A Novel Secure Video Steganography Technique using Temporal Lifted Wavelet Transform and Human Vision Properties

Ahmed Thahab

Department of Electrical and Electronic Engineering, University of Babylon, Iraq

Abstract: *Steganography is a term that refers to the process of concealing secret data inside a cover media which can be audio, image and video. A new video steganography scheme in the wavelet domain is presented in this paper. Since the convolutional discrete wavelet transform produces float numbers, a lifted wavelet transform is used to conceal data. The method embeds secret data in the detail coefficients of each temporal array of the cover video at spatial localization using a unique embedding via YC_bC_r color space and complementing the secret data to minimize error in the stego video before embedding. Three secret keys are used in the scheme. Method's performance matrices such as peak signal to noise ratio and Normalized Cross Correlation (NCC) expresses good imperceptibility for the stego-video. The value of Peak Signal to Noise Ratio (PSNR) is in range of 34-40dB, and high embedding capacity.*

Keywords: *Data hiding, integer wavelets transform, color space, peak signal to noise ratio, first complement.*

1. Introduction

Steganography is a technique known to conceal secret data inside a cover media without being detectable to hackers. The technique conceals the fact that a message exists in the cover media and sends the message to the receiver-side [18]. Unlike cryptography, that manipulates secret message to be indefinite to hackers unless a possession of a decryption key [5, 16].

Steganography algorithms explore maximum amount of redundancy from the cover media in order to embed secret data. Embedding message data inside a cover media will introduce distortion to the cover media after embedding which is known as "Stego" [17, 22]. The amount of distortion must be at minimum levels and visually imperceptible [15]. Other essential evaluating factors such as capacity, security, quality and complexity are also essential factors to assess steganography algorithms. Capacity refers to the amount of message data that can be embedded inside the cover media [3], while quality refers to the distortion introduced to the stego compared to the original cover with respect to the amount of message data. In addition to quality, the embedded data should be concealed in a method that does not permit direct access [17, 19, 20]. The cover media can be audio, image and video media's. Secret data embedded in an image cover is called "Image Steganography". Image Steganography has been a field of interest for researchers and various proposed methods for embedding algorithms are presented to enhance security, capacity and quality.

Karim *et al.* [13] suggested a technique in an effort to enhance security. The secret data is embedded in the cover media using different positions depending on a secret key. In spite of attaining a maximum Peak Signal to Noise Ratio (PSNR) of 53.78dB and a good security, the method ignores the factor of capacity of secret data embedded in cover media. Hossain *et al.* [10] proposed an efficient stenographic digital image method. Since the images contain smooth and edged zones, a fixed number of bits are embedded in the smooth areas while variable lengths of bits are embedded in edged zones of the image. The method introduces some artifacts to the stego-image which arouses suspicion of secret embedding.

Video steganography is advantageous than other types of media's since video signal possess ample redundancy in the spatial and temporal domain which is essential for embedding data, in addition, video steganography is more secure than image steganography since secret data is dispersed in numerous frames depending on the length of the video cover media. Video steganography can be used in the spatial domain excluding a utilization of a signal transform. Gupta and Chaturvedi [9] suggested a combination of the least significant bit algorithm and an encryption standard algorithm. The method uses one of the three key lengths 128, 192 or 256 bits to make it difficult for hackers to suspect the existence of data inside the stego video. Jue *et al.* [11] proposed a video steganography based on motion vectors. The algorithm

selects motion vector macro blocks as carriers and the embedding capacity is controlled by the design of the motion vectors. The algorithm also takes into account the human visual system to increase embedding capacity. The main drawback of the algorithm is the use of search algorithms for motion detection. Mstafa and Elleithy [17] proposed a steganography method based on the hamming code principle. Before the operation of embedding, the secret message is encoded using hamming code and then Exclusive-OR (XOR) with random values. A private key is utilized to randomly reorder the pixel positions. The algorithm is based on spatial embedding which is considered fragile in terms of security. Dasgupta *et al.* [6] proposed a video steganography technique that uses genetic algorithm to optimize and modify embedded coefficients using a particular cost function. The embedding scheme uses 3-3-2 least significant bit embedding scheme. Other domains can be used for embedding such as frequency domain in order to increase security and noise immunity [14]. Recent papers use signal transformation such as Discrete Wavelet Transform (DWT) on video cover to exploit redundancy and conceal data Chantrapornchai *et al.* [4] and Euphrasi and Rani [8] proposed a video steganography that hides an image using lifted multi-level wavelet transform. A wavelet transform is applied on the video sequence and secret image. Secret image coefficients are hided in frames that contain similar pixels. Most techniques utilize DWT in the spatial domain without considering that video data is highly correlated in the temporal domain and ample redundancy exists among video frames. Applying DWT in the temporal domain of a video media will produce low magnitude high frequency coefficients which are known as the detail band; therefore, secret data is embedded in high frequency coefficients resulting low errors between cover and stego coefficients. In this paper, a video steganography algorithm is proposed using a cover video media. The algorithm utilizes the Human Visual System (HVS) since the human eye are sensitive to the intensity layer than the two color layers C_b and C_r, therefore; the YC_bC_r color space is used instead of RGB. A lifted wavelet transform is used to localize frequency bands. The rest of the paper organized as follows: section two describes the integer wavelet transform. Section three explains the hiding and extraction algorithm while section four illustrates the results of some tests for the proposed steganography algorithm and comparison with the related algorithms. Section five illustrates a comparison with other algorithms and finally section six states the conclusion

2. Integer Wavelet Transform

The Integer wavelet transform is considered as a more rapid transform than the discrete wavelet transform [7].

All coefficients produced from the transform are integer since the transform uses a function that finds the largest or equal value to the resulting float, therefore; it is termed as Integer Wavelet Transforms (IWT). When applying a one dimension of IWT on an array of values [*V*], two bands of frequencies are produced, an average of values produces smooth coefficients that possess the low frequency content called "Approximation band" (A_b) and a method of difference of values that possess the high frequency content called "Detail band"(D_b). Equations (1), (2), and (3) represent these operations [21]:

$$V_j\ (e),\ V_j\ (O) \tag{1}$$

$$D_{b(j-1)} = V_j\ (0) - floor\ (P\ \{V_j(e)\}) \tag{2}$$

$$A_{b(j-1)} = V_j\ (e) + floor\ (U\ \{S_j\ (o)\}) \tag{3}$$

Where: $V_j\ (e)$, $V_j\ (O)$: are the even and odd splitted pixels. *P* and *U*: are the prediction and updating function depending on the wavelet family used.

   A_b coefficients are delicate coefficients for the image representation while D_b coefficients contain information regarding the edges of an image. Operation in Equation (2) explains that detail band coefficients results from a difference operation, therefore; the difference between a value and its prediction is equal to zero. This property can be utilized the video steganography operation.

3. Video Steganography Algorithm

In this section, a description of the proposed video steganography algorithm for hiding and recovering secret data is presented. The reason behind the selection of a video as cover media is the embedding capacity of a video since a colour video is a four dimension signal. In order to exploit redundancy in the video signal, wavelet transform is applied in either of domains spatial domain or temporal domain. Applying DWT transform on a smooth (non-fluctuating) one dimension array, produces a detail band coefficients which are least in values than applying on a non-smooth array, this can be illustrated in the following example:
If DWT is applied on vectors [*V*]*and [Q]* $\in R^+$, where: V= [100 12 60 400 20 1], and Q= [10 12 20 30 20 10]. The approximation band (A_{bv}) and detail band (D_{bv}) resulted for applying DWT on vector [V]:
A_{bv}= [79.1960 325.2691 14.8492]
D_{bv}= [62.2254 -240.4163 13.4350]
 While for vector [Q], the detail and approximation:
A_{bq} = [15.5563 35.3553 21.2132]
D_{bq} = [-1.4142 -7.0711 7.0711]
The detail float coefficients produced from vector [*V*] are high in magnitude than detail float coefficients produced from the transform in vector [*Q*]. It is observed that the output of convolution DWT produces detail band coefficients that are:

- High in magnitude when the input vector is fluctuating.
- Float numbers which are produced from converting 8-bits unsigned integer pixels into float coefficients.

In order to overcome the mentioned conclusions, the vector input should possess non-fluctuating values in order to produce low magnitude detail coefficients and a lifting scheme is applied to produce an integer to integer transform of the same spatial pixel resolution. A temporal embedding scheme is proposed using Lifted Wavelet Transform (LWT) as illustrated in Figure 1. Video frame sequences are highly correlated, therefore; similar temporal values are identical throughout the video sequence excluding sequence change and limited motion. Therefore, the detail coefficient (D_b) of the integer to integer wavelet transform is negligible.

Consider the vector [234, 234, 234, 234, 234, 234], according to Equation (2) the detail coefficients of IWT are [0, 0, 0].

Secret data can be embedded in high frequency content band resulting less distortion. However; scene change of video cover media is crucial to performance assessment parameters of the algorithm, therefore; video sequence is separated to scenes. The mechanism proposed in this paper to split image sequences to scenes (group of frames) is the third moment of statistics "Skewness".

Skewness measures the asymmetry of the measuring data around the mean value. If the skewness of data is negative, an intuition that data is spread to the left. While positive value reflects that data is spread to the right [23]. The video input to the algorithm is splited into frames, if absolute skew difference of the Y component of current frame and previous frame is higher than a value of threshold (T_d), a new scene has emerged as in Equation (4):

$$\left| I_s^{f+1} - I_2^f \right| \geq T_d \qquad (4)$$

Where: I_s skewness of a frame, f: frame index. Creating group of sequences for embedding. A basic and famous embedding technique which is widely used steganography is the Least Significant Bit (LSB) technique [12]. In a certain byte of bit stream, the immediate left of a byte stream is known as Most Significant Bit (MSB), while the immediate right is known as LSB. Altering the least significant bit of a bit stream, a minor change will take place for the value of byte. An example below illustrate the LSB technique, an 8-bit codeword representation of a decimal value $(200)_{10}$ is $[11001000]_2$, if two bits $[10]_2$ are embedded in the LSB 8-bit codeword, results $[11001010]_2$ which yield to a decimal value of $(202)_{10}$. Embedding the same two bits in the MSB of the 8-bit codeword $[10001000]_2$ yield to $(136)_{10}$. Therefore; embedding in the LSB is more distortion less than embedding in the MSB. The conventional LSB is fragile to security hacking since secret codewords are directly embedded. Embedding complemented code words of secret data in the cover data media reduces the error between the stego video and cover pixels and robust the security of the technique. An example of the technique is illustrated:
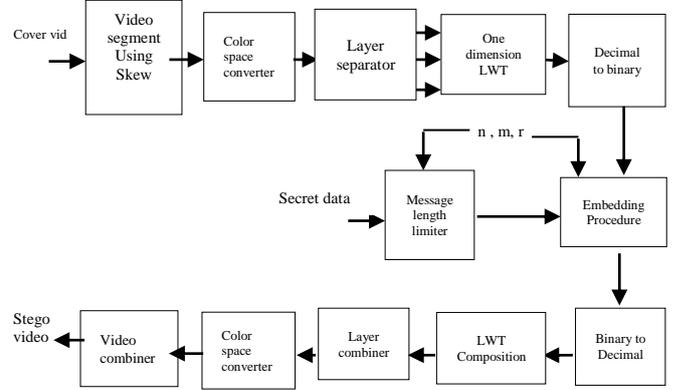
Figure 1. Block diagram of the proposed color video.

The cover binary value is $[10010110]_2$ and a secret code word of $[1010]_2$ is required to be embedded. Directly embedding the data $[10011010]_2$ results in a value of $(154)_{10}$, while embedding the complemented data $[0101]_2$ in the cover binary value $[10010101]_2$ results a value of $(149)_{10}$. For this example, an error of four units is reduced in the output when utilizing the complemented value of the secret bit stream. This will eventually decrease the stego-output distortion and increase quality. The embedding and extracting process of embedding algorithm is detailed below:

a. *Embedding Process*:

1. Convert each frame of the RGB to YC_bC_r color space and collect all Y, C_b and C_r layers individually of cover video.

$$Z_1 = Y_1 \cup Y_2 \cup Y_3 \ldots\ldots\cup Y_{le} \qquad (5)$$

$$Z_2 = C_{b1} \cup C_{b2} \cup C_{b3} \ldots\ldots\cup C_{ble} \qquad (6)$$

$$Z_3 = C_{r1} \cup C_{r2} \cup C_{r3} \ldots\ldots\cup C_{rle} \qquad (7)$$
$$le: \text{length of video.}$$

2. Apply a one dimension "Haar" lifted wavelet transform on each of the collected three dimension matrices Z_1, Z_2, Z_3:

$$S(Z_x)^f = IWT\{Z_{x_{(i,j,k+1)}}, \ldots\ldots, Z_{x_{(i,j,k+L)}}\}^f \qquad (8)$$

Where: S: one dimension array, f: frame index.

3. Preserve the sign of the detail coefficients of the cover frame video in a sign map and convert each coefficient to 8-bit binary value.

4. Extract (n) bits of secret data:

If: The value of (n) bit data $\geq 2^n/2$; Take the first complement for (n) bit data and embed the complemented data in the detail band coefficient of the Y layer by LSB technique.

Else: Embed (n) bits of secret data in the binary data of the Y layer detail band coefficient by LSB technique.

5. Extract (*m*) bits of secret data:

If: The value of (*m*) bit data $\geq 2^m/2$;

Take the first complement for (*m*) bit data and embed the complemented data in the detail band coefficient of the C_b layer by LSB technique.

Else: Embed (*m*) bits of secret data in the binary data of the C_b layer detail band coefficient by LSB technique.

6. Extract (*r*) bits of secret data:

If: The value of (*r*) bit data $\geq 2^r/2$;

Take the first complement for (*r*) bit data and embed the complemented data in the detail band coefficient of the C_r layer by LSB technique.

Else: Embed (*r*) bits of secret data in the binary data of the C_r layer detail band coefficient by LSB technique.

7. Reintegrate the sign map with the detail coefficients and apply inverse LWT to the embedded one dimension array of each color layer and separate the components to their original frames.

8. Convert the color space of the stego video frames to RGB color space and reproduce the stego video.

b. *Extraction Process*:

Parameters n, m, and r are secret keys that should be known to the receiver in order to extract the secret data from cover video.

1. Convert RGB to YC_bC_r color space and collect the Y, C_b and C_r layers of the stego video.
2. Locate temporal arrays and apply a one dimension "Haar" LWT on each one dimension array at (x, y) location for each matrix.
3. Convert the detail coefficients to binary.
4. Retrieve: n bit secret data stream, from Y stego bit stream, m bit secret stream from C_b stego bit stream, r bit secret stream from C_r stego bit stream.
5. Invert the (n),(m), and (r) bits:

 If: The inverted bits $\geq 2^n/2$, $2^m/2$, $2^r/2$ respectively, reproduce the inverted bits as secret data
 Else: Reproduce the extracted bits as secret data.

4. Results and Discussion

The method is experimented using various color cover video of size (128*128) and (256*256) using Matlab R2014b. The performance is assessed in terms of PSNR given in Equation (9) [2]. The Average peak signal to noise ratio (APSNR) for the complete video is given in Equation (10). The NCC is given in Equation (11) [2] for each frame of the stego video and averaging for the complete stego-video.

$$(PSNR)^f = 10\log_{10}\frac{255^2}{\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\left(I(i,j)-\bar{I}(i,j)\right)} \quad (9)$$

$$APSNR = \frac{PSNR^1 + PSNR^2 + \dots + PSNR^{l_e}}{le} \quad (10)$$

$$(NCC)^f = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\left(I(i,j)\bar{I}(i,j)\right)}{\sum_{i=1}^{N}\sum_{j=1}^{M}I(i,j)^2} \quad (11)$$

Where: *N* and *M* dimension of video, *I*: original frame, $\bar{I}$: stego-frame, n:number of frames. Various values of thresholding for splitting video scenes to sequence of images where used, the preferable value used during experiments is $T_d =0.01$ and "Haar" filter is used for integer wavelet transform. Experiments are conducted on a 2GB RAM and 2GHz core duo processor and results for the video quality and capacities are shown in Table 1.

Table 1. Shows the practical results for the algorithm with various videos clips.

(Video Name) 100 frames	Payload in bits	m	n	r	APSNR in dB	NCC
Container 128*128	4102528	1	1	4	37.898	0.999
	7372800	3	2	4	36.436	1.000
	8192000	4	2	4	33.574	1.000
Highway 128*128	4102528	1	1	4	40.776	0.998
	7372800	3	2	4	38.905	0.998
	8192000	4	2	4	35.463	0.997
Paris 256*256	4102528	1	1	4	37.576	0.999
	7372800	3	2	4	36.747	1.000
	8192000	4	2	4	33.530	1.000
Xyphone 256*256	4102528	1	1	4	36.477	1.000
	7372800	3	2	4	36.020	1.000
	8192000	4	2	4	35.249	1.000
Barcode 128*128	4102528	1	1	4	36.883	1.000
	7372800	3	2	4	36.883	1.000
	8192000	4	2	4	36.012	1.000
Ice 128*128	4102528	1	1	4	39.736	0.998
	7372800	3	2	4	39.081	0.998
	8192000	4	2	4	38.066	0.997
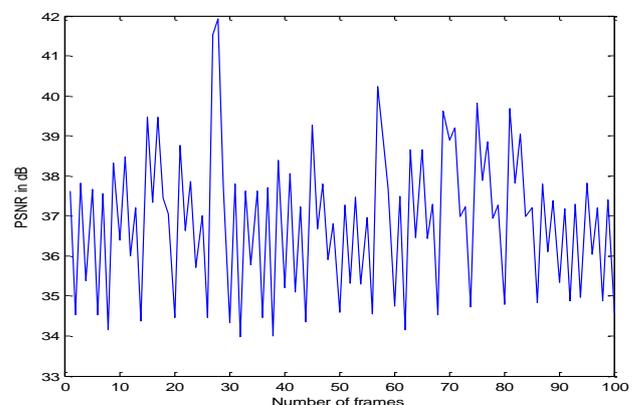
Figure 2. PSNR for each frame for barcode video.

a) Original 39th frame.   b) Original 68th frame.

c) Stego 39th frame.   d) Stego 68th frame.
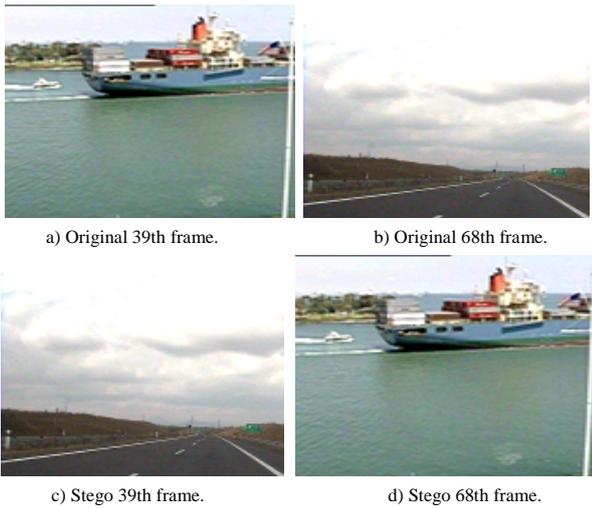
Figure 3. Stego and original frames for container and highway for m=4, n=2, r=4.

a) Original 30th frame.   b) Stego30th frame.
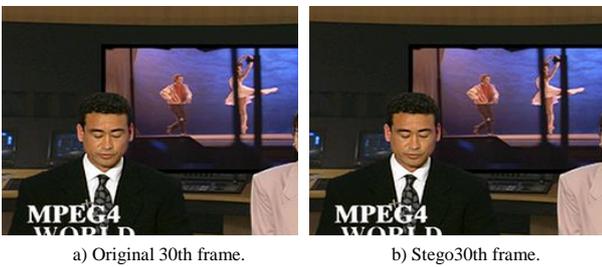
Figure 4. Frames of news cover media for m=4, n=2, r= 4.

a) Moving picture quality: Generally a value of PSNR above 30dB is considered as undistinguishable for the human eye [1]. The quality of the stego-video in terms of PSNR is in the range of (34-40 dB) and NCC is ranging (1-0.99) for the experiments. This imposes that the algorithm preserves visual and statistical quality of the cover media and that stego-video does not arouse suspicion about secret data being hidden in the cover media.

a) Original 30th frame.   b) Stego30th frame.
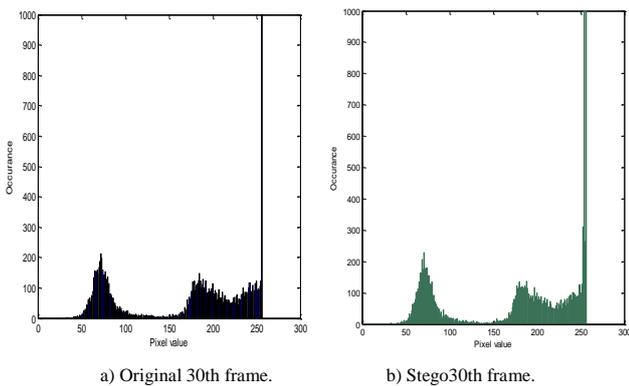
Figure 5. Histogram for stego and original frame video for m=3, n=2, r=4.

Another factor imposes video steganography performance is stego video frames ought to be highly correlated as distortion among video frames causes suspicion of hidden data. Figure 2 Illustrates that all stego-video frames are visually correlated since the proposed algorithm embeds complemented data in the

temporal domain and correlated arrays at specific spatial points for a group of scene frames are resulted.

Figures 3 and 4 illustrates sample frames of visual correlation between the stego-video and cover video frame for two experiments. However, decreasing the number of bits n and *m*, and *r*, increases the PSNR which highly correlates stego video frames with cover frames. A histogram analysis for the original and cover frame is illustrated in Figure 5 which presents a highly matching distribution of pixels between the cover and stego video.

b) Capacity: The capacity of the algorithm is defined as the number of bits that are embedded in a cover media [2]. The number of bits embedded in video cover for the proposed algorithm is depended on the number of bits embedded in the component color space and video length as in Equation (12):

$$payload = Num_{\det(i)y} * n * size(Z_1) + Num_{\det(i)Cb} * m$$
$$* size(Z_2) + Num_{\det(i)Cr} * r * size(Z_3) \qquad (12)$$

Bits embedded in a single frame are variable between three color components Y, C_b, and C_r, (n, m, r) are number of bits embedded in Y, C_b and C_r components respectively. The algorithm exploits good capacity as illustrated in Table 1, since the error resulting from embedding complemented bits are less compared to the original frame.

c) Security: Embedding secret data in wavelet domain of the cover media produces a good security strategy. The embedding procedure of complemented or uncomplemented secret data in YC_bC_r color space depends randomly on the value of the secret data for the color layers, in addition to the number of bits (keys) embedded in the coefficient of layers.

5. Performance Comparison

The proposed algorithm performance is compared with other work in video steganography field. The technique in [11] embeds random data in video sequences and the visual quality is assessed by PSNR. Table 2 shows the stego video quality in terms of PSNR. An Average of PSNR (APSNR) is calculated for the scenes.

Table 2. Result comparison of APSNR between proposed algorithm and [11] with various videos clips.

Video name	Frame number	APSNR in proposed	APSNR in [11]
Mother& Daughter	(1:45) (45:90)	47.5255	38.452
Container	(1:40) (81:120)	46.8169	36.276
Mobile	(1:50) (101:150)	46.6253	34.227

The proposed algorithm is also compared to work in [6, 17]. Authors' in [17] concealed a 150*150 resolution secret message inside a cover video in avi video format, while [6] concealed a binary image of resolution size 128*128 inside various video

sequences. The APSNR is determined for three video sequences in Tables 2 and 3. The tables show a comparison in terms of visual quality between [6, 17] and the proposed algorithm. From Tables 2, 3, and 4, the proposed algorithm is superior over [6, 11, 17] in terms of visual quality since distortion is decreased using the complemented bits and embedding in the detail coefficients of the temporal domain.

Table 3. Result comparison of PSNR between proposed algorithm and [17] with various videos clips.

Video name	APSNR in proposed	APSNR in [17]
Container	53.8122	52.0328
Mother and Daughter	62.3307	51.8454
Mobile	54.1996	52.0003

Table 4. Result comparison of APSNR between proposed algorithm and [6] with various videos clips.

Video name	APSNR in proposed	APSNR in [6]
Tree.avi	48.1456	39.37
Globe.avi news	48.5176	34.37
Computer.avi	47.7017	41.61

6. Conclusions

A new method for video steganography is proposed using temporal embedding. Applying integer to integer wavelet transform on correlated vector arrays produces an integer eight bit resolution coefficient and detail coefficients are less in magnitude values which contributes to an excellent embedding position for secret data. The algorithm obtains a high carrier capacity with a good visual quality because embedding is based on the principle that Human Vision System (HVS) is more sensitive to the intensity layer than the color layers; therefore, more bits are embedded in the color layers than the intensity layers by complementing high secret values. User defines the number of bits that can be embedded in the cover video with the variables (n, m and r). This work can be developed to embed secret image data or secret video data inside the cover video using a random embedding strategy.

The proposed video steganography efficiency is limited to determining the non-linear of the temporal arrays; therefore, defining optimum boundaries of groups in temporal arrays improve visual quality of the stego-output. Fragmenting temporal arrays into smaller group of arrays can contribute to increase visual and statistical quality. In order to increase protection of secret data from eavesdroppers, encryption can be used to encrypt secret data before embedding.

References

[1]   Abbas S., El-Arif T., Ghaleb F., and Khami S., "Optimized Video Steganography Using Cuckoo Search Algorithm," *in Proceedings of IEEE 7th International Conference on Intelligent Computing and Information Systems*, Cairo, pp. 572-577, 2015.

[2]   Al Korbi H., Al-Ataby A., Al-Taee M., and Al-Nuaimy W., "High-Capacity Images Steganography Based on Haar DWT for Hiding Miscellaneous Data," *in Proceedings of IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies*, Amman, pp. 1-6, 2015.

[3]   Al-Ataby A. and Al-Naima F., "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform," *The International Arab Journal Information Technology*, vol. 7, no. 4, pp. 358-364, 2010.

[4]   Chantrapornchai C., Churin K., Preechasuk J., and Adulkasem S., "Video Steganography for Hiding Image with Wavelet Coefficients," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 9, no. 6, pp. 385-396, 2014.

[5]   Chanu Y., Tuithung T., and Singh K., "A Short Survey on Image Steganography and Steganalysis Techniques," *in Proceedings of 3rd National Conference on Emerging Trends and Applications in Computer Science*, Shillong, pp. 52-55, 2012.

[6]   Dasgupta K., Mondal J., and Duttac P., "Optimized Video Steganography using Genetic Algorithm," *Procedia Technology*, vol. 10, pp. 131-137, 2013.

[7]   EI-Safy R., Zayed H., and EI-Dessouki A., "An Adaptive Steganographic Technique Based on Integer Wavelet Transform," *in Proceedings of International Conference on Networking and Media Convergence*, Cairo, pp. 111-117, 2009.

[8]   Euphrasi K. and Rani M., "A Comparative Study on Video Steganography in Spatial and IWT Domain," *in Proceedings of IEEE International Conference on Advances in Computer Applications*, Coimbatore, pp. 104-109, 2016.

[9]   Gupta H. and Chaturvedi S., "Video Steganography through LSB Based Hybrid Approach," *International Journal of Engineering Research and Development*, vol. 6, no. 12, pp. 32-42, 2014.

[10]   Hossain M., Al Haque S., and Sharmin F., "Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Information," *The International Arab Journal of Information Technology*, vol. 7, no. 1, pp. 34-38, 2009.

[11]   Jue W., Zhang M., and Sun J., "Video Steganography Using Motion Vector Components" *in Proceedings of IEEE 3rd International Conference on Communication Software and Networks*, Xi'an, pp. 500-503, 2011.

[12] Juneja M. and Sandhu P., "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption," *in Proceedings of International Conference on Advances in Recent Technologies in Communication and Computing*, Kottayam, pp. 302-305, 2009.

[13] Karim S., Rahman M., and Hossain M., "A new Approach for LSB Based Image Steganography Using Secret Key," *in Proceedings of 14th International Conference on Computer and Information Technology*, Dhaka, pp. 286-291, 2011.

[14] Kumar V. and Kumar D., "Performance Evaluation of DWT Based Image Steganography," *in proceedings of IEEE 2nd International Advance Computing Conference*, Patiala, pp. 223-228, 2010.

[15] Mishra M., Tiwari G., and Yadav A., "Secret Communication using Public key Steganography," *in Proceedings of IEEE International Conference on Recent Advances and Innovations in Engineering*, Jaipur, pp. 9-11, 2014.

[16] Moon S. and Raut R., "Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data Security," *in Proceedings of IEEE 2nd International Conference on Image Information Processing*, Shimla, pp. 660-665, 2013.

[17] Mstafa R. and Elleithy K., "A Highly Secure Video Steganography Using Hamming Code (7, 4)," *in Proceedings of IEEE Long Island Systems, Applications and Technology Conference*, Farmingdale, pp. 1-6, 2014.

[18] Rajalakshmi K. and Mahesh K., "Video Steganography Based on Embedding the Video Using PCF Technique," *in Proceedings of International Conference on Information Communication and Embedded Systems*, Chennai, pp. 1-4, 2017.

[19] Ramalingam M. and Isa N., "A Steganography Approach over Video Images to Improve Security," *Indian Journal of Science Technology*, vol. 8, no. 1, pp. 79-86, 2015.

[20] Ramaswamy R. and Arumugam V., "Lossless Data Hiding based on Histogram Modification," *The International Arab Journal of Information Technology*, vol. 9, no. 5, pp. 445-451, 2012.

[21] Shahadi H., Thahab A., and Ali M., "Adaptive Embedding Approach in Color Image Carrier for Covert Communication," *Indian Journal of Science and Technology*, vol. 9, no. 46, pp. 1-11, 2016.

[22] Swain G. and Lenka S., "A Novel Approach to RGB Channel Based Image Steganography Technique," *The International Arab Journal of E-Technology*, vol. 2, no. 4, pp. 181-186, 2012.

[23] Yusoff S. and Wah Y., "Comparison of Conventional Measures of Skewnwss and Kurtosis for small Sample Size," *in Proceedings of International Conference on Statistics in Science, Business and Engineering*, Langkawi, pp. 1-6, 2012.

Ahmed Thahab received his B.Sc in Electrical Engineering from the University of Babylon and M.Sc from the University of Babylon in 2011 in Electronic and Communication Engineering. Currently he is a faculty member in the University of Karbala. His research interest is in video, image processing and Information security.