International Journal of Engineering

Journal Homepage: www.ije.ir

Singular Value Decomposition based Steganography Technique for JPEG2000 Compressed Images

G. Kasana*[a], K. Singh[b], S. Singh Bhatia[c]

[a] *Computer Science and Engineering Department, Thapar University, Patiala-147004 India.*
[b] *Electronics and Communication Engineering Department, Thapar University, Patiala-147004, India.*
[c] *School of Mathematics, Thapar University, Patiala-147004, India*

PAPER INFO

Paper history:
Received 18 June 2015
Received in revised form 17 November 2015
Accepted 24 December 2015

Keywords:
Discrete Wavelet Transform
Singular Value Decomposition
Peak Signal to Noise Ratio
Genetic Algorithm
Scaling Factor

ABSTRACT

In this paper, a steganography technique for *JPEG*2000 compressed images using singular value decomposition (*SVD*) in wavelet transform domain is proposed. In this technique, discrete wavelet transform (*DWT*) is applied on the cover image to get wavelet coefficients and singular value decomposition is applied on these wavelet coefficients to get their singular values.Secret data bits are embedded into these singular values using scaling factor. Different compression rates are also considered for *JPEG*2000 images after embedding the secret images. Genetic algorithm (*GA*) is used to optimize the value of scaling factor (*SF*). Maximum capacity of the proposed technique is 25% of cover image size and maximum peak signal to noise ratio(*PSNR)* values between cover and its stego image is more than the *PSNR* of existing techniques. Embedding capacity of proposed technique is also higher than the embedding capacity of existing techniques. Also, *PSNR* between secret image and extracted image is high and hence the visual quality of the extracted secret image is good enough to the human visual system. Steganalysis tests are performed on the stego images to show imperceptibility of proposed technique.

***doi**: 10.5829/idosi.ije.2015.28.12c.04*

1. INTRODUCTION

In recent years, hasty expansion of public networks and development of digital multimedia technologies have dramatically increased the transmission of digital contents like digital images, videos and audios. One of the important requirements of this transmission is to prevent the data theft. Steganography is a data hiding technique, which is used in various applications of information security. It is used to transmit secret data by hiding its existence so that an attacker cannot identify the existence of secret data and hence is not able to misuse it. The main advantage of steganography is that it will not attract/fascinate the attackers. It pays attention to the degree of invisibility.

Steganography can be done in spatial domain, frequency domain and compressed domain. Many techniques have been proposed in these domains. Proposed technique is related to compressed domain, therefore we have reviewed the existing data hiding techniques for *JPEG*2000. Seo et al. [2] proposed a discrete wavelet transform (*DWT)* based watermarking method for *JPEG*2000 to embed watermark into wavelet coefficients. Noda et al. [3] proposed a steganography scheme for *JPEG*2000 lossy compression and bitplane complexity segmentation. Main objective of their scheme is to increase the robustness of steganography methods for lossy compressed cover image. Lazy mode compression based steganography technique for *JPEG*2000 image was proposed by Su et al. [4]. In their technique, secret data bits are embedded in the raw encoded magnitude refinement passes of *JPEG*2000 encoder. Distortion induced in the stego image is computed during the embedding of secret data. When distortion in the stego image crosses a threshold value, secret bits embedding is over. Hai-ying et al. [5] proposed a steganography

* Corresponding Author's Email: gkasana@thapar.edu (G. Kasana)

algorithm for *JPEG*2000 image to embed secret messages directly into the output of the tier-2 process. Zhang et al. [6] proposed a steganography scheme for *JPEG*2000 baseline encoder in which bit plane encoding procedure is used twice to solve the problem due to bit stream truncation in tier-2 coding of *JPEG*2000 standard.

Recently, the concept of *SVD* has been exploited in data hiding technique [1, 15]. Liu et al. [7] used *SVD* to propose a watermarking algorithm for digital images. In their algorithm, singular values of the cover image are calculated and watermark is then added into these values to get resultant matrix of singular values. This resultant matrix of singular values is again transformed using *SVD* for finding the modified singular values. Ganic et al. [8] proposed a wavelet transform based watermarking technique in which the wavelet coefficients of the cover image are obtained using DWT and then *SVD* transform is performed on these wavelet coefficients and watermark image. To embed the watermark bits, singular values of watermark and the cover image are added and finally watermarked image is generated using inverse *SVD* transform. Chang et al. [9] used diagonal matrix and unitary matrix of cover image to conceal the bits of watermark. Chandra et al. [10] proposed a watermarking technique in which the singular values of the watermark are embedded in the singular values of the cover image.

Aslantas [11] combined the concept of *GA* [22] and *SVD* to propose a watermarking technique. In their technique, *GA* is utilized to obtain the highest robustness without losing transparency. Abdallah et al. [12] utilized left singular vectors of cover image to propose a steganography approach. Secret data bits in their approach are embedded into left singular vectors which reduces the embedding errors and the image fidelity is also maintained. Hybrid image watermarking scheme using *DWT*, *DCT* and *SVD* is proposed by Hu et al. [13]. In this scheme, the cover image is transformed into *YCbCr* color space from the *RGB* color space to obtain on grey level image and hybrid transforms are applied. *SVD* is then applied to obtain frequency components to embed the watermark bits.

Kasana et al. [14] proposed a histogram based steganography technique for *JPEG*2000 compressed images in the wavelet domain. Peak wavelet coefficients of the histogram are used to embed secret data and their technique provides a good embedding capacity and high visual quality stego image. But their technique is applicable to the lossless compression only. Going through these literature surveys, one can find that there is the need to design a steganography technique for *JPEG*2000 lossy compressed images which can provide high embedding payload as well as acceptable quality of stego images.

This paper proposes steganography technique using *SVD* for *JPEG*2000 compressed images. The singular values of the cover image are altered to embed the secret data by employing *SF*. Since the values of scale factors determine the strength of secret data embedded in the cover image. *GA* is used to find the optimal value in order to enhance the visual quality of the stego image and the robustness of the proposed technique.

The paper is structured into following sections. The embedding and extraction algorithms and optimization of *SF* are described in section 2. Experimental results and steganalysis tests are discussed in section 3 and section 4, respectively, prior to conclusion in last section.

2. PROPOSED STEGANOGRAPHY TECHNIQUE

In proposed technique, *SVD* is applied on wavelet coefficients of cover image and then secret data is embedded into transformed wavelet coefficients after scaling by a scaling factor *SF* before embedding process. *SF* is used to control the secret data strength.

2. 1. Embedding Algorithm

Following steps are used to embed secret image into a cover image.

Step 1. Decompose the cover image upto three levels using *DWT* to obtain ten wavelet subbands b_i; $1 \le i \le 10$.

Step 2. Apply *SVD* on each subband b_i to get the following decomposition.

$$b_i = [U_i \, S_i \, {V_i}^T]$$

Step 3. Modify the singular values of S_i using *SF* and secret image to get new matrix S_i^{new}. Here α is value of *SF* (0< α <1) which is optimized using *GA* and Se is the secret image.

$$S_i^{new} = S_i + \alpha \times Se$$

Step 4. Since the secret image is directly added to the singular values of the subbands using scaling factor, it is wise to reconstruct it by applying *SVD* again on modified singular values S_i^{new} as a result three another matrices are obtained.

$$S_i^{new} = [U_i' \, S_i' \, {V_i'}^T]$$

Step 5. Take inverse of *SVD* by taking product to form modified subbands b_i'.

$$b_i' = (U_i \times S_i' \times {V_i}^T)$$

Step 6. Compress the modified wavelet subbands b_i' using remaining processes of *JPEG*2000 encoder.

2. 2. Use of Comment Marker *JPEG*2000 code stream is structured as a main header followed by a sequence of tile streams. There are many boxes in the main header which are used by the encoder as well as by the decoder. One of the boxes is comment (*COM*) marker box which provides a facility for including unstructured comment information in the code stream of a compressed image when this image is compressed using *JPEG*2000 encoder. The *COM* marker segment is shown in Figure 1. *TY* parameter is a two byte unsigned integer. *TY*=1 indicates that the Comment Data comprises a equence of bytes in the form of IS 8859-15:1999(Latin) character data. *TY* = 0 indicates general library Comment Data. No other values for *TY* are allowed in *JPEG*2000. The *COM* marker segment length satisfies 5<= L_{COM}<=65535. Here L_{COM} is the length of the box.

COM	L_{COM}	TY	Comment Data

Figure 1. *COM* marker of *JPEG*2000 Header

In this proposed technique, two *SVD* based vectors built by singular values for each wavelet subband Sb_i of the cover image, S_i and S_i^{new} are transmitted to the decoder for the secret image extraction. This *COM* box is not used by the decoder so any value can be stored in this box. Extra information stored in the *COM* marker segment depends upon the size of the cover image. For example, size of cover image is 512×512. If three level wavelet transform is used to decompose the cover image, then we get three subbands of size 256×256, three subbands of size 128×128 and four subbands of size 64×64. If we apply *SVD* on 128×128 size data, singular values of size 128 are obtained. So for all subbands, total singular values are 1408. As S_i and S_i^{new} need to be transmitted to the receiver side, so total singular values are 1408 + 1408 = 2816. These are stored into *COM* marker and extracted on the receiver side which makes the proposed technique semi blind in nature.

2. 3. Extraction Algorithm

Step 1.Extract information stored in the COM marker and then apply *Tier*-2 of the *JPEG*2000 standard followed by *Tier*-1 on stego image. Then perform three level wavelet transform to get wavelet subbands b_i'.

Step 2.Apply *SVD* on each wavelet subbands to obtain matrix S_i'' for each subband *i*.

$$b_i' = [U_i'' \; S_i'' \; {V''_i}^T]$$

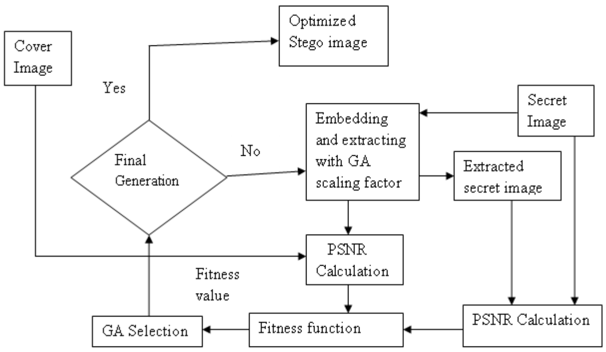

Figure 2. Flowchart for *GA* based steganography

Step 3. Apply *SVD* on S_i^{new} to obtain three matrices U_i', S_i' and ${V_i'}^T$.

$$S_i^{new} = [U_i' \; S_i' \; {V_i'}^T]$$

Step 4. Calculate the difference between S''_i and S_i'

$$S_i^{w2} = b \times S''_i + (1-b) \times S_i'$$

where b is factor having value between 0 and 1in order to improve the quality of extracted image.

Step 5.Multiplying matrices U_i', $S_i^{w2}$and V_i' to get new matrix S_i^{w3}.

$$S_i^{w3} = (U_i' \times S_i^{w2} \times {V_i'}^T)$$

Step 6. Extract the secret data using below equation:

$$Extracted\ data = \frac{(S_i^{w3} - S_i)}{\alpha}$$

Here, ^{T} is the transpose of matrix.

2. 4. Optimization of *SF* Using *GA* In proposed technique, the value of *SF* is optimized using *GA* in order to achieve visual quality of the stego images. An effective steganography has two conflicting requirements: $PSNR_1$which is *PSNR* between cover image and its stego version and $PSNR_2$ which is *PSNR* between original secret image and extracted secret image. These two requirements are correlated in such a way that maximization of one *PSNR* decreases the value of other *PSNR* and vice versa. If *SF* is increased then $PSNR_2$ of extracted image decreases and if the value of *SF* is decreased $PSNR_1$ increases. So there is the need to have optimal value of *SF* so that both requirements of $PSNR_1$and $PSNR_2$ are acceptable to the user. Using *GA*, the optimal value of *SF* is obtained.

Search Space: *GA*'s search space includes all the possible values of *SF*. The optimal value of the *SF*, selected properly from this search, may result in good imperceptibility of steganography technique. *GA* is used to find such optimal value. It is an iterative procedure which is used to achieve optimization using the genetic operators like selection, reproduction, crossover and mutation and a fitness function.

The Fitness Function: Fitness function *Fi* used by *GA* is formed by adding two common performance evaluation metrics $PSNR_1$ and $PSNR_2$.

$$Fi = PSNR_1 + PSNR_2 \quad (2)$$

Steps are used in optimization of *SF*, as shown in Figure 2.

3. EXPERIMENTAL RESULTS

Proposed technique is implemented using *JASPER* software tool [16]. *PSNR*, evaluated between cover image and its stego version, is taken as an evaluation parameter. It gives the statistical difference between the cover image and stego image and it is calculated using following equation:

$$PSNR = 10\log_{10}\frac{(2^z-1)^2}{MSE}$$

where z is the bit depth of the image, MSE is the mean square error and is defined as:

$$MSE = \sum_{m=1}^{h}\sum_{n=1}^{w}\frac{\left(Y(m,n)-X(m,n)\right)^2}{h\times w}$$

where $Y(m,n)$ is the pixel of stego image and $X(m,n)$ is the pixel of cover image, h and w are the height and width of the images, respectively. The larger the *PSNR*, better is the quality of stego image. In general, a stego image is acceptable by human perception if its *PSNR* is greater than 30 dB [20, 21]. The *PSNR* is used for evaluating the imperceptibility of data hiding techniques. In order to show the effectiveness of the proposed technique, eight images, namely, Lena, Boat, Baboon, Bridge, Couple, Crowd, Pepper and Airplane are used as cover images, each of size 512×512. Barbara image of size 256×256 is taken as secret image. These cover images are compressed using different bit rate, namely, 4 bits per pixel (*bpp*), 2 *bpp*, 1 *bpp* and 0.5 *bpp*. *SF* is used in embedding process and the optimal value of *SF* is determined using *GA*. Five generations with 20 population size are considered in *GA* optimal process using fitness of (2). Then secret image is embedded into cover image while compressing using *JPEG*2000 standard, using optimal *SF* value. Same value of *SF* is required in the extraction process to extract the bits of the secret image. These results are presented in Table 1.

TABLE 1. PSNR values of Stego, extracted images and Fitness Function at different bit rates

Image	Compression rate (in *bpp*)	*SF*	*PSNR* between cover and stego image(dB)	*PSNR* between secret and extracted image(dB)	Fitness function(dB)
Lena	0.5	0.0128	41.9778	37.3690	79.3468
	1	0.0121	42.3777	40.4160	82.7937
	2	0.0163	62.8817	43.0685	105.9556
	4	0.0135	59.8595	48.4600	108.3195
Boat	0.5	0.0108	42.5444	32.7005	75.2449
	1	0.0258	56.9242	35.4283	92.3526
	2	0.0147	60.3981	40.1746	100.5727
	4	0.0165	59.1585	45.8956	105.0541
Baboon	0.5	0.0167	41.1318	26.0706	67.2024
	1	0.0172	51.7809	30.1322	81.9131
	2	0.0339	56.2301	36.2695	92.4996
	4	0.0280	56.3471	44.2034	100.55.5
Pepper	0.5	0.0254	46.3629	32.4005	78.7635
	1	0.0239	53.4267	34.3730	87.7997
	2	0.0125	59.3401	38.4398	97.7799
	4	0.0165	58.7752	44.4486	103.2237
Crowd	0.5	0.0151	47.8918	32.8942	80.7860
	1	0.0120	58.9368	37.6524	96.5892
	2	0.0139	59.8273	42.6664	102.4937
	4	0.0108	57.3945	47.0427	104.4372
Couple	0.5	0.0165	47.0583	32.2345	79.2110
	1	0.0151	58.0380	36.2200	94.2580
	2	0.0177	62.8419	40.6095	103.4814
	4	0.0122	60.4361	46.9275	107.3636
Bridge	0.5	0.0211	43.5567	26.8258	70.3825
	1	0.0192	51.8156	30.1249	81.9402
	2	0.0244	54.6305	35.6631	90.2936
	4	0.0227	58.3084	42.8909	99.6301
Airplane	0.5	0.0484	35.4212	27.5382	62.9594
	1	0.0235	59.3622	38.9899	98.3501
	2	0.0192	62.2953	42.6105	104.9058
	4	0.0118	57.8692	47.9833	105.8525

Figure 3. (a) Lena cover image, Lena Stego at (b) 4 bpp, (c) 2 bpp, (d) 1 bpp, (e) original Barbara secret image, extracted Barbara secret image at (f) 4 bpp, (g) 2 bpp and (h) at 1 bpp

TABLE 2. Embedding Capacity/*PSNR* comparison of stego image using proposed technique and existing techniques for *JPEG*2000 Images

Image	Zhang et al.[6]	Ishida et al. [17]	Ishida et al. [18]	Goudia et al. [19]	Proposed Technique
Boat	14000/-	-	-	-	524288/54.75
Lena	14000/-	19568/ 37.1	14936/37.4	6768/34.29	524288/51.77
Pepper	14000/-	19568/ 36.3	14936/35.2	-	524288/54.47
Baboon	19500/-	19568/ 30.1	14936/33.25	10480/34.01	524288/51.37

-means *PSNR* of stego images is not given for particular image in particular technique

Cover image Lena and stego images at different bit rates are shown in Figures 3(a) to 3(d). Original secret image and extracted secret images at different bit rates are shown in Figures 3(e) to 3(h). From these images, one cannot observe any difference between cover and stego images. Hence imperceptibility is maintained using the proposed steganography technique. Also, the visual quality of the secret image is not degraded.

Proposed technique is compared with existing steganography techniques applicable to *JPEG*2000 compressed images. For this comparison, maximum embedding capacity of each existing technique is considered and then *PSNR* value between stego and cover images are taken into consideration at that capacity.

Maximum undetectable capacity of Zhang et al. [6] is 19,500 bits for Baboon image; undetectable utmost capacity of Ishida et al. is 19,568 bits and 37.1 *d*B *PSNR*; most undetectable capacity of Ishida et al. is 14,936 bits and *PSNR* is 37.4 *d*B; maximum capacity of Goudia et al. is 10,480 bits and *PSNR* is 34.29 *d*B whereas maximum undetectable capacity of proposed technique is 5,24,288 bits and *PSNR* is 54.75 *d*B. This comparison shows that proposed technique provides higher *PSNR* than existing at high embedding capacity.

4. STEGANALYSIS TESTS

Steganalysis tests are used to detect whether an image contains a hidden data. By analyzing different features between stego and cover images, a steganalysis test is able to detect stego images. To test the effectiveness of the proposed technique, three steganalysis tests have been performed on the stego images.

4. 1. Histogram Steganalysis First test is histogram steganalysis test. In this test, the histogram of cover image and its stego version is taken. Histograms of both types of images are almost similar. This shows that histogram steganalysis cannot detect the presence of secret image in the stego images.

Histogram of Lena and Baboon cover images are shown in Figure 4 (a) to 4(b) and histogram of stego images Lena, Baboon at 2 *bpp* and 1 *bpp* are shown in Figure: 4(c) to 4(f). From these figures, one can conclude that histogram of the cover and stego images are similar. Hence, on the basis of histogram, no one can suspect the existence of secret image embedded in the stego image.

4. 2. Chi-square Steganalysis Test Second test is Chi-square steganalysis test which is statistical test to measure similarity between set of observed data and an expected set of data. . Let *Cc* and *Cs* denote the Chi-square value of cover and stego image, respectively, and are calculated at different compression rates. Differences and percentage differences between *Cc* and *Cs* are shown in Table 3.

From this comparison, one can observe that there is small difference between Chi-square values of the cover image and stego image, *i.e* visual quality of stego image is not deviated from cover image.

Hence, on the basis of this test, no one can suspect the existence of secret image embedded in the stego image. So imperceptibility is achieved by the proposed technique.

4. 3. First and Second Order Moments Steganalysis Tests In these steganalysis tests, first and second order moments of different cover and stego images are calculated. For steganalysis purpose and also to show imperceptibility, mean μ and standard deviation *σ* *i.e.* first and second order moments, of cover and stego images, are used. The comparison between these characteristics of cover and stego images are shown in Table 4. From this comparison one can observe that difference in first and second moments of cover and stego images are very small and that it does not create the suspicion on the existence of secret data in the stego images. So imperceptibility is achieved using the proposed technique.

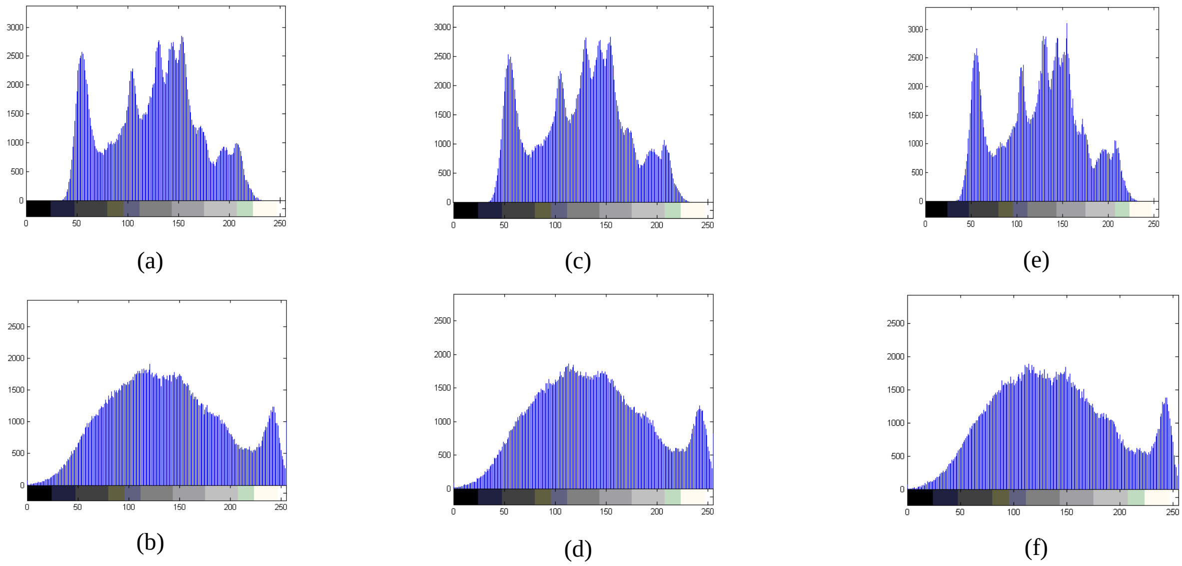

Figure 4. Histogram of cover images (a) Lena and (b) Baboon. Histogram of Stego at 2 bpp (c) and Lena (d) Babbon . Histogram of Stego at 1 bpp (e) Lena and (f) Baboon

TABLE 3. Chi-square test difference between cover image and stego image at different bit rates

Compression rate (in bpp)	*Cc* of cover image (in 10^6)	*Cs* of stego image (in 10^6)	Absolute difference (*Cs*-*Cc*) (in 10^6)	Percentage difference
		Lena image		
0.5	3.1889	3.2155	0.0266	0.8300
1	3.1889	3.1995	0.0106	0.3324
2	3.1889	3.2049	0.0160	0.5017
4	3.1889	3.1858	0.0031	0.0972
		Baboon image		
0.5	3.4384	3.2222	0.2162	6.2878
1	3.4384	3.4075	0.0309	0.8987
2	3.4384	3.5398	0.1014	2.9490
4	3.4384	3.4735	0.0351	1.0208

TABLE 4. First and second order moments of stego and cover images at different compression bit rates

Compression rate (in bpp)	Mean of cover image($\mu 1$)	Mean of stego image ($\mu 2$)	Absolute difference ($\mu 1 - \mu 2$)	Standard deviation of cover image ($\sigma 1$)	Standard deviation of stego image ($\sigma 2$)	Absolute difference ($\sigma 1 - \sigma 2$)
			Lena image			
0.5	125.1605	125.6820	0.5215	11.8995	12.0362	0.1367
1	125.1605	125.3129	0.1524	11.8995	11.9136	0.0141
2	125.1605	125.1925	0.0320	11.8995	11.8552	0.0443
4	125.1605	125.1475	0.0130	11.8995	11.8598	0.0397
			Baboon image			
0.5	137.7682	138.4722	0.7040	10.1646	10.6847	0.5201
1	137.7682	138.2763	0.5081	10.1646	10.2912	0.1266
2	137.7682	137.8592	0.0910	10.1646	10.0895	0.2017
4	137.7682	137.7349	0.0333	10.1646	10.0898	0.2014

5. CONCLUSION

A novel steganography technique for *JPEG*2000 compressed images using *SVD* and *GA* is proposed in this paper. *SVD* is applied on the wavelet coefficients of the cover images. Embedding of secret data bits is performed in singular values using *SF* and *GA* is used to optimize *SF*. Different compression rates are considered to compress the cover images using *JPEG*2000 encoder. Proposed technique's embedding capacity and *PSNR* are more than existing steganography techniques applicable for *JPEG*2000 compressed images. Steganalysis tests also confirm the imperceptibility of the stego images produced by proposed technique.

6. REFERENCES

1. Leon, S. J., Linear Algebra with Applications, Prentice Hall, New Jersey (Chapter 7), (1998).
2. Seo, Y., Kim, M. S., Park, H., Jung, H. Y., Chung, H. Y., Huh, Y. and Lee, J. D., " A secure watermarking for JPEG2000", ***IEEE***, (2001), 530-533.
3. Noda, H., Spaulding, J., Shirazi, M. N. and Kawaguchi, E., "Application of bit plane decomposition steganography to JPEG2000 encoded images", *IEEE Signal Processing Letters*, Vol. 9, (2002), 410-413.
4. Su, P. C. and Kuo, J., "Steganography in JPEG2000 compressed images**", *IEEE Transactions on Consumer Electronics***, Vol. 49. (2003), 824-832.
5. Hai-ying, G., Yin, X. and Guo-qiang, L., "A steganographic algorithm for JPEG2000 images*", IEEE computer society,* ***International Conference on Computer Science and Software Engineering***, (2008), 1263-1266.
6. Zhang, L., Wang, H., and Wu, R., "A high capacity steganography scheme for JPEG2000 baseline system", ***IEEE Transactions on Image Processing,*** Vol.18, (2009), 1797-1803.
7. Liu, R. and Tan, T., "An SVD based watermarking scheme for protecting rightful ownership", ***IEEE Transactions on multimedia***, Vol. 4, (2002), 121-128.
8. Ganic, E. and Eskicioglu, A. M., "Robust embedding of visual watermarks using DWT-SVD", ***Journal of Electronic Imaging***, Vol. 14, (2005), 43-54.
9. Chang, C. C., Tsai, P. C. and Lin, C., "SVD based digital watermarking scheme", ***Pattern Recognition Letters***, Vol. 26 (2005), 1577-1586.
10. Chandra, D. S., "Digital image watermarking using singular value decomposition", ***Proceedings of the 45th Midwest Symposium on Circuits and Systems***, Vol. 3, (2002), 264-267.
11. Aslantas, V., "A singular value decomposition-based image watermarking using genetic algorithm", ***International Journal of Electronics and Communications***, Vol. 62, (2008), 386-394.
12. Abdallah, H. A., Hadhoud, M. M. and Shaalan A. A., "An efficient SVD image steganographic approach", ***IEEE***, (2009), 257-262.
13. Hu, W. C., Chen, W. H. and Yang, C. Y., "Robust image watermarking based on discrete wavelet transform-discrete cosine transform-singular value decomposition", ***Journal of Electronic Imaging,*** Vol. 21, (2012), 1-7.
14. Kasana, G., Singh, K. and Bhatia, S. S., "Steganography technique for JPEG2000 compressed images using histogram in Wavelet Domain", ***International Journal of Security and its Applications,*** Vol. 8, No.6, (2014), 211-224.
15. Ling, H. C., Raphael, C., Phan, W. and Heng, S. H., "On the security of ownership watermarking of digital images based on singular value decomposition", ***Journal of Electronic Imaging, Letters,*** (2011), 1-2.
16. JASPER software, www.ece.uvic.ca/~frodo/jasper/
17. Ishida, T., Yamawaki, K., Noda, H. and Niimi, M., "Performance improvement of *JPEG*2000 steganography using QIM", ***Journal of Communication and Computer***, Vol. 6, (2009), 1-5.
18. Ishida, T., Yamawaki, K., Noda, H. and Niimi, M., "An Improved *QIM-JPEG*2000 Steganography and Its Evaluation by Steganalysis", ***Journal of Information Processing***, Vol. 17, (2009), 267-272.
19. Goudia, D., Chaumont, M., Puech, W. and Said, N. H., "A Joint Trellis Coded Quantization Data Hiding Scheme in the *JPEG*2000 Part-2 Coding Framework", ***19th European Signal Processing Conference,*** Sept, (2011), 1110-1114.
20. Hassanpour H. and Asadi S. R. "Image Enhancement using pixel wise gamma correction", ***International Journal of Engineering –Transaction B: Applications***, Vol. 24, No. 4,(2011), 301-312.

21. Hassanpour H. and Ghadi A. R. "Image Enhancement via Reducing Impairment Effects on Image Components", ***International Journal of Engineering–Transaction B: Applications*** Vol. 26, No. 11, (2013), 1267-1274.

22. Guo Z., Wang S., Yue X., Jiang D. and Li K. "Elite opposition –based Artificial Bee Colony algorithm for global optimization", ***International Journal of Engineering –Transaction C:Aspects***, Vol. 28, No. 9,(2015),1268-1275.

Singular Value Decomposition based Steganography Technique for JPEG2000 Compressed Images

G. Kasana[a], K. Singh[b], S. Singh Bhatia[c]

[a] *Computer Science and Engineering Department, Thapar University, Patiala-147004 India.*
[b]*Electronics and Communication Engineering Department, Thapar University, Patiala-147004, India.*
[c] *School of Mathematics, Thapar University, Patiala-147004, India*

PAPER INFO

Paper history:
Received 18 June 2015
Received in revised form 17 November 2015
Accepted 24 December 2015

Keywords:
Discrete Wavelet Transform
Singular Value Decomposition
Peak Signal to Noise Ratio
Genetic Algorithm
Scaling Factor

چکیده

در این مقاله، یک روش پنهان نگاری برای فشرده سازی تصاویر JPEG2000 با استفاده از تجزیه مقدار منفرد در دامنه تبدیل موجک ارائه شده است. در این روش، تبدیل موجک گسسته (DWT) در عکس روی جلد اعمال می شود تا ضرایب موجک به دست آید و تجزیه مقدار منفرد (SVD) روی این ضرایب موجک اعمال شد تا مقادیر منفردشان حاصل گردد. بیت داده های پنهان با استفاده از فاکتور مقیاس بندی در این مقادیر منفرد قرار داده می شوند. نرخ فشرده سازی مختلف نیز برای تصاویر JPEG2000 پس از تعبیه تصاویر مخفی در نظر گرفته می شود. از الگوریتم ژنتیک (GA)برای بهینه سازی مقدار SFاستفاده می شود. حداکثر ظرفیت روش پیشنهادی ۲۵٪ از اندازه عکس روی جلد است و حداکثر ارزش PSNR بین پوشش و تصویر stego بیشتر از PSNR تکنیک های موجود است. ظرفیت جاسازی روش پیشنهادی نیز بالاتر از ظرفیت جاسازی تکنیک های موجود است. همچنین، PSNR بین تصویر مخفی و تصویر استخراج شده بالا است و از این رو کیفیت بصری تصویر مخفی استخراج شده به اندازه کافی برای سیستم بینایی انسان خوب است. تست Steganalysis در تصاویر stego غیر محسوس بودن روش پیشنهادی را نشان می دهد.

***doi**:10.5829/idosi.ije.2015.28.12c.04*