Diyala Journal of Engineering Sciences

Journal homepage: https://en.enginmag.uodiyala.edu.iq/

ISSN: 1999-8716 (Print); 2616-6909 (Online)

Digital Image Steganography Scheme Based on DWT and SVD

Fadhil Kadhim Zaidan*

Electronic Computer Center – Daiyla University, 32001 Diyala, Iraq

ARTICLE INFO

Article history:
Received 3 March 2020
Accepted 1 November 2020
Keywords:

Steganography; Cryptography; Transform domain; Robustness; Imperceptibility; DWT

ABSTRACT

In this work, a grayscale image steganography scheme is proposed using a discrete wavelet transform (DWT) and singular value decomposition (SVD). In this scheme, 2-level DWT is applied to a cover image to obtain the high frequency band HL2 which is utilized to embed a secret grayscale image based on the SVD technique. The robustness and the imperceptibility of the proposed steganography algorithm are controlled by a scaling factor for obtaining an acceptable trade-off between them. Peak signal to noise ratio (PSNR) and Structural Similarity Index Measure (SSIM) are used for assessing the efficiency of the proposed approach. Experimental results demonstrate that the proposed scheme still holds its validity under different known attacks such as noise addition, filtering, cropping and JPEG compression.

1. Introduction

With the increasing development in the use of digital multimedia in computer networks and the internet, computerized information such as (audio, image, text, and video) can now be created, distributed, and transmitted through the internet or other networks quickly and simply. Therefore, digital multimedia can be illegally copied, changed, and effortlessly distributed. So, the transmission of information via the internet may be risky and insecure. For resolving this challenge, many approaches of information security have been suggested. The most common and closely related are steganography and cryptography, which are mainly utilized to protect data from harmful activity or unwanted parties [1].

The main difference between steganography and cryptography is to keep the message secret. In the cryptography technique, the message is encrypted in such a way that it is visible and can only be understood by the intended person. In the case of steganography, the fact that the message exists is concealed by hiding it into other digital media. Steganography is a method of embedding secret information into data carrier in such a way that the existence of the secret message is not noticeable. Hence, steganography technique provides an additional layer of protection to data transfer as compared with cryptography technique. Generally, the quality of the steganography scheme is determined by two challenging factors: robustness and imperceptibility. The robustness factor measures the ability of the steganography scheme to resist digital signal processing operations and other intentional attacks while preserving the integrity of the hidden information. Whereas, imperceptibility means the ability of steganography scheme to hide the secret information so that it is unnoticed by human detects without distortion the quality of the data carrier. These two factors are conflict with each

*Corresponding author.
E-mail address: fadelkad2@gmail.com
DOI: 10.24237/djes.2020.13402

other, where increasing imperceptibility means reducing robustness and vice versa. Therefore, there is a need to develop a steganography method that provides an acceptable trade-off between imperceptibility and robustness [2,3].

In general, image steganography techniques are divided into two main parts: spatial domain and frequency domain. In the spatial domain, the secret information is embedded into the carrier image by modifying the pixel value directly such as in the Least Significant Bit (LSB) algorithm [4]. Where as in the frequency domain, the carrier image is firstly converted into the frequency domain then the secret information is embedded into the coefficients of carrier image. Discrete Wavelet Transform (DWT) [5] and Discrete Cosine Transform (DCT) [6] are the most commonly used algorithms in the frequency domain. These transformation techniques are more efficient than spatial domain techniques for achieving imperceptibility and robustness as clarified by several surveys [7,8,9]. Hence, the frequency domain is used for the proposed scheme.

2. Discrete wavelet transform

DWT is one of the most powerful mathematical tools used in digital image applications that decomposes an image hierarchically into sub-images. For two dimensional applications, DWT is applied in the horizontal direction followed by the vertical direction. Hence, an input image is firstly divided into two sub-bands: high frequency and low frequency bands by applying high pass (H) and low pass (L) filters horizontally. Then, each sub-band is divided again into two sub-bands by applying high pass and low pass filters vertically. As a result, four sub-bands are produced called: approximation (LL), vertical (LH), horizontal (HL), and diagonal (HH) as shown in figure 1. The low frequency component of the decomposed image is represented by the approximation (LL) band that contains the most significant features of the image. Whereas, the high frequency component is represented by the other three bands (LH, HL, and HH) that contain edge and image details. The high frequency components are commonly utilized for image hiding techniques because the Human Visual System (HVS) is less sensitive to changes in image details [10,11]. Hence, the horizontal sub-band HL is employed in this work for secret image hiding to optimize both imperceptibility and robustness requirements at the same time.

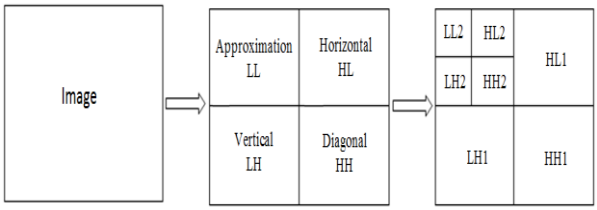

Fig 1. 2-level 2-D discrete wavelet transform.

3. Singular value decomposition

SVD is one of the most useful matrix factorization methods which can be used to decompose a matrix into its eigenvalues and eigenvectors based on linear algebra. It has been successfully applied in various fields of digital image processing such as pattern analysis, image compression, watermarking, noise removal, and image steganography due to its high stability analysis against several image processing operations. In SVD, an image A with a size of M×N can be decomposed into three matrices namely U, S, V such that [12]:

$$A = U\,S\,V^T \tag{1}$$

where U and V represent the left and the right orthogonal matrices with a size of m×m and n×n respectively, S represents the diagonal matrix with a size of m×n and the superscript T indicates the transpose operator. The columns of the matrices U and V are called left singular vectors and right singular vectors respectively which specify the geometry of image. While the elements of S are known as singular values that specify the luminance of the image [13]. The use of SVD in the field of image steganography improves the imperceptibility and robustness requirements based on two properties of SVD. The first one is any small alteration made to an image will not change significantly it's singular values. The second one is a few singular values specifies a large part of an image signal so fewer cover image values will be changed [14].

4. Proposed work

In this work, two different transformation techniques DWT and SVD are utilized to improve the performance of the proposed steganography scheme. The proposed scheme is divided into two main parts, secret image embedding process and secret image extraction process as shown in Figures 2 and 3. The secret image embedding and extraction algorithms are clarified below.

4.1. Embedding algorithm

Step 1: Reading the original host image I and the secret image g.

Step 2: obtaining the HL2 band by applying two level 2D-DWT as follows:
$[LL1, LH1, HL1, HH1] = \text{DWT}(I)$
$[LL2, LH2, HL2, HH2] = \text{DWT}(LL1)$

Step 3: Applying SVD to the selected HL2 band and to get the singular value matrix as:
$[U_I\ S_I\ V_I\ ] = \text{SVD}(HL2)$.

Step 4: obtaining the singular value of the secret image g as:
$[\ U_g\ S_g\ V_g\ ] = \text{SVD}(g)$

Step 5: Getting the singular value of stego image as follows:

$S_{I'} = S_I + \alpha * S_g$
where, α is the scaling factor which is discussed in section 5.

Step 6: obtaining the modified HL2' by combining the modified singular value $S_{I'}$ with the original U_I and V_I matrices of HL2 band as:

$$HL2' = U_I\ S_{I'}\ V_I{}^T$$

Step 7: Getting the stego image I' by performing two level inverse 2D-DWT as:

$$LL1' = \text{IDWT}\ [LL2\ , LH2, HL2'\ , HH2\ ]$$
$$I' = \text{IDWT}\ [LL1'\ , LH1, HL1, HH1\ ]$$

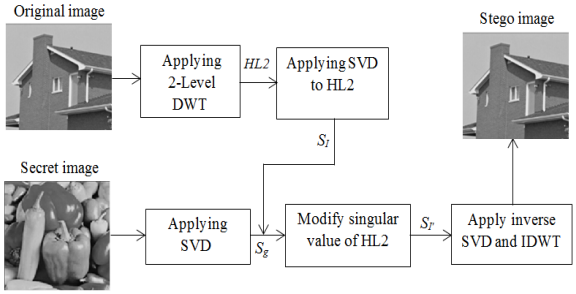

Fig 2. Embedding algorithm

4.2 Extraction algorithm

Step1: Reading the stego image (I')

Step2: Obtaining HL2 band of the stego image (I') by applying two level 2D-DWT as follows:
$[LL1, LH1, HL1, HH1] = \text{DWT}(I')$
$[LL2, LH2, HL2, HH2] = \text{DWT}(LL1)$

Step3: Decomposing the selected HL2 by performing SVD as:
$[U_{I'}\ S_{I'}\ V_{I'}\ ] = \text{SVD}\ (HL2)$.

Step4: Getting the singular values of the secret image by using the following formula:
$S_e = (S_I - S_{I'}) / \alpha$

Step5: Extracting the secret image g_e by combining the extracted singular value S_e with orthogonal matrices U_g and V_g as follows:
$g_e = U_g\ S_e\ V_g{}^T$

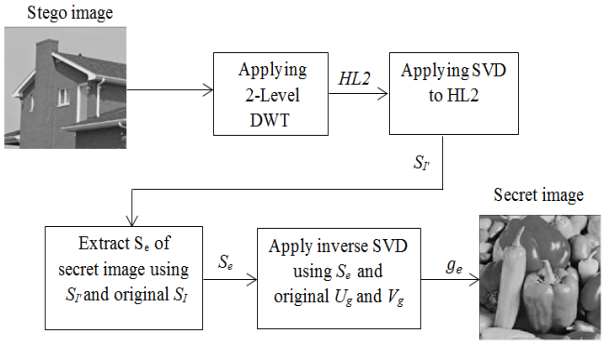

Fig 3. Extraction algorithm

5. Experimental results and simulation

The efficiency of steganography techniques is commonly estimated according to the imperceptibility of the stego image to human observers and the robustness of the inserted secret image under external attacks as well as the common signal processing operations. In order to evaluate the robustness of the proposed method, Structural Similarity Index Measure (SSIM) is utilized to measure the similarity degree between the original secret image and the extracted one. This metric is commonly used to estimate the quality of the restored images due to its correlation with the quality perception of the human.

The maximum value of SSIM is 1, which means that the extracted image and the restored image are precisely identical. SSIM value for two images f and g is calculated by the following equation [15]:

$$\mathrm{SSIM}(f,g) = \frac{(2\mu_f\mu_g + c_1)(2\sigma_{fg} + c_2)}{(\mu_f^2 + \mu_g^2 + c_1)(\sigma_f^2 + \sigma_g^2 + c_2)} \qquad (2)$$

where μ_f and $\mu_g$represent the mean values and σ_f^2 and σ_g^2 represent the variance of the original and extracted image respectively. σ_{fg} represent the covariance of the two images. The variables c_1 and c_2 are positive constants added to avoid a null denominator and defined as $c_1 = (0.01\max(f))^2$ and $c_2 = (0.03\max(f))^2$. In order to evaluate the imperceptibility requirements for the proposed method, peak signal to noise ratio (PSNR) is used to measure the quality of the stego image. PSNR value is calculated as [16]:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right) \qquad (3)$$

where MSE represent the mean square error of the original and stego image which is expressed as:

$$\mathrm{MSE} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(I(i,j) - I'(i,j))}{M \times N} \qquad (4)$$

The proposed scheme is simulated with MATLAB platform by using four widely known grayscale images are used which are Cameraman, House, and Boats as a cover image with the size of (512×512) in addition to Peppers image with the size of (64×64) as a secret image as shown in Figure 4.

(a) (b) (c) (d)

Fig 4. Test images: (a) Cameraman, (b) House (c) Boats, (d) Peppers

In the proposed scheme, the robustness and imperceptibility are controlled by adjusting the scaling factor (α) to give the desired trade-off between the robustness and imperceptibility. Where the lower value of α increases the perceptual quality of the stego image, but at the same time reduces the algorithm robustness level and vice versa as demonstrated visually in Figure 5 and quantitatively in table 1. Based on experiments, α=0.1 is selected and it can be changed depending on the image characteristics.

(a) (b) (c) (d) (e)

Fig 5. Stego House images with various scaling factor: (a) Original, (b) α = 0.05, PSNR = 43.67, (c) α = 0.1, PSNR = 37.70, (d) α = 0.3, PSNR = 29.00, (e) α = 0.5, PSNR = 25.46

Table 1 Performance comparison with different values of scaling factor α

Image	Attack	α = 0.01		α = 0.05		α = 0.1		α = 0.2		α = 0.3	
		PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Boats	None	57.61	0.8102	43.99	0.9879	38.52	0.9747	33.32	0.9286	30.43	0.8845
	Gaussian noise μ=0, v=0.001	30.00	0.1998	29.82	0.6120	29.43	0.7855	28.41	0.8641	27.26	0.8510
	Speckle noise 1%	25.32	0.1449	25.29	0.3533	25.16	0.5422	24.73	0.7249	24.20	0.7644
	Salt & pepper noise 1%	25.50	0.1553	25.34	0.3679	25.38	0.5621	24.73	0.7267	24.25	0.7789
	Cropping 1/8	16.52	0.5691	16.51	0.9730	16.49	0.9710	16.43	0.9276	16.35	0.8833
	Median filter 3x3	30.96	-0.1506	30.93	-0.2030	30.66	-0.1497	29.72	0.2124	28.63	0.4595
	compression (QF =10)	28.13	0.0142	28.05	0.6781	27.82	0.8343	27.15	0.8360	26.35	0.8038
	compression (QF =30)	31.82	0.3802	31.59	0.8762	31.04	0.9243	29.59	0.9015	28.15	0.8608
House	None	57.48	0.9123	43.67	0.9938	37.70	0.9980	32.07	0.9942	29.00	0.9816
	Gaussian noise μ=0, v=0.001	29.98	0.1672	29.83	0.4145	29.32	0.6206	27.94	0.8166	26.51	0.8939
	Speckle noise 1%	24.90	0.1544	24.84	0.2646	24.70	0.3840	24.21	0.5737	23.56	0.6972
	Salt & pepper noise 1%	25.49	0.1498	25.47	0.2696	25.23	0.4060	24.62	0.6109	23.85	0.7226
	Cropping 1/8	14.74	0.8018	14.74	0.9859	14.72	0.9963	14.66	0.9937	14.58	0.9813
	Median filter 3x3	44.29	-0.1668	41.87	0.5912	38.22	0.8138	33.23	0.8867	30.03	0.8954
	compression (QF =10)	33.91	-0.0481	33.59	0.5517	32.73	0.7648	30.07	0.9247	27.93	0.9315
	compression (QF =30)	39.26	0.2759	38.01	0.8738	35.46	0.9546	31.34	0.9818	28.66	0.9748
Camer-aman	None	57.63	0.8835	43.91	0.9919	38.11	0.9896	32.60	0.9752	29.56	0.9532
	Gaussian noise μ=0, v=0.001	30.07	0.1446	29.93	0.4601	29.50	0.6789	28.22	0.8468	26.88	0.8801
	Speckle noise 1%	25.60	0.1048	25.55	0.2562	25.37	0.4285	24.83	0.6386	24.18	0.7347
	Salt & pepper noise 1%	24.77	0.1111	24.95	0.2589	24.85	0.4299	24.24	0.6387	23.58	0.7462
	Cropping 1/8	15.69	0.7198	15.68	0.9816	15.66	0.9858	15.60	0.9738	15.51	0.9523
	Median filter 3x3	38.12	-0.1562	37.59	-0.1363	36.0	0.1884	32.77	0.5746	30.23	0.6920
	compression (QF =10)	31.81	-0.1330	31.65	0.3248	31.11	0.6850	29.52	0.8435	27.95	0.8494
	compression (QF =30)	37.08	-0.0699	36.42	0.6378	34.76	0.8625	31.47	0.9215	29.03	0.9205

In Figure 6, the extracted Peppers images with the corresponding stage House images which are exposed to various well-known attacks. Table 2 presents a performance analysis of the proposed scheme based on SSIM and PSNR, the tested images are subjected to different attacks including median filtering, image cropping, speckle noise, salt & pepper noise, Gaussian noise, and JPEG compression with different quality factor (QF). Additionally, a comparison analysis of the proposed method with the steganography method in [17] is presented.

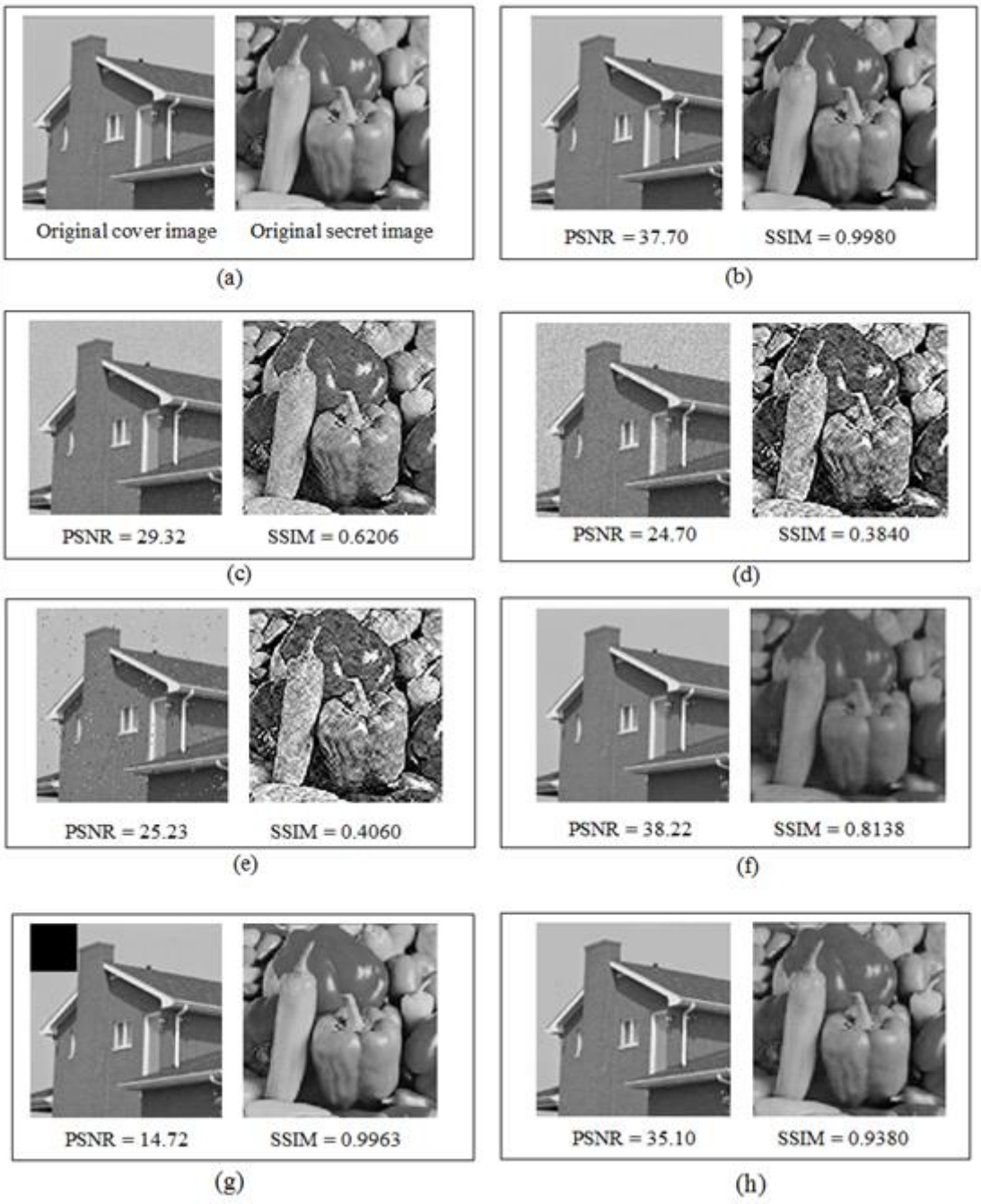

Fig 6. Stego House image exposed to various statistical attacks with the extracted secret Peppers image of each one: (a) Original cover and secret images, (b) Stego and extracted secret images with no attack, (c) Gaussian noise (μ =0,=0.001), (d) Speckle noise (1%), (e) Salt & pepper noise (1%), (f) Median filtering 3x3 (g) Cropping 1/8, and (h) image compression (QF=25)

Table 2 Performance analysis and comparison

Image	Attacks	Scheme in [17]		Proposed scheme	
		PSNR	SSIM	PSNR	SSIM
Boats	None	32.85	0.9278	38.52	0.9747
	Gaussian noise μ=0, v=0.001	28.20	0.4656	29.43	0.7855
	Speckle noise 1%	24.66	0.2942	25.16	0.5422
	Salt & pepper noise 1%	24.69	0.2974	25.38	0.5621
	Cropping 1/8	16.42	0.9225	16.49	0.9710
	Cropping 1/4	10.35	0.8116	10.36	0.3810
	Median filter 3x3	30.42	-0.0212	30.66	-0.1497
	JPEG compression (QF =10)	27.72	-0.1129	27.82	0.8343
	JPEG compression (QF =30)	30.35	0.0152	31.04	0.9243
House	None	31.68	0.9929	37.70	0.9980
	Gaussian noise μ=0, v=0.001	27.75	0.3544	29.32	0.6206
	Speckle noise 1%	24.09	0.2568	24.70	0.3840
	Salt & pepper noise 1%	24.48	0.2629	25.23	0.4060
	Cropping 1/8	14.65	0.9882	14.72	0.9963
	Cropping 1/4	9.82	0.6919	9.82	0.4463
	Median filter 3x3	38.39	0.1327	38.22	0.8138
	JPEG compression (QF =10)	31.86	0.4189	32.73	0.7648
	JPEG compression (QF =30)	32.65	0.6459	35.46	0.9546
Cameraman	None	32.88	0.9320	38.11	0.9896
	Gaussian noise μ=0, v=0.001	28.30	0.3494	29.50	0.6789
	Speckle noise 1%	24.89	0.2583	25.37	0.4285
	Salt & pepper noise 1%	24.45	0.2520	24.85	0.4299
	Cropping 1/8	15.60	0.9314	15.66	0.9858
	Cropping 1/4	11.15	0.8592	11.17	0.2946
	Median filter 3x3	36.15	0.1095	36.05	0.1884
	JPEG compression (QF =10)	30.58	0.4349	31.11	0.6850
	JPEG compression (QF =30)	33.15	0.5828	34.76	0.8625

6. Conclusions

In this study, steganography algorithm for concealing a secret grayscale image based on DWT and SVD techniques is suggested. The imperceptibility level of the stego image is increased by embedding the secret image with the coefficients of high frequency wavelet HL2 of the cover image using SVD matrices. Furthermore, the robustness level is controlled by adjusting the scaling factor based on the

desired level and the characteristics of the host image. The stego image is subjected to various attacks (speckle noise, salt and peppers noise, Gaussian noise, median filtering, cropping, and JPEG compression) for evaluating the proposed scheme. Experimental results and simulations show that the proposed algorithm based on DWT and SVD techniques has been able to meet robustness and imperceptibility requirements and makes a trade-off between them.

References

[1]. V. Reshma, S. J. Gladwin and C. Thiruvenkatesan, Pairing-Free CP-ABE based Cryptography Combined with Steganography for Multimedia Applications, 2019 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, pp. 0501-0505, 2019.

[2]. Ghazwan Jabbar Ahmed, Adel Jalal Yousif and Fadhil Kadhim Zaidan, A Digital Image Watermarking Scheme based on Discrete Cosine Transform, Journal of Engineering and Applied Sciences ,Volume 14, Issue 16, pp 5762-5768, 2019.

[3]. Adel Jalal Yousif, Image Steganography Based on Wavelet Transform and Color Space Approach, Diyala Journal of Engineering Sciences, Vol. 13, No. 3, pp. 23-34, June 2020.

[4]. Ashty M. Aaref, Video Steganography Using LSB Substitution and Sobel Edge Detection, Diyala Journal of Engineering Sciences, Vol. 11, No. 2, pp. 67-73, June 2018.

[5]. S. Al-Azawi, A. Abedelkareem, Low complexity multilevel 2-D DHWT architecture. The second engineering scientific conference-college of engineering, Diyala University. Diyala Journal of Engineering Sciences. 8(4), pp. 493–500, 2015.

[6]. Adel Jalal Yousif, A Discrete Cosine Transform Based Watermarking Scheme For Color Image Using Ycbcr Space, Journal of Engineering and Sustainable Development Vol. 22, No.06, pp. 1-12, November 2018.

[7]. R.E. Vinodhini, P. Malathi and T.G. Kumar, A survey on DNA and image steganography, in: Proceedings of the 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 2017.

[8]. D. N. Aini, D. R. I. Moses Setiadi, S. N. Putro, E. H. Rachmawanto and C. A. Sari, Survey of Methods in the Spatial Domain Image Steganography based Imperceptibility and Payload Capacity, 2019 International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang, Indonesia, pp. 434-439, 2019.

[9]. S.S. Baawi, M.R. Mokhtar, and R. Sulaiman, A comparative study on the advancement of text steganography techniques in digital media, ARPN J. Eng. Appl. Sci. 13 pp. 1854–1863, 2018.

[10]. M. Parul and R. Harish, Optimized Image Steganography Using Discrete Wavelet Transform (DWT), International Journal of Recent Development in Engineering and Technology, vol. 2, no. 2, pp. 75–81, 2014.

[11]. O. Abodena, and M. Agoyi, Colour Image Blind Watermarking Scheme Based on Fast Walsh Hadamard Transform and Hessenberg Decomposition, Studies in Informatics and Control 27, pp.339-348, 2018.

[12]. HS Devi and KM Singh, Red-cyan anaglyph image watermarking using DWT, Hadamard transform and singular value decomposition for copyright protection, Journal of Information Security and Applications 50Elsevier, pp. 2214-2126, 2020.

[13]. M. S. Subhedar and V. H. Mankar, High capacity image steganography based on discrete wavelet transform and singular value decomposition, in Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, ACM, pp. 1-7, 2014.

[14]. Dr. Rajaa aldeen Abad Khalid and Aman Ala'a Hussain, Multi-level Steganography System Using Wavelet Transform, Journal of Engineering and Sustainable Development Vol. 22, No. 03, pp. 50-61, May 2018.

[15]. HA Ilgin and A Akbulut, An Artifact Reduction Method for Block-Based Video Coding, Communications Faculty of Sciences University of Ankara Series A2-A3: Physical Sciences and Engineering, pp. 1-13, 2020.

[15] Muna M. Jawad, Dr. Ekbal H. Ali and Adel J. Yousif, A Fuzzy Random Impulse Noise Detection and Reduction Method Based on Noise Density Estimation, International Journal of Scientific & Engineering Research, Volume 5, Issue 3, pp. 455-468, March-2014.

[16] M. Douglas, K. Bailey and M. Leeney, K. Curran, Using SVD and DWT Based Steganography to Enhance the Security of Watermarked Fingerprint Images, Telkomnika, vol. 13, pp. 1368-1379, June 2015.