Proceedings of the International Conference on Computing and Communication Systems, vol 24, pp. 705-711, 2018.
[17] H. Al-Dmour and A. Al-Ami, “A steganography embedding method based on edge identification and XOR coding,” Expert Systems with Applications, vol. 46, pp. 293-306, 2016.
[18] T. Idbeaa, et al., “A secure and robust compressed domain video steganography for intra and inter-frames using Embedding-Based Byte Differencing (EBBBBD) Scheme,” Plos One, vol. 11, no. 3, pp. 1-22, 2016.
[19] M. Ramalingam and N. A. M. Isa, “Fast retrieval of hidden data using enhanced hidden markov model in video steganography,” Applied Soft Computing, vol. 34, pp. 744-757, 2015.
[20] K. B. Sudeepa, et al., “A new approach for video steganography based on randomization and parallelization,” Procedia Computer Science, vol. 78, pp. 483-490, 2016.
[21] N. Kar, et al., “Improved chaos-based video steganography using DNA alphabets,” *ICT Express*, vol. 4, pp. 6-13, 2018.
[22] C. Xu, et al., “Steganography in compressed video stream,” *Proceedings of the First International Conference on Innovative Computing, Information and Control*, pp. 1-4, 2006.
[23] Z. Gao and G. Zhai, “Dual-view display based on spatial psychovisual modulation,” *IEEE Access*, vol. 6, pp. 41356-41366, 2018.
[24] A. J. Hussain, et al., “Image compression techniques: A Survey in Lossless and Lossy Algorithms,” *Neurocomputing*, vol. 300, pp. 44-69, 2018.
[25] F. Ernawan, et al., “Bit allocation strategy based on psychovisual threshold in image compression,” *Multimedia Tools and Applications*, vol. 77, no. 11, pp. 1-24, 2017.
[26] F. Ernawan and M. N. Kabir. “A robust image watermarking technique with an optimal DCT-Psychovisual threshold,” *IEEE Access*, vol. 6, pp. 20464-20480, 2018.
[27] F. Ernawan, et al., “A blind multiple watermarks based on human visual characteristics,” *International Journal of Electrical and Computer Engineering*, vol. 8, no. 4, pp. 2578-2587, 2018.
[28] F. Ernawan and D. Aritmanto, “Image watermarking based on integer wavelet transform-singular value decomposition with variance pixels,” *International Journal of Electrical and Computer Engineering*, vol. 9, no. 3, pp. 2185-2195, 2019.
[29] F. Ernawan, “Tchebichef image watermarking along the edge using YCoCg-R color space for copyright protection,” *International Journal of Electrical and Computer Engineering*, vol. 9, no. 3, pp. 1850-1860, 2019.
[30] Video Trace Library, Arizona State University, [Online]. Available: http://trace.eas.asu.edu/yuv/, 2019.

**BIOGRAPHIES OF AUTHORS**

Fuad Abdullah was born in Pahang, Malaysia, in 1991. He received the bachelor’s degree in Graphic and Multimedia from Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang in 2017. He is currently pursuing the master’s degree in computer science from Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang. His research interests include information hiding and video coding.

Ferda Ernawan was born in Semarang, Central Java, Indonesia, in 1988. He received the master’s degree in software engineering and intelligence and the Ph.D. degree in image processing from the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka in 2011 and 2014, respectively. He is currently a Senior Lecturer with the Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang. His research interests include image compression, digital watermarking and steganography.