Bulletin of Electrical Engineering and Informatics
Vol. 11, No. 4, August 2022, pp. 1959~1969
ISSN: 2302-9285, DOI: 10.11591/eei.v11i4.2922

High capacity video hiding based on multi-resolution stationary wavelet transform and hybrid-matrix decomposition techniques

Reham A. El-Shahed, Maryam N. Al-Berry, Hala M. Ebied, Howida A. Shedeed
Department of Scientific Computing, Faculty of Computer and Information Sciences, Ain Shams University, Cairo, Egypt

Article Info

Article history:

Received Feb 27, 2021
Revised May 2, 2022
Accepted Jun 1, 2022

Keywords:

Data hiding
QR factorization
Singular value decomposition
Stationary wavelet transform
Steganography

ABSTRACT

Internet simplified digital data transferring. This data needs to be secured; so securing digital data becomes an important concern. Steganography provides security for data by inserting it into a cover and concealing it. In this paper, a steganography algorithm was introduced. This algorithm used the stationary wavelet transform (SWT) and hybrid-matrix decomposition techniques, singular value decomposition (SVD) and QR factorization to conceal a video in another video. The algorithm performance was measured with reference to the peak signal to noise ratio (PSNR) and structural similarity index measure (SSIM) for the cover and the secret videos. The algorithm successfully hid a video in another cover video and both are of the same size; the hiding capacity was 100%. The algorithm achieved a SSIM that reached 0.97 and a high PSNR value that reached 68.8 proving that the imperceptibility of the proposed algorithm is very high. The comparative analysis shows that the suggested algorithm achieved higher imperceptibility than the other state-of-the-art algorithms regarding the average PSNR. The enhanced version of the proposed method was more robust against different types of attacks.

Corresponding Author:

Reham A. El-Shahed
Department of Scientific Computing, Faculty of Computer and Information Sciences
Ain Shams University
Cairo, Egypt
Email: rehamahmed@cis.asu.edu.eg

1. INTRODUCTION

Through time, the issue of information security is very critical at wars, innovations, …etc. These days, with a huge amount of digital data, there is a frequent need for new data hiding and security techniques. Watermarking and steganography are types of data hiding techniques. Watermarking is used to authenticate the data of the owner of a digital image. But in steganography techniques, the cover object is changed in a way that only the sender and the recipient can detect the message sent through it.

Watermarking could be visible or invisible, steganography is always invisible. Both are applying the same techniques for hiding data. The secret object, the cover media, the secret key (optional), and the hiding algorithm make up a digital steganography system. The message that must be kept hidden is the secret object; it may be a text, audio, image or video file. The cover medium is the object that contains the secret object. The hiding algorithm is the followed technique for hiding the secret object in the cover medium [1]. There are four concerns about any steganography technique. First, 'undetectability' which is the probability for the human visual system (HVS) to detect that there is something invisible in the cover object. The second one is 'hiding capacity', i. e., the size of the secret data that could be concealed in the cover object. Third property is 'robustness'. This is about the robustness of the steganography technique against problems or distortions that occurred during transmission or compression. The last one is 'security', which means that the algorithm and the key used in hiding should be kept secret. If the attacker detects that something is hidden, he will not be able to extract the secret message. [2]. Video file properties make it more ideal to be used in steganography applications. Because video files consist of frames and audio, audio and image steganography could be applied to provide more hiding capacity. Many algorithms could be applied to video files, such as motion detection, object detection and scene change detection. These algorithms can also be used to hide the secret message and that increases the security of the hiding process [3].

There are two types of video steganography techniques: compressed and uncompressed (raw) [4]. Intra-frame prediction, inter-frame prediction, motion vectors, transform coefficients, and entropy coding are some of the approaches utilised in compressed domains. In the raw domain, two methods could be used, which are the spatial domain methods and the transform domain methods. In the spatial domain techniques, the cover frames pixels are directly used to embed the secret message [4]. Many steganography techniques, such as least significant bit (LSB) substitution, pixel value differencing (PVD), spread spectrum, region of interest (ROI), histogram manipulation, most significant bit (MSB), and quantization index modulation (QIM), rely on the spatial domain for hiding [5]. In the transform domain, the cover frames pixels are used in the frequency domain. multiple transforms can be applied to videos, for example, discrete wavelet transform (DWT) [6], discrete fourier transform (DFT) [7], discrete cosine transform (DCT) [8], integer wavelet transform (IWT) [9], haar transform, discrete curvelet transform (DCVT) [10] and stationary wavelet transform (SWT) [11]. DCT, DWT and SWT are the most widely used for steganography. DCT provides greater security but its data embedding capacity is less than spatial domain techniques. DWT techniques provide better performance in terms of embedding capacity and robustness. [12]. The second generation of wavelet transform called lifting wavelet transform (LWT) was recently used in watermarking applications [13]. Some other steganography techniques are based on matrix factorization by using methods such as singular value decomposition (SVD) [14], QR decomposition, and lower-upper (LU) decomposition. A matrix factorization method is used to decompose the cover image into matrices, and the secret image is concealed into one of these matrices [15].

This is an overview of existing work in the video steganography field using transform domain techniques. Mumthas and Lijiya [16] introduced a new method for hiding text data within a video file using DCT. RSA and random DNA encryption techniques are applied to the hidden message. DCT is applied to the cover video after dividing each frame into 8×8 blocks. A compressed message was hidden into less significant areas of the coefficients obtained. The performance of this method was measured using peak signal to noise ratio (PSNR) and mean squared error (MSE) using different videos and different message lengths. Compared to the method proposed by Rajesh and Nargunam [17], this method reduced the MSE and increased the PSNR values. Using video scene change detection a technique was proposed by Ramalingam and Isa [18] to hide a secret image within a video series. DCT was applied to the video series; the resulted coefficients were then used to detect the scene change. After the scene change was detected, the embedding process was performed by replacing the LSB of the DCT coefficient with the message bit. The quality of this algorithm was measured in terms of the embedding capacity, distortion level, and PSNR. The comparison results implied that the proposed data-hiding method showed better security and minimized distortions to enhance video quality. Kuraparthi *et al.* [19] proposed a video watermarking technique. That technique combined DWT and SVD in addition to artificial bee colony (ABC) optimization algorithm. The "LL" sub-band was selected for the watermark insertion process. Then the singular value decomposition (SVD) technique was applied to the selected DWT block. At last, ABC algorithm was applied to select the best blocks. The method was evaluated in the presence of video processing attacks and the results proved the robustness of the algorithm. The PSNR is above 53 dB.

Korgaonkar and Gaonkar [20] proposed a DWT–DCT combined approach for video steganography. Non-key frames were selected from the cover video to hide secret data files. Each frame was then converted into the YCbCr color space model. DWT and DCT transformations were applied on Y, Cb, and Cr. The secret message was taken as input. It was then divided into a number of blocks equal to a number of non-key frames. Each block was split into three sub-blocks and converted into the binary bitstream to be hidden in the high-frequency sub-bands. Combining DCT and DWT techniques increased the value of PSNR and the capacity of hiding ratio. Fuad and Ernawan [3] also proposed a DCT based video steganography technique. The proposed technique depended on hiding the secret message in the object motion in the cover video. The secret message was embedded by modifying DCT coefficients. The results showed robustness against compression with average NC of 0.94. Mstafa *et al.* [21] used object tracking algorithms to propose a robust and secure video steganography method based on DWT and DCT. Motion detection was applied on the cover video to extract motion regions, DWT and DCT were then applied on motion regions. The encrypted secret message was hidden in DWT and DCT coefficients. This algorithm achieved good results in terms of hiding capacity and robustness. Another framework was proposed by Hadad *et al.* [22] to conceal private data gathered by surveillance systems. The main objective of the framework was using the in-paint approach to remove the target object from the scene. Then a data hiding technique was used to hide the original frame in the in-painted one. The implemented technique was implemented in the DCT domain based on the H.264 compression concept. The visual quality of the stego-frame was maintained very high in terms of PSNR. Another wavelet-based technique was proposed by Thakur *et al.* [23]. First, the cover video was separated into different frames. Then, a one-level discrete wavelet transform was applied to both a selected frame and a secret image. At last, an inverse DWT was applied to get the stego-video. Experimental results showed that the stego-video had a good PSNR value and the algorithm was highly secured with good visual quality. Ibrahim *et al.* [24] proposed combining spatial and frequency domain techniques to conceal a secret message in a video series. The algorithm used DCT and LSB techniques to hide the binary form of the secret message. The performance of the algorithm was measured using PSNR, MSE and correlation between original and stego-videos. The algorithm achieved good quality as the value of PSNR above 50 dB. Because of the rapid advancement in communication devices, the internet of things (IoT) is now widely used and faces numerous security issues. Arunkumar *et al.* [25] proposed a two-layer security technique. The first layer was located on the IoT sensor device, and the second layer was located on the server. A hybrid cryptography-steganography technique was used on the server side. The redundant integer wavelet transform (RIWT) and QR factorization were used in the steganography algorithm. In terms of PSNR and NCC, the algorithm performance was great.

Regarding techniques that hide a video in another one, Al-Kadei [26] proposed a method to hide video frames in another video frames. To begin, two keys were used in conjunction with an XOR bit operation to generate a huge number of different keys. Second, the high-resolution video frames were embedded using a modified method based on the LSB methodology, which provided two security layers. Many secret videos were used to test the encrypting and hiding video data techniques. The experimental result showed a good performance with very high PSNR and low correlation of the stego-video frames. Another hiding video technique was proposed by Danti *et al.* [27]. The proposed technique depended on DWT, sequence and random embedding techniques. The wavelet transform was applied to divide the cover video sequence and the least significant wavelet band was replaced by the secret frames. Sequence embedding was tested which shows good results in terms of PSNR and MSE and showed less distortion compared to the random embedding technique. Most of the previously discussed methods achieved good visual quality in terms of PSNR and other visual quality assessments but the hiding capacity is low. The proposed method aims to achieve good visual quality and high capacity for hiding. There are rare researches that hide a video; this research aims to successfully hide a video in another video.

A novel technique will be introduced in this study. To embed a video into another, this technique uses multi-resolution 3D SWT, SVD, and QR decomposition. SWT provides additional hiding capacity, while SVD allows us to improve the stego-perceptual video's quality. With reference to PSNR and structural similarity index measure (SSIM), we have improved the performance of video steganography by integrating 3D SWT and SVD.

2. PROPOSED METHOD

2.1. Stationary wavelet transform

The proposed steganography technique depends on the 3D SWT. The stationary wavelet transform is a wavelet transform that is shift-invariant. The sub-band is of the same size as the video size which enables more capacity to hide the secret message. The SWT coefficients are computed in [28] .

Figure 1, shows the implementation of one level resolution of SWT. ‘I’ is the input image, H is the details (ω_j^d, the output of the high-pass filter) and L is the approximation (output of the low-pass filter). In the second and third resolutions, LLL sub-band is considered as a source object.

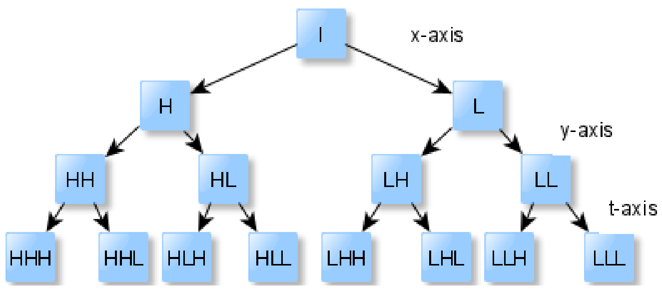

Figure 1. A 3D SWT is implemented as a 3 successive 1D SWT

2.2. Singular value decomposition

The SVD is a linear algebra-based theorem. It says that a rectangular matrix Mof size $x \times y$ can be decomposed into three matrices [14].

$$M = USV^T \quad (1)$$

Where U is an orthogonal $x \times x$ matrix, V is an orthogonal $y \times y$matrix and S is a diagonal matrix and it has the same size as M.

2.3. QR factorization

The QR factorization is used to determine a matrix's eigenvalues. The matrix is initially transformed into a Hessenberg matrix using an orthogonal similarity transformation, the eigenvalue and eigenvector are then obtained using the QR method, and the decomposition process is completed using the Gram-Schmidt orthogonalization approach. The false-positive problem produced by SVD is eliminated via QR factorization. For any real matrix M, there is an orthogonal matrix Q and an upper triangular matrix R, such that [29]:

$$M = QR \quad (2)$$

3. RESEARCH METHOD

A video hiding method in the SWT domain based on SVD is presented. A gray-scale video is used as a secret message and its singular values are hidden in the blue channel of the cover video because the blue component is less sensitive to the human visual system [30]. In the beginning, the cover video is divided into blocks each block contains eight successive frames. Three resolutions 3D SWT is then applied to the video frames' blue channel which produce eight sub-bands. One of the bands is selected to be decomposed into three matrices using SVD decomposition. SVD decomposition is applied also to the secret video frames to be embedded in the cover video coefficients. This results in the stego-video. This method showed high visual quality for the stego-video but it was not robust against attacks.

3.1. Enhanced method

An enhanced method is proposed that is more robust against attacks. The main stages of the method are illustrated in Figure 2. A gray-scale video is used as a secret message. One resolution SWT is applied for the secret video frames. In the beginning, the cover video is divided into blocks each block contains eight successive frames. These blocks are then converted to YCbCr color space. Three- resolutions 3D SWT is then applied on the Y channel of the video frames which results in eight sub-bands. One of the bands is selected to be decomposed into two matrices using QR factorization. QR factorization is applied also for the LLL sub-band of the secret video. SVD decomposition is applied for R matrices of both cover and secret videos. The singular values for both matrices are embedded using the alpha value. The R matrix of the cover video is then calculated using the modified singular matrix. The cover sub-band is also re-calculated using the modified R matrix. Inverse 3D SWT is then applied. This results in the stego-video as illustrated in Figure 2.

3.2. Embedding process

The singular values of the low sub-band of the cover video are modified by the singular values of the secret video. In the present work, we consider a cover video C of size M*N and a secret video S of size M*N. The embedding process is as follows:
Step1. Decompose the cover video to blocks of eight successive frames.
Step2. Convert the video to YCbCr color space
Step3. Apply 3D-SWT on the Y channel of each block.
Step4. Apply QR factorization on LLL3 sub-band to obtain the R matrix

$$[q_c \; r_c] = QR(LLL3) \quad (3)$$

Step5. Apply SVD on the R matrix

$$[\mathrm{Uc\ Sc\ Vc}] = \mathrm{SVD}(\mathrm{r}_c) \quad (4)$$

Step6. For each frame (i=1, 2…8) in secret video S perform the following:
a. Apply one-resolution 3D SWT

b. Apply QR factorization for sub-band LLL of secret video frames

$$[q_{si}\ r_{si}] = QR(LLL) \tag{5}$$

c. Apply SVD for the R matrix

$$[\mathrm{U_i}\ \mathrm{S_i}\ \mathrm{V_i}] = \mathrm{SVD}(r_{si}) \tag{6}$$

d. Embed $\mathrm{S_i}$ into Sc using this formula

$$\mathrm{D_i} = \mathrm{Sc_i} + \mathrm{alpha} * \mathrm{S_i} \tag{7}$$

Where alpha is the scaling factor.

e. Re-compute R matrix

$$r_i' = \mathrm{Uc_i}\ \mathrm{D_i}\ \mathrm{Vc_i}^{\mathrm{T}} \tag{8}$$

f. Re-compute LLL3 coefficients

$$\mathrm{LLL3'}_{\mathrm{i}} = \mathrm{q}_{ci} * r_i' \tag{9}$$

g. To get the Y component of the frame, apply inverse 3-level SWT to the adjusted LLL3'sub-band coefficients. Convert the cover video to RGB to produce the stego-video

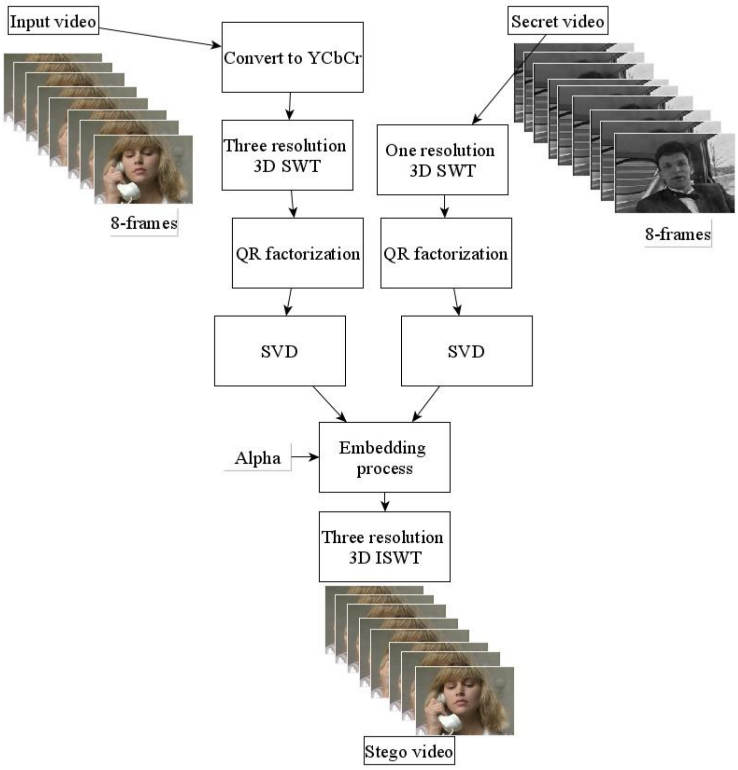

Figure 2. The proposed video steganography algorithm

3.3. Extraction process

Step1. Convert stego-video to YCbCr space
Step2. Apply 3 level SWT on the Y component of stego-video and original video to obtain the LLL3′ and LLL3 sub-band coefficients respectively.
Step3. For each frame (i=1, 2…8) in secret video perform the following:

a. Apply QR factorization on $LLL3'$ and $LLL3$ sub-band coefficients to obtain the R matrix r_i^* and r_i respectively.

$$[q_{ci}\ r_{ci}] = QR(LLL3) \quad (10)$$

$$[q_{ci}^*\ r_{ci}^*] = QR(LLL3') \quad (11)$$

b. Apply SVD for r matrix

$$[\mathrm{Uc_i}\ \mathrm{Sc_i}\ \mathrm{Vc_i}] = \mathrm{SVD}(\mathrm{r}_{ci}) \quad (12)$$

$$[\mathrm{Uc_i^*}\ \mathrm{Sc_i^*}\ \mathrm{Vc_i^*}] = \mathrm{SVD}(r_{ci}^*) \quad (13)$$

c. Extract the embedded singular values using this formula

$$\mathrm{Sw_i} = (\mathrm{Sc_i^*} - \mathrm{Sc_i}) / \text{ alpha} \quad (14)$$

d. Compute the R matrix of the secret video frames

$$\mathrm{r_{si}} = \mathrm{U_i}\ \mathrm{Sw_i}\ \mathrm{V_i^T} \quad (15)$$

e. Compute the LLL coefficients of the secret video frames

$$LLL' = q_{si} * r_{si} \quad (16)$$

f. Apply inverse SWT to extract the secret video frames

4. RESULTS AND DISCUSSION

4.1. Performance criteria

For the quantitative evaluation of the method, two measures are used there are PSNR [27] and SSIM index [31]. The PSNR calculates the ratio between two signals. The PSNR is defined using the MSE. The MSE is defined as:

$$\mathrm{MSE} = \frac{1}{xy}\sum_{i=0}^{x-1}\sum_{j=0}^{y-1}[\mathrm{M}(i.j) - \mathrm{N}(i,j)]^2 \quad (17)$$

The PSNR is defined as:

$$\mathrm{PSNR} = 10.\log_{10}\left(\frac{\mathrm{MAX_M^2}}{\mathrm{MSE}}\right) \quad (18)$$

Where MAX is the maximum possible pixel value of the image, image M of size x × y and N is its noisy approximation.
SSIM compares two images structurally. It is defined as follows:

$$\mathrm{SSIM}\ (x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (19)$$

Where x and y are two windows of common size,μ_x is the average of x, μ_y is the average of y, σ_x^2 is the variance of x, σ_y^2 is the variance of y and σ_{xy} is the covariance of x and y.

4.2. Results and discussion

The proposed algorithm has been tested using a cover color video with moving objects and secret grayscale videos. The used cover videos were of 15 seconds duration. The frame size is 144×176. Different parameters were tested to detect the best values that derive the best resolution in terms of PSNR and SSIM.

4.2.1. Qualitative results

Figure 3(a) shows the same cover video before and Figure 3(b) after embedding data. Figures 4(a) to (f) shows the same frame in the original secret video and after its extraction from stego-video.

(a) (b)

Figure 3. Sample of the cover video frames before embedding and after embedding (a) the original cover video frame and (b) the stego-video frame

(a) (b)

(c) (d)

(e) (f)

Figure 4. Sample of secret video frames before embedding and after extraction left-hand side are the original frames (a) carphone, (c) foreman, (e) akiyo, right-hand side are the extracted frames, (b) carphone, (d) foreman and (f) akiyo

4.2.2. Quantitative results

The algorithm depends on multiple parameters that affect the quality of cover and secret videos with reference to PSNR and SSIM. Table 1 shows the stego-video and secret video quality at various resolution levels. The results show that the third resolution is the best as the cover PSNR is 68.8. Figure 5 displays the effect of changing the alpha value which derives that, the best range is [0-0.5]. ‘Carphone’ video is used for testing parameters.

The algorithm is tested for different sub-bands. The same secret video is embedded in the same cover video in different sub-bands. Table 2 shows the quality achieved using each sub-band. The best quality is hiding the secret video in the third resolution of the LLL sub-band as the similarity of the extracted secret video is 97%. Another parameter that controls the quality of the videos is the wavelet mother function. Table 3 shows that, the quality of the secret video is better when using ‘db4’ rather than using ‘haar’ or ‘db2’. At the end Table 4, shows the quality of different secret videos in terms of PSNR and SSIM using the best parameter values: third resolution, db4, LLL sub-band and alpha=0.05. The results show that the average value for cover PSNR is 66.7 and the similarity of secret video is 97%.

Table 1. Quality for the stego and the secret videos for different levels of resolution, mother wavelet db4, alpha=0.05, sub-band ‘LLL’

Resolution	Secret PSNR	Secret SSIM	Cover PSNR
1	37.4	0.98	46.4
2	37.3	0.97	53.8
3	36.3	0.97	68.8

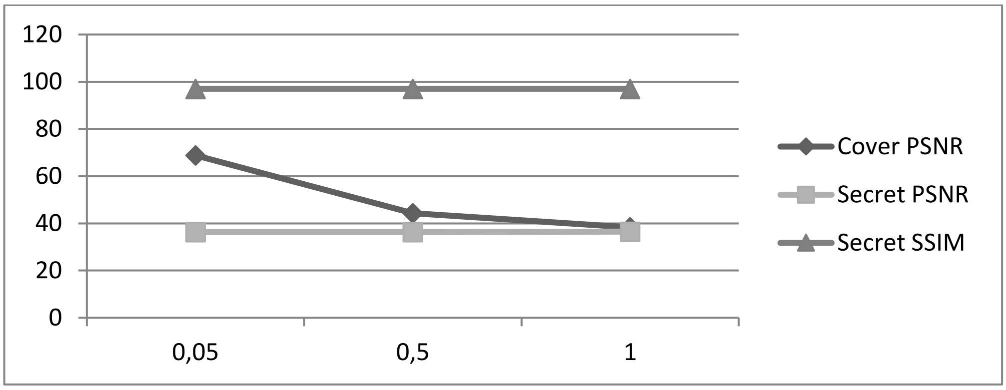

Figure 5. The performance using different values of alpha, mother wavelet db4, level of resolution=3, Sub-band ‘LLL’

Table 2. The quality measures using different sub-bands of the cover video, mother wavelet db4, alpha=0.05, level of resolution=3

Sub-band	Secret PSNR	Secret SSIM	Cover PSNR
LLL3	36.3	97	68.8
LLH3	14.8	30	76
LHL3	26.4	87	74.7
LHH3	15	35	90.2
HLL3	17.9	58	77.1
HLH3	14.1	42	Inf
HHL3	13.3	34	70.4
HHH3	13.1	28	82.8

Table 3. The quality measures using different wavelet mother functions, level of resolution=3, alpha=0.05, sub-band ‘LLL’

Wavelet mother	Secret PSNR	Secret SSIM	Cover PSNR
Haar	31.3	93	69.1
Db2	34.8	96	68.9
Db4	36.3	97	68.8

Table 4. The quality measures using different secret videos, mother wavelet ‘db4’, Level of resolution=3, alpha=0.05, sub-band ‘LLL’

Secret video	Cover PSNR	Secret PSNR	Secret SSIM
Carphone	68.8	36.3	97
Foreman	63.8	33.1	96
Akiyo	67.7	32.2	97

4.2.3. Comparative analysis

We compared our proposed technique with two algorithms that were used to hide a video in another one. The first algorithm proposed in [26], is a spatial domain-based which uses XOR encryption and LSB to hide a video series within another one. The second algorithm proposed in [27] is a transform domain-based that uses DWT. It proposed two techniques sequence and random embedding techniques.

Table 5, shows how the proposed algorithm compared to the other algorithms in terms of average PSNR between cover and stego-videos. The comparison proved that the imperceptibility of the proposed algorithm is very high as the results overcome the results from other recent algorithms in the field.

Table 5. Comparison between the proposed algorithm and other techniques

Algorithm	Used techniques	Average PSNR
Faten H. [26]	XOR encryption + LSB technique	54
Ajit Danti [27] – sequence embedding	DWT	39
Ajit Danti [27] – random embedding	DWT	38
Proposed technique	SWT + SVD	66.7

4.2.4. Embedding capacity

The largest amount of secret data that can be hidden in a cover video is called "capacity." Capacity is determined by the embedding process and the properties of the cover video. The percentage of the amount of embedded data to the size of the original cover video is known as capacity. The proposed algorithm achieved 100% embedding capacity which proves its higher efficiency. Embedding capacity is calculated as: [17].

$$\text{capacity} = \frac{\text{maximum size of embedded data}}{\text{size of original cover video}} \times 100 \quad (28)$$

$$\text{capacity} = \frac{144 \times 176}{144 \times 176} \times 100 = 100\% \quad (29)$$

4.2.5. Enhanced method results

The proposed method was enhanced and tested against different types of attacks noise, rotation and sharpening. This method was tested using the same parameters in the main method, the mother wavelet is‘db4’, level of resolution=3, alpha=0.05 and sub-band ‘LLL’. The enhanced method using SVD in YCbCr color space achieved good results in terms of the similarity of the extracted secret video. Applying QR factorization added a slight enhancement in the quality of the extracted video as the similarity reached 84% and did not affect the visual quality of the cover object as the cover PSNR in both cases is 46.4 dB. Table 6, shows the SSIM percentage for ‘carphone’ video under various types of attacks.

Table 6. The SSIM of extracted secret video under various types of attacks

Attack	RGB		YCbCr	
	SVD	SVD+QR	SVD	SVD+QR
Salt&pepper 0.001	70	73	83	84
Salt&pepper 0.005	51	48	55	57
Rotate 15	57	57	57	57
Rotate 30	55	55	57	57
Sharpen	59	59	68	68

5. CONCLUSION

This paper presents a review on different steganography algorithms in the transform domain. The suggested algorithm uses SWT and SVD to hide a video within another one. Three resolution SWT is applied to the cover video. SVD is applied to the LLL sub-band and the secret video frames. The singular values of the secret video are embedded in the singular values of the LLL sub-band using the value of alpha. The inverse transform is then applied to get the stego-video. The experimental results show that the third resolution is better than the first and second resolutions as the PSNR value of the cover video in the third resolution is 68.8. Hiding the secret video in different sub-bands is also tested to detect the best sub-band and the results show that the ‘LLL’ sub-band is the best. Two parameters affect the quality of videos; the value of alpha and the mother wavelet function. The experimental results show that the best value that achieved the highest result is 0.05.and the wavelet mother function ‘db4’ provides good quality. The comparative analysis shows that the introduced algorithm achieved high imperceptibility than the other state-of-the-art algorithms with reference to the average PSNR. An enhanced method that uses SVD and QR factorization in YCbCr color space achieved more robustness against attacks as the SSIM of extracted secret video reached 84%. Both methods achieved a high-capacity percentage of 100%.

REFERENCES

[1] F. Q. A. Alyousuf, R. Din, and A. J. Qasim "Analysis review on spatial and transform domain technique in digital steganography." Bulletin of Electrical Engineering and Informatics vol. 9, no. 2, pp. 573-581, 2020, doi: 10.11591/eei.v9i2.2068.

[2] P. Joseph and S. Vishnukumar, "A study on steganographic techniques," *2015 Global Conference on Communication Technologies (GCCT)*, 2015, pp. 206-210, doi: 10.1109/GCCT.2015.7342653.

[3] M. Fuad and F. Ernawan, "Video steganography based on DCT psychovisual and object motion," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 3, pp. 1015-1023, 2020, doi: 10.11591/eei.v9i3.1859.

[4] R. J. Mstafa, K. M. Elleithy, and E. Abdelfattah, "Video steganography techniques: Taxonomy, challenges, and future directions," *2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 2017, pp. 1-6, doi: 10.1109/LISAT.2017.8001965.

[5] Disha and K. Saini, "A review on video steganography techniques in spatial domain," *2017 Recent Developments in Control, Automation & Power Engineering (RDCAPE)*, 2017, pp. 366-371, doi: 10.1109/RDCAPE.2017.8358298.

[6] A. Graps, "An introduction to wavelets," *IEEE Computational Science and Engineering*, vol. 2, no. 2, pp. 50-61, Summer 1995, doi: 10.1109/99.388960.

[7] S. W. Smith. "The scientist and engineer's guide to digital signal processing." 2nded, Publisher: California Technical Publishing, USA, Chapter 8, pp. 141-167, 1999.

[8] N. Ahmed, T. Natarajan and K. R. Rao, "Discrete Cosine Transform," *IEEE Transactions on Computers*, vol. C-23, no. 1, pp. 90-93, Jan. 1974, doi: 10.1109/T-C.1974.223784.

[9] A. R. Calderbank, I. Daubechies, W. Sweldens, and B. L. Yeo, "Wavelet transforms that map integers to integers." *Applied Computation Harmonic Analysis*, vol. 5, pp. 332–369, 1998, doi: 10.1006/acha.1997.0238.

[10] E. Candès, L. Demanet, D. Donoho, and L. Ying, "Fast Discrete Curvelet Transforms." SIAM Journal Multiscale Model. Simul, vol. 5, pp. 861–899, 2006, doi: 10.1137/05064182X.

[11] D. Sundararajan. "The Discrete Stationary Wavelet Transform." In *Discrete wavelet Transform: A Signal Processing Approach, chapter 13*, pp. 234-246, 2015, doi:10.1002/9781119113119.ch13.

[12] M. M. S. Rani, S. Lakshmanan, and P. Saranya, "A Study on Video Steganography using Transform Domain Techniques," *Conference: 5th National conference on Computational Methods, Communication Techniques and Informatics*, vol. 1, 2017.

[13] D. B. Taha, T. B. Taha, and N. B. A. Dabagh, "A comparison between the performance of DWT and LWT in image watermarking," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 3, pp. 1005-1014, 2020, doi: 10.11591/eei.v9i3.1754.

[14] R. G. Kabra and S. S. Agrawal, "Robust embedding of image watermark using LWT and SVD," *2016 International Conference on Communication and Signal Processing (ICCSP)*, 2016, pp. 1968-1972, doi: 10.1109/ICCSP.2016.7754516.

[15] Ching-Sheng Hsu and Shu-Fen Tu "Enhancing the robustness of image watermarking against cropping attacks with dual watermarks," *Multimed Tools Appl*, vol. 79, pp. 11297–11323, 2020, doi: 10.1007/s11042-019-08367-6.

[16] S. Mumthas and A. Lijiya, "Transform Domain Video Steganography Using RSA, Random DNA Encryption and Huffman Encoding." *Procedia Computer Science*, vol. 115, pp. 660-666, 2017, doi: 10.1016/j.procs.2017.09.152.

[17] G. R. Rajesh and A. S. Nargunam, "Steganography algorithm based on discrete cosine transform for data embedding into raw video streams," *IET Chennai Fourth International Conference on Sustainable Energy and Intelligent Systems (SEISCON 2013)*, 2013, pp. 554-558, doi: 10.1049/ic.2013.0370.

[18] M. Ramalingam and N. A. M. Isa, "A data-hiding technique using scene-change detection for video steganography," *Computers and Electrical Engineering*, vol. 54, pp. 423-434, 2016, doi: 10.1016/j.compeleceng.2015.10.005.

[19] S. Kuraparthi, M. Kollati, and P. Kora, "Robust Optimized Discrete Wavelet Transform-Singular Value Decomposition Based Video Watermarking," *Traitement du Signal*, vol. 36, no. 6, pp. 565-573, 2019, doi: 10.18280/ts.360612.

[20] V. V. Korgaonkar and M. N. Gaonkar, "A DWT-DCT combined approach for video steganography," *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 2017, pp. 421-424, doi: 10.1109/RTEICT.2017.8256631.

[21] R. J. Mstafa, K. M. Elleithy and E. Abdelfattah, "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, 2017, doi: 10.1109/ACCESS.2017.2691581.

[22] A. Elhadad, S. Hamad, A. Khalifa, and H. Abulkasim, "A steganography approach for hiding privacy in video surveillance systems." Digital Media Steganography, pp. 165–187, 2020, doi: 10.1016/B978-0-12-819438-6.00017-7.

[23] A. Thakur, H. Singh, and S. Sharda, "Secure Video Steganography based on Discrete Wavelet Transform and Arnold Transform," *International Journal of Computer Applications*, vol. 123, no. 11, pp. 25-29, 2015, doi: 10.5120/ijca2015905596.

[24] A. E. Ibrahim, M. A. Elshahed, and T. I. Elarif, "Video Steganography Using Least Significant Bit in Frequency Domain," *International Journal of Intelligent Computing and Information Science*, vol.16 no. 1, 2016, doi: 10.21608/IJICIS.2016.10012.

[25] S. Arunkumar, S. Vairavasundaram, K. S. Ravichandran, and L. Ravi, "RIWT and QR factorization based hybrid robust image steganography using block selection algorithm for IoT devices," Journal of Intelligent & Fuzzy Systems, vol. 36, no. 5, pp. 4265-4276, 2019, doi: 10.3233/JIFS-169984.

[26] F. H. M. S. Al-Kadei, "Robust video data security using hybrid cryptography-steganography technique," *Periodicals of Engineering and Natural Sciences*, vol. 8, no. 3, pp. 1741-1751, 2020, doi: 10.21533/pen.v8i3.1612.

[27] A. Danti, G. R. Manjula, and Pallavi B. M., "Wavelet based color video steganography using sequence and random technique," *International Journal of Engineering Applied Sciences and Technology*, vol. 1, no. 8, 294-298, 2016.

[28] R. A. El-Shahed, M. N. Al-Berry, H. M. Ebeid, and H. A. Shedeed, "Video Steganography using 3D Stationary Wavelet Transform," *Proceedings of the 11th International Conference on Informatics & Systems INFOS*, 2018, doi:10.2139/ssrn.3475348.

[29] K. -H. Ng, S. -C. Liew, and F. Ernawan, "An Improved RDWT-based Image Steganography Scheme with QR Decomposition and Double Entropy," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 3, 2020, doi: 10.14569/IJACSA.2020.0110327.

[30] D. Dhaou, S. B. Jabra, and E. Zagrouba, "An Efficient Group of Pictures Decomposition based Watermarking for Anaglyph 3D Video," in *Proceedings of the 13th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications*, vol. 4, pp. 501-510, 2018, doi: 10.5220/0006619305010510.
[31] H. Zhang, B. Yuan, B. Dong, and Z. Jiang, "No-Reference Blurred Image Quality Assessment by Structural Similarity Index" *Applied Sciences*, vol. 8, no.10, p. 2003, 2018, doi: 10.3390/app8102003

BIOGRAPHIES OF AUTHORS

Reham A. El-Shahed received the Bsc and Msc degree in computer science, Scientific computing, from Ain Shams university, faculty of computer and information science 2013. She is now a teaching assistant at Scientific Computing department, in Faculty of Computers and Information Sciences, Ain Shams University, Cairo, Egypt. Her research activity can be found at: https://www.researchgate.net/profile/Reham-El-Shahed/research. She can be contacted at email: rehamahmed@cis.asu.edu.eg.

Maryam N. Al-Berry is an Assistant Professor at Scientific Computer Department, Faculty of Computer and Information Sciences, Ain Shams University. She is specialized in machine learning, image processing and computing in mathematics. More about her bibliography is listed in https://www.researchgate.net/profile/Maryam_Al-berry. She can be contacted at email: maryam_nabil@cis.asu.edu.eg.

Hala M. Ebied is a professor in Scientific Computing Department and the vice dean for education and student affairs at faculty of computer and information science (FCIS), Ain Shams University, Egypt. From 2006 to 2008, she was a Ph.D. student at Heinz Nixdorf Institute, University of Paderborn, Germany. Her research interests include image processing, computer vision, computational intelligence, deep learning, parallel computing and robotics. She can be contacted at email: halam@cis.asu.edu.eg.

Howida A. Shedeed received the Bsc, Msc and finally the Phd. degree in electrical engineering, Computers and systems engineering, from Ain Shams university, faculty of engineering 2005. She is Now a professor and the Head of Scientific Computing department, in faculty of computers and information sciences, Ain Shams University, Cairo, Egypt. Dr Howida has supervised more than 25 M.Sc. and Ph.D. degrees and has more than 65 Scopus indexed publications in different international and local conferences and journals, has Scopus H-index=10, her research interests are: biomedical signal and image processing, human computer interaction, machine learning, AI, and E-learning systems. Dr Howida shared in much computer science local and international conferences as a program committee chair or member, session committee, reviewer or invited speaker. Dr. Howida is a reviewer in many distinguished international journals such as: IEEE Access, IEEE Transactions on Emerging Topics in Computational Intelligence, Computer Methods and Programs in Biomedicine, International journal of Medical Imaging and Health Informatics, Remote Sensing Applications: Society and Environment, Egyptian computer Science Journal (ECJ), International Journal of Intelligent Computing and Information systems, Journal of advances in Computer Science and others. She can be contacted at email: dr_howida@cis.asu.edu.eg.