Analysis on the Robustness SVD-Based Watermarking Algorithms

Zoran Milivojević
Department of Communicanion
Technical College
Niš, Serbia
e-mail: zoran.milivojevic {at} vtsnis.edu.rs

Zoran Stevanović
Department of Communicanion
Technical School 'Mija Stanimirović'
Niš, Serbia

Abstract—**This paper deals with the testing of the robustness of two algorithms for embedding and extraction of digital watermark into a monochromatic image, based on SVD transformation. The first algorithm was proposed by Liu and Tan [1], and the second, named Technique 1, was proposed by Mohammad et al. [3]. In the first part of the paper, the influence of the watermark contents on the the image for both algorithms was analyzed. Thus, the optimal scale factor of embedding watermark was determined. Then, the images with the watermark were tested under the conditions where various deformations were applied. The robustness was analyzed as well on the basis of objective and subjective parameters. In the second part of paper, impulse noise with percentage of 10-50% was added to the watermark images. Then, an efficient algorithm for impulse noise elimination was applied. The watermark was extracted from the reconstructed images and its quality was analyzed on the basis of subjective and objective parameters. PSNR and correlation coefficient rcorr were used as objective parameters. The visibility of the extracted watermark was used as a subjective parameter. On the basis of the results, an estimation of the robustness of the tested algorithms was made.**

Keywords-Image processing; digital watermarking; SVD transformation; impulse noise;

I. INTRODUCTION

The modern way of comunication via local and global computer network, simple access and exchange of data, have made it possible for illigal access and reproduction of digital information. Consequences are massive violations of copyright. For that reason the problem of ascertaining of technical solution for copyright protection is actual today. One of the most advocated solutions is introducing of the digital watermark [1,2]. The basic idea of the digital watermark is embedding of the watermark signal into the original information (audio, image or video) in order to protect the copyright, control the access to the original information etc. Embedding of the digital watermark can be performed in: a) space and b) frequency domain. In the space domain embedding is performed by direct modification of pixel values of the original image [4,5]. In transformation domain the watermark is embedded by modulation of transformation coefficient. For that purpose complex transformation are used like Singular Value Decomposition SVD [1,3,15-20], Discrete Cosine Transformation DCT [6,7], Discrete Wavelet Transformation DWT [8]-[11], Discrete Fourier Transform DFT [12].

In the paper [1] Liu and Tan proposed the algorithm for embedding and extracting the watermark into a image based on SVD transformation. As the main caracteristics of the proposed algorithm, they emphasized: a) security and b) the robustness of the embedded watermark. Algorithm was tested by applying the following attacks on the image with watermark: a) adding noise**,** b) low pass filtering**,** c) JPEG compression**,** d) scaling, e) image cropping and f) rotation**.** They confirmed the superiority of their solution over the metod proposed by Cox [2]. Since then, many authors have dealt with SVD transformation and suggested various algorithms for watermark embedding and extraction [15]-[20].

Zhang and Li [14] showed that algorithm proposed in [1] made a false positive detection possible, which means that except the original watermark, some other watermark can be extracted besides the original one. If this is a case, the copyright seems impossible to be proved.

Taking into account the results of Zhang and Li [14], Mohammad et al. proposed in [3] the modification of the algorithm made by Liu and Tan [1], now under the name Technique 1. As the main characteristics of this solution, they emphasized: a) overcoming a false positive detection, b) robustness, c) noninvertibility and d) less operations (saving up to $15(N)^3$). However, in [3] Technique 1 was not tested. So, the emphasized characteristics were not experimentally proved.

In this paper, a comparative analysis of the robustness of the algorithms for embedding of the digital watermark was made, as proposed by Liu and Tan [1] and Mohammad et al. [3] Technique 1. A image and a watermark of the same dimensions was used. In the first part of the paper, the chosen watermark (white letters on a black background) and its inverse variant (black letters on a white background) were used, in order to analyze the influence of the contents of the watermark over the factor of embedding α. On the basis of the obtained results, the embedding factor α for both algorithms was defined. Thus, in both cases the peak-signal-to-noise-ratio was the same. Both images with the watermark were exposed to the same attacks as in [1]: compression, rotation, an image cropping, resizing, low pass filtering, an addition of an impulse (salt & peppers) and

Gaussian noise. As seen in [1] and [3], the analysis of the robustness of the proposed watermarking algorithms in the presence of the impulse noise with random spatial determination wasn't done.

In the second part of the paper, the watermark robustness testing was done through the following steps: *Step 1*: Impulse noise with the percentage of p=10-50% was added to the image with the watermark; *Step 2*: applying the efficient algorithm as it was proposed in the paper [13], a noise elimination was done with a great percentage (98.92-99.6%); *Step 3*: the watermark extraction from the reconstructed image.

The results obtained by these tests can show a real robustness of the algorithm for embedding and extracting the watermark in comparison with the influence of impulse noise. PNSR (peak-signal to noise ratio), correlation coefficient r_{corr} were used as objective parameters for analyzing the gained results. The extracted watermark visibility was used as a subjective parameter for the same purpose.

The paper was organized as follow. The algorithms for embbeding and extaction of the watermark and extraction of the impulse noise from the image, were presented in the section II. Section III, presents the testing algorithm. Section IV, presents experimental results and the comparative analysis. Finally, Section V, gives the conclusion.

II. ALGORITHMS USED IN THE PAPER

A. LIU and TAN algorithm

Algorithm proposed in [1] (hereafter called **Algorithm 1)** for watermark embedding is based on SVD transformation and consists of the following steps:

Step 1: SVD transformation is performed over the original image *A* dimensions *nxn*:

$$A = U\Sigma V^T , \quad (1)$$

where *U*, *Σ* and *V* are matrices one of which is *Σ* diagonal matrix whose elements are singular values of *A* and ordered in a decreasing order and *U* and *V* are unitary matrices.

Step 2: To the matrix *Σ* a watermark W_{nxn} is added and the new matrix Σ_n is obtained:

$$\Sigma_n = \Sigma + \alpha W , \quad (2)$$

where *α* represents the watermark embedding scale factor.

Step 3: Over the matrix Σ_n SVD transformation is performed:

$$\Sigma_n = U_w \Sigma_w V_w^T , \quad (3)$$

Step 4: The image with the watermark is obtained as:

$$A_w = U\Sigma_w V^T . \quad (4)$$

Algorithm for extracting the watermark out of image with noise A_w^* is performed in the following way:

Step 1: SVD transformation of the image with noise A_w^* is performed:

$$A_w^* = U^* \Sigma_w^* V^{*T} , \quad (5)$$

Step 2: By using of matrices U_w and V_w it is obtained:

$$D^* = U_w \Sigma_w^* V_w , \quad (6)$$

Step 3: The extracted watermark is obtained as:

$$W^* = (D^* - \Sigma) / \alpha . \quad (7)$$

From the presented algorithm it can be seen that for extraction of the watermark it is necessary to have the original matrices U_w, *Σ* and V_w.

The authors pointed out the following caracterisics of the proposed algorithm: a) security and b) the robustness in contrast to many distortions of the image.

B. Mohammad et al. algorithm

Algorithm for watermark embedding proposed in [3] as Technique 1 (hereafter called **Algorithm 2**) consists of the following steps:

Step 1: SVD transformation is performed over the original image *A* dimensions *nxn*:

$$A = U\Sigma V^T , \quad (8)$$

Step 2: The watermark *W* is added to the matrix *Σ* and the new matrix Σ_n is obtained:

$$\Sigma_n = \Sigma + \alpha W , \quad (9)$$

where *α* represents the watermark embedding scale factor.

Step 3: The image with the watermark is obtained as:

$$A_w = U\Sigma_n V^T . \quad (10)$$

Algorithm for watermark extracting from the image with noise A_w^* is performed through following steps:

Step 1: SVD transformation of the image with noise A_w^* is performed:

$$A_w^* = U^* \Sigma_n^* V^{*T} . \quad (11)$$

Step 2: The extracted watermark is obtained as:

$$W^* = (\Sigma_n^* - \Sigma) / \alpha . \quad (12)$$

From the presented algorithm it can be seen that for extraction of the watermark it is necessary to have the original matrix *Σ*. They also mentioned: a) overcoming of the false positive detection problem, that appears in the Algorithm 1, which was proved in paper [14], b) robustness, c) noninvertibility and d) less operations.

C. Elimination of the impulse noise

The algorithm for impulse noise elimination used in this paper is proposed in the paper [13] hereafter called SODA (*Second-Order Difference Analysis*) algorithm as a non linear filter for impulse noise reduction. Pixels corrupted by the impulse noise are identified through two steps and filtered in one step. In the first step for identifying of corrupted pixels the local window 7x7 pixels is used. Potentially corrupted pixels detected in the first step are tested in the second step using the local window 3x3. The third step represents filtering pixels noise using median filter.

Testing of SODA algorithm turned out as exceptionally effective in detection of pixels corrupted by noise and in replacing of these pixels by new values. This algorithm gave also good results in preserving of fine details of the image. Percentage of elimination of the impulse noise ranged till 99%, and for that reason it was chosen for testing.

One of the aims of the testing is to make a comparative analysis between Algorithm 1 and Algorithm 2 with a respect to the robustness when impulse noise is applied. Impulse noise was added to the images with the watermark, and then a correction was made applying SODA algorithm. By applying Algorithm 1 and Algorithm 2 to the reconstructed images, the watermark is to be extracted. The basic idea for this kind of testing is that, if the algorithm is capable to almost thoroughly recover the image and make it usable, the presupposition of robustness implies that in such a image there must be a preserved watermark which can be extracted. Analyzing the obtained results, the performances of the algorithms can be proved.

III. THE TESTING ALGORITHM

The testing algorithm of the robustness of the embedded watermarks was carried out in two parts. The first part consisted of the following steps:

Step 1: The watermark *W*, in its basic and inverse variant *WI*, were embedded in the image *A* using of both algorithms with different scale factors α. The aim of the testing was to define the optimal scale factor and to show that watermark contents had an influence on the scale factor at both algorithms.

Step 2: By applying Algorithm 1 and Algorithm 2, the watermark *W* was embedded in the image *A*, with previously chosen scale factor *α*. The factor *α* in both cases was chosen in such a way that the ratio between the original image and the image with the watermark was PSNR=45 dB.

Step 3: The images were exposed to: JPEG compression, rotation, resizing, the white Gaussian noise, low pass filter, and applying Algorithm 1 and 2, the watermark is extracted.

Step 4: PSNR is calculated as well as the correlation coefficient r_{corr} for the extracted watermark.

The second part of the testing algorithm consisted of the following steps:

Step 1: Impulse noise was added to the images with the watermarks with percentage of 10%-50%.

Step 2: Applying SODA algorithm for noise elimination, impulsive noise filtration was done.

Step 3: Applying Algorithm 1 and Algorithm 2, the extraction of the watermark *W** was done.

Step 4: PSNR was calculated as well as the correlation coefficient r_{corr} for the extracted watermark.

Step 5: Based on the obtained result the analysis was made and the robustness estimation of the Algoritam 1 & 2 was done.

Correlation of the embedded and extracted watermark was calculated using MATLAB's function **corr2** and the relation of PSNR ginen by:

$$PSNR = 10 \log_{10}\left(\frac{255^2}{MSE}\right) , \quad (13)$$

$$MSE = \frac{1}{mn} \sum_1^m \sum_1^n \left| W - W^* \right|^2 . \quad (14)$$

In (14) *m* and *n* represent dimensions of the image and the watermark, *W* and W^* are embedded and extracted watermark, respectively.

IV. EXPERIMENTAL RESULTS AND COMPARATIONS

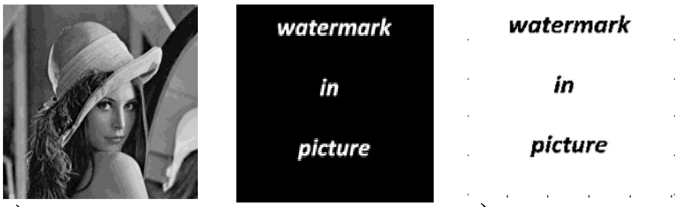
A. Testing parameters

Algorithms for testing described in Section 3. were applied to the image Lena A_{mxn} (Fig. 1.a), watermark W_{mxn} (Fig. 1.b) and watermark WI_{mxn} (Fig. 1.c), where m=n=512.

B. Experimental results

The results of the first part of the testing are shown in the Fig. 2 and 3, and in the Table 1 and Table 2. In the Fig. 2 and 3, the ratio between the original image and the image with the watermark is presented as expressed by PSNR. Its function is expressed by the scale factor *α* for both the watermark *W* and its inverse variant *WI*. As seen from the Fig. 2 and 3, one can conclude that a great care about the watermark contents and the scale factor *α* must be taken while the watermark embedding.

Due to the more convenient ratio between the PNSR and α, watermark W was chosen. On the basis of the objective results and the subjective estimation of the quality of the image with the watermark, the scale factor α was chosen, to give PSNR=45dB. For the Algorithm 1 and watermark W, the value of α=0.15, and for the Algorithm 2 under the same conditions α=0.03. These values were used in further testing.



a) b) c)

Figure 1. a) Image Lena A_{mxn}, b) Watermark W_{mxn} and c) Inverse watermark W_{mxn}.

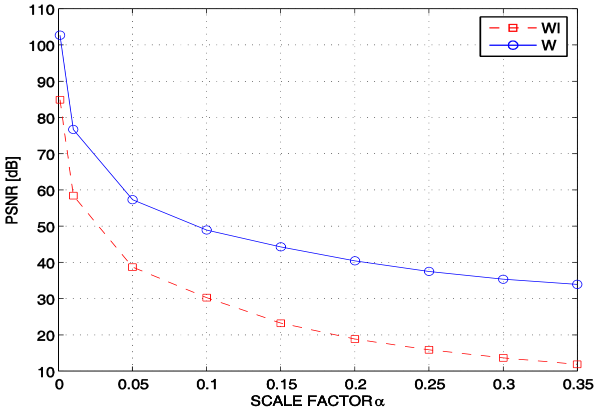


Figure 2. PSNR for the original and the image with the watermark, depending on the scale factor α for Algorithm 1.

The results of testing the images with the watermarks for both algorithms and mentioned attacks, were presented in the Table 1 and Table 2. The Tables gives the ratio between the original watermark and the extracted watermark after the mentioned attacks were applied. The ratio is expressed via PSNR and correlation coefficient r_{corr}. The extracted watermark is presented as well, in order for the visual quality to be rated.

Table 3 contains the results of SODA algorithm for elimination of the impulse noise in the image with the watermark. This Table is relevant both to the image with the watermark according to Algorithm 1 and to the image with the watermark according to Algorithm 2.

Table 4 contains the total results of robustness testing for both algorithms to the effect of the impulse noise in the percentage from 10-50%. Empty spaces in the Table 4 indicate that in those cases the watermark could not be extracted from the image.

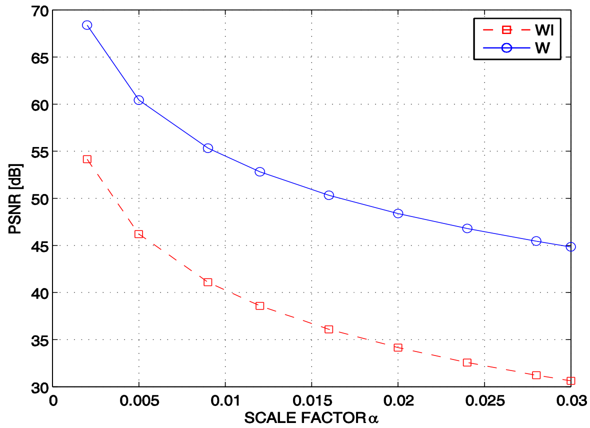


Figure 3. PSNR for the original and the image with the watermark, depending on the scale factor α for Algorithm 2.

TABLE I. RESULTS FOR ROBUSTNESS TESTING OF THE EMBEDDED WATERMARKS (ALGORITHM 1) TO THE EFECT OF THE ATTACKS.

Attack	Algorithm 1	
	PSNR	r_{corr}
No attack	276.1495	1
JPEG compression 25%	30.75	0.9879
Rotation 30 deg.	-5.9199	0.0824
Resize 25%	13.7848	0.6621
Salt & pepper 10% and median filter [3x3]	12.8741	0.5902
Low pass filter [16x16] σ=1	8.999	0.3680
Gaussian noise m=0, v=0.005	0.0469	0.1827
Cropping	0.4793	0.1919

TABLE II. RESULTS FOR ROBUSTNESS TESTING OF THE EMBEDDED WATERMARKS (ALGORITHM 2) TO THE EFECT OF THE ATTACKS.

Attack	Algorithm 2	
	PSNR	r_{corr}
No attack	265.77	1
JPEG compression 25%	14.72	0.3417
Rotation 30 deg.	-5.9199	0.0209
Resize 25%	3.6185	0.2119
Salt & pepper 10% and median filter [3x3]	3.0236	0.0615
Low pass filter [16x16] σ=1	-1.2234	0.0245
Gaussian noise m=0, v=0.005	-10.408	0.0529
Cropping	-9.9756	0.0583

TABLE III. EFFICIENCY OF THE ALGORITHM FOR ELIMINATION OF THE IMPULSE NOISE.

Noise percentage p[%]	Correctly detected points [%]	False detected points [%]
10	99.35	0.07
20	99.28	0.11
30	99.08	0.18
40	99.06	0.28
50	99.02	0.40

TABLE IV. RESULTS FOR ROBUSTNESS TESTING OF THE EMBEDDED WATERMARKS TO THE EFFECT OF THE IMPULSE INTERFERENCES.

Impulse noise p[%]	Algorithm 1		Algorithm 2	
	r_{corr}	PSNR	r_{corr}	PSNR
10	0.6432	13.4278	0.0402	3.3805
20	0.4914	10.3525	0.0247	0.3540
30	0.3899	8.3521	-[a]	-
40	0.3274	7.0095	-	-
50	0.2571	5.5043	-	-

a. Empty spaces indicate that in those cases the watermark could not be extracted from the image.

C. *Experimental results*

On the basis of the graphic presentation in the Fig. 2 and 3, the following may be concluded: the watermark contents have an influence over the original image with both algorithms in such a way that it influences the values of PSNR function and the scale factor. Thus, while the watermark embedded one must take care of both factors. On the basis of the results in the Fig. 2 and 3, the watermark *W*, the scale factor for Algorithm 1 (α=0.15), and for the Algorithm 2 (α =0.03) was chosen.

The following algorithm was used as a criterum for robustness evaluation. In the case: a) r_{corr}=0-0.2 robustness is extremely bad and watermark is invisible; b) r_{corr}=0.2-0.5 robustness is weak and watermark is hardly visible; c) r_{corr}=0.5-1 robustness is good and watermark is visible.

By analyzing the watermark extraction results in the case of the mentioned attacks, the following conclusions are reached.

I.a) On the basis of the results shown in the Table 1, for Alorithm 1 it can be concluded that the robustness is extremely bad and the extracted watermark is invisible and thus useless in the following cases: a) rotation (PSNR=-5.9199, r_{corr}=0.0824), b) Gaussian noise (PSNR=0.0469, r_{corr}=0.1827) and c) cropping (PSNR=0.4793, r_{corr}=0.1919) are applied. Robustness is weak and watermark is hardly visible in the case low pass filtration (PSNR=8.999, r_{corr}=0.368).

Robustness is good and watermark is visible in the following cases: a) JPEG compression 25% (PSNR=30.75, r_{corr}=0.9879), b) resizing 25% (PSNR=13.7848, r_{corr}=0.6621), and c) a salt & pepper 10% (PSNR=12.8741, r_{corr}=0.5902).

I.b) The robustness of the Algorithm 2 is satisfactory under none of the circumstances mentioned above.

The testing results of Algorithm 1 and Algorithm 2 were shown in the Tables 2 and 3 in the case impulse noise *p*=10-50% was added. They show the following:

II.a) Table 2 shows the exceptional efficiency of SODA algorithm for elimination of noise in detecting of pixels infected by noise (99.02-99.35%). In Table 3 in coloumn *Image with noise*, images with impulse noise *p* were shown. In coloumn *filtered image*, images with watermark after SODA algorithm application were shown. Filtered image in the Table 3 shows SODA algorithm effectivness in replacing of pixels with noise, i.e. in restoration of the image. Quality of the filtered image is good even in the cases of high percentage of noise (50%).

II.b) Algorithm 1 has a more complex process of embeding and extracting of the watermark, greater number of calculating operations, but it is much robuster and practically it is impossible to eliminate the watermark (Table 3, coloumn *Extracted watermark Algorithm 1*). When *p*=0-20%, r_{corr}=1-0.491 robustness is good and watermark is visible. When *p*=30-50% r_{corr}=0.389-0.257 robustness is weak, watermark is hardly visible. Therefore, the watermark shows the good characteristic of robustness, i.e. it is present in the image as long as the image is usable.

II.c) On the basis of the results shown in the Table 3 for Algorithm 2, it can be concluded that robustness is extremely bad and the extracted watermark is invisible even for the lowest percentage of impulse noise (*p*=10%, PSNR=3.38, r_{corr}=0.04).

Based on the obtained results, it may be concluded that Algorithm 2 proposed by the authors Mohammad et al. in [3], is not a better solution for embedded and extracted watermark in image then Algorithm 1 proposed by Liu and Than [1]. The exception has to be made for false-positive detection, which wasn’t subject of testing. Looking at the practical side with a respect to the robustness, Algorithm 2 seems to be useless.

V. CONCLUSION

In this paper, the comparative analysis of the robustness of Algorithm 1 and Algorithm 2 for digital watermark embedding, based on SVD transformation, was made. Algorithm 2 was proposed by the authors Mohammad et al. in [3], as a modification and a better version of Algorithm 1 proposed by Liu and Than [1]. The robustness was tested by applying many standard attacks (compression, rotation, image cropping, resizing, low pass filtering, an addition of impulse and Gaussian noise) in the first part of paper . In the second part of paper, the testing of images with watermark where impulse noise is added with the percentage of 10-50% was done. Before the watermark is extracted, preprocessing of the image with watermark is done by SODA algorithm in order to eliminate impulse noise. SODA algorithm showed a remarkable efficiency at impulse noise elimination over 99%.

The results have shown that both algorithms are very sensitive to the watermark contents, thus, for every chosen watermark, a scale factor must be determined respectively. The testing has also shown that Algorithm 1 had a far better robustness during all the tests, whereas Algorithm 2 was sensitive to all transformations that the image had gone through. In none of the elements it did show the characteristics of robustness. The simpler way of embedding apart, as authors have mentioned as a special advantage of Algorithm 2, all other advantages are prescribed to Algorithm 1. On the basis of the things mentioned above, it may be concluded that Algorithm 2 doesn't present a better version of Algorithm 1, especially when robustness comes to the question and thus, it has a very limited use.

REFERENCES

[1] R. Liu, T. Tan, "A SVD-based watermarking scheme for protecting rightful ownership", IEEE Trans. Multimedia, vol. 4, no. 1, 2002, pp. 121-128.

[2] I. Cox, J. Kilian, F. Leighton, T. Shamoon, "Secure spread spectrum watermarking for multimedia", IEEE Trans. Image Process., vol. 6, no. 12, 1997, pp. 1673-1687.

[3] A. Mohammad, A. Alhaj, S. Shaltaf, „An improved SVD-based watermarking scheme for protecting rightful ownership", Signal Process., vol. 88, 2008, pp. 2158-2180.

[4] I. Nasir, Y. Weng, J. Jiang, "A New Robust Watermarking Scheme for Color Image in Spatial Domain", Third International IEEE Conference on Signal-Image Technologies and Internet-Based System, 2007, pp. 942-947.

[5] L. Li, B. Guo, "Localized image watermarking in spatial domain resistant to geometric attacks", Int. J. Electron. Commun., (AEÜ), vol. 63, 2009, pp. 123-131.

[6] J. Hernandez, M. Amado, F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: detector performance analysis and a new structure", IEEE Trans. Image Process., vol. 9, no. 1, 2000, pp. 55-67.

[7] I. Natgunanathan, X. Yong, R. Yue, Z. Wanlei, G. Song, "Robust Patchwork-Based Embedding and Decoding Scheme for Digital Audio Watermarking", IEEE Trans. Audio, Speech, and Language Process., vol.20, no.8, pp.2232-2239.

[8] A. Bohraa, O. Farooq, "Blind self-authentication of images for robust watermarking using integer wavelet transform", Int. J. Electron. Commun. (AEÜ), vol. 63, 2009, pp. 703-707.

[9] K. Liu, "Wavelet-based watermarking for color images through visual masking", Int. J. Electron. Commun. (AEÜ), vol. 64, 2010, pp. 112-124.

[10] A. Reddy, B. Chatterji, "A new wavelet based logo-watermarking scheme", Pattern Recognition Lett., vol. 26, 2005, pp 1019-1027.

[11] W. Chuntao, N. Jiangqun, H. Jiwu, "An Informed Watermarking Scheme Using Hidden Markov Model in the Wavelet Domain", IEEE Trans. Inform. Foren. and Secur., vol. 7, no. 3, 2012, pp. 853-867.

[12] X. Wang, Z. Xu, P. Niu, "A feature-based digital watermarking scheme for halftone image", Int. J.Electron.Commun. (AEÜ), vol. 64, no. 10, 2010, pp. 924-933.

[13] D. Dang, W. Luo, „Impulse noise removal utilizing second-order difference analysis", Signal Process., vol. 87, 2007, pp. 2017-2025.

[14] X. Zhang, K. Li, "Comments on an SVD-based watermarking scheme for protecting rightful ownership", IEEE Trans. Multimedia, vol. 7, no. 3, 2005, pp. 593-594.

[15] C. Chang, P. Tsai, C. Lin, "SVD-based digital image watermarking scheme", Pattern Recognition Lett., vol. 26, 2005, pp. 1577-1586.

[16] W. Liyun, L. Hefei, Z. Fuhao, L. Zhengding, "Real-Time Compressed-Domain Video Watermarking Resistance to Geometric Distortions", IEEE Multimedia, vol. 19, no. 1, 2012, pp. 70 – 79.

[17] Y. Wu, "On the security of SVD based ownership watermarking", IEEE Trans. Multimedia, vol. 7, no. 4, 2005, pp. 624-627.

[18] F. Huang, Z. Guan, "A hybrid SVD-DCT watermarking method based on LPSNR", Pattern Recognition Lett., vol. 25, no. 15, 2004, pp. 1769-1775.

[19] A. Valizadeh, Z. Wang, "An Improved Multiplicative Spread Spectrum Embedding Scheme for Data Hiding", IEEE Trans. Information Forensics and Security, vol. 7, no. 4, 2012, pp. 1127-1143.

[20] V. Aslantas, „A singular value decomposition based image watermarking using genetic algorithm", Int. J. Electron. Commun., vol. 62, 2008, pp. 386-394.