Author(s):	Zolotavkin, Yevhen; Juhola, Martti
Title:	A New Blind Adaptive Watermarking Method Based on Singular Value Decomposition
Main work:	Proceedings of 2013 International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS)
Year:	2013
Pages:	184-192
ISBN:	978-1-4673-6451-5
Publisher:	IEEE
School / Other Unit:	School of Information Sciences
Item Type:	Article in Conference Proceeding
Language:	en
URN:	URN:NBN:fi:uta-201305281101

A New Blind Adaptive Watermarking Method Based on Singular Value Decomposition

Yevhen Zolotavkin
Computer Science, School of Information Sciences
University of Tampere
Tampere, Finland
yevhen.zolotavkin@uta.fi

Martti Juhola
Computer Science, School of Information Sciences
University of Tampere
Tampere, Finland
martti.juhola@sis.uta.fi

***Abstract*— A blind watermarking method on the basis of Singular Value Decomposition is proposed in this paper. Each bit of a watermark is being enclosed in 4x4 blocks. The method modifies the both left and right orthonormal matrices in order to embed a bit. A new embedding rule with adjustable parameters has been proposed for watermarking. The modification of orthonormal matrices is accomplished according to Van Elfrinkhof's rotational model. Distortions of watermark embedding are minimized. A criterion of watermarking performance has been proposed that combines robustness and transparency. An adaptation on the basis of the criterion has been employed. Popular attacks have been applied and experimental results have been represented. The proposed watermarking method demonstrates better robustness toward some attacks in comparison with other known blind watermarking methods.**

Keywords- Digital Image Watermarking, Singular Value Decomposition, Robustness, Distortions, Transparency

I. INTRODUCTION

Security of data is a very important requirement of modern society. There are many different aspects of security that are applicable in different circumstances. One of the most important aspects is a protection of digital rights for a work produced by an author. These kinds of information security problems are addressed by Digital Image Watermarking (DIW).

To protect a digital image by the means of DIW it is necessary to enclose a digital watermark that would witness an owner [1]. Therefore there are three important characteristics for a particular watermarking method: robustness, transparency and data payload.

Robustness is an ability to withstand different kinds of attacks [2]. It is impervious to provide robustness toward all the possible attacks especially if their intensities are high. Hence this requirement is quite specific. However, mostly robustness against noise, some kinds of filtering and geometric attacks is required. The most approved index of robustness for an extracted watermark is Bit Error Rate (BER).

Transparency is an ability to preserve original image by watermarking it. There are many measures of image quality that could be applied to define transparency quantitatively [3]. Though, the most popular measure is Peak Signal to Noise Ratio (PSNR).

Data payload is a number of watermark bits embedded into an image. There might be different requirements to data payload as there might be different kind of information to witness an ownership. Nevertheless higher payload provides better protection as the watermark can be more unique. Small binary graphical logos are the most popular choice in watermarking. Sequences of randomly generated bits without visual meaning are also favored.

The original image can be modified in many different ways to embed a watermark. Original pixel values can be changed directly which is a kind of spatial transform. Modification of the Least Significant Bit is a good example of such kind of transforms [1]. Another kind of embedding is to change coefficients that have some spectral meaning which is a frequency domain transform. Some suitable examples are watermarking methods on the basis of Discrete Cosine Transform (DCT) [4] and Discrete Wavelet Transform (DWT) [5]. Robustness and transparency can be greatly influenced by the kind of transform chosen for embedding. Usually modification of some spectral coefficients is more favorable as they are more robust against noise and image processing attacks.

Singular Value Decomposition (SVD) is a unique kind of transform [6]. It separates an image fragment on several independent layers. The number of layers is much less than that, for example, for DCT. Therefore the most important layer is quite stable to various attacks.

An efficiency of watermarking also depends on a rule exploited for embedding. Each embedding rule could have several parameters that influence robustness-transparency tradeoff. Those parameters could remain constant for the whole watermarking procedure or be different (adopted) for each independent block. Usually embedding with adopted parameters provides better watermarking performance.

There are many existing SVD-based watermarking methods. The best of them provide adaptation of embedding parameters. However, additional information is usually required for extraction which limits their usage. For those few methods that do not urge transfer of additional information embedding requires modification of more coefficients in a

block. This implies that larger blocks are used and lower data payload can be maintained.

In this paper we propose new SVD-based blind watermarking method with adaptation. The method does not need additional information except a key to extract a watermark. It uses the both orthonormal matrices obtained by SVD of 4x4 block to embed a bit of a watermark. The proposed method provides good robustness-transparency tradeoff and high data payload.

The rest of the paper is organized as following: a short review of relevant watermarking methods exploiting SVD is given in the Section II; Section III bears our own approach which is described in detail; then, some experimental results are represented in Section IV followed by a discussion of their importance in Section V; finally, in Section VI the paper is concluded by general remarks regarding relevance of our approach and its influence on future research.

II. SVD-BASED WATERMARKING

An image fragment I_k of size $n \times n$ is being decomposed according to SVD [6] in the following way:

$$I_k = USV^T = \begin{pmatrix} U_{1,1} \cdots U_{1,n} \\ U_{2,1} \cdots U_{2,n} \\ \vdots \\ U_{n,1} \cdots U_{n,n} \end{pmatrix} \times \begin{pmatrix} S_{1,1} & 0 & \cdots & 0 \\ 0 & S_{2,2} & \cdots & 0 \\ & & \vdots & \\ 0 & 0 & \cdots & S_{n,n} \end{pmatrix} \times \begin{pmatrix} V_{1,1} \cdots V_{1,n} \\ V_{2,1} \cdots V_{2,n} \\ \vdots \\ V_{n,1} \cdots V_{n,n} \end{pmatrix}^T, \quad (1)$$

where U and V are some orthonormal matrices and S is a diagonal matrix of singular values.

An alternative representation demonstrates that fragment I_k is being decomposed on n independent layers where geometry of i-th layer is defined by a pair of i-th columns (one from matrix U and one from V) and a luminance component $S_{i,i}$:

$$I_k = \sum_i S_{i,i} U(1 \dots n, i) V(1 \dots n, i)^T \quad (2)$$

The luminance $S_{1,1}$ has the biggest value and mostly this value is much bigger than the other values $S_{i,i}$, $i > 1$. Therefore the first layer is the most substantial and provides the best robustness for watermarking.

A. Methods Modifying Singular Values

Popular strategy for SVD-based methods that modify singular values is to quantize the biggest value of a block depending on the corresponding bit of a watermark.

The first paper introducing SVD for Digital Image Steganography and Watermarking was [7]. A blind technique with high data payload and without adaptation was proposed for color RGB images. However, the resulting robustness-transparency tradeoff was not satisfying mostly because of inability to quantize singular values of different blocks with different steps.

Another pioneering paper exploiting SVD for watermarking is [8] where noninvertible non-blind scheme was introduced. However, later in [9] it has been shown that the scheme is vulnerable to a kind of attack counterfeiting an original watermark because too much of reference information should be saved for a detector.

In the paper [10] the first in the literature DWT-SVD watermarking method was proposed. The method demonstrates good robustness and provides high data payload. However, distortion of original image is quite considerable, the method is non-blind and does not assume an adaptation.

The method proposed in [11] applies adoptive quantization to DWT-SVD. The method is robust against JPEG-compression. However, it is made deliberately fragile to other kinds of distortions like noise, median filtering or cropping. The information about quantization steps for all blocks should be transmitted. Another drawback is considerable degradation of original image.

Among the recent works exploiting adoptive quantization of singular values the paper [12] introduces quite robust watermarking method. However, information about quantization parameters should be transferred to extract a watermark.

One of the most robust blind watermarking schemes based on SVD-DCT transform was proposed in [13]. Two bits of a watermark are being embedded in 32x32 macro-block. An adaptation is applied to each block. The method does not require any additional information except a key for extraction.

B. Methods Modifying Orthonormal Matrices

In the literature there are few watermarking approaches that modify orthonormal matrices of SVD. The advantage of such kind of watermarking is that more elements are available for modification.

The paper [14] proposes a watermarking method that modifies the left orthonormal matrix of SVD. The whole image of size 512x512 is split on fragments 4x4 and SVD is applied to each of them. A bit of the watermark is embedded by modifying the second and the third elements in the first column of left orthonormal matrix. The method provides sufficient data payload and quality of watermarked images which PSNR was higher than 42 dB. However, robustness toward common distortions like JPEG-compression, Gaussian noise and cropping is not high.

Another paper exploiting the idea of embedding a watermark in orthonormal matrix of SVD is [15]. The watermarking scheme proposed in [14] was developed further in order to improve robustness-invisibility tradeoff. Instead of embedding a bit of a watermark with constant threshold for all the blocks the authors proposed to adjust the threshold. The adjustment is done in a way that PSNR of each modified blocks is higher 42 dB whenever it is possible. The method provides considerable data payload equal to 2048 bit per

image. Robustness-invisibility tradeoff is also better compared to [14]. Nevertheless its robustness is not sufficient toward, for example, JPEG-compression.

There are several shortcomings in the mentioned above two methods proposed in [14] and [15]. First modified matrices are not orthonormal which could cause an embedded bit to be lost even without influence of the third person or noise. Second none of the methods uses an adequate criterion to adapt the threshold for each block. The PSNR-based criterion and 42dB limit are not obvious. Third both methods utilize only the left orthonormal matrix while utilization of the both could provide more elements for watermarking and improve robustness-transparency tradeoff.

III. Proposed Watermarking Method

Proposed in this paper watermarking method modifies U and V that are left and right orthonormal matrices of SVD of particular image block I_k.

Each new watermarked image fragment I'_k that carries corresponding bit is composed from two orthonormal matrices $\{U', V'\}$ and a diagonal matrix of singular values:

$$I'_k = U'S'(V')^T. \tag{3}$$

Image block I'_k should be decomposed by SVD again in order to extract a bit. The decomposition always returns orthogonal matrices. With the aim to assure that a bit is extracted correctly matrices U' and V' should be orthogonal when I'_k is composed. Otherwise the matrices of the decomposition will not be the same as the matrices used to compose a watermarked block.

In order to provide orthogonality of U' and V' a multiplication with rotational matrix can be applied. Any rotational matrix R is always orthonormal and multiplication with another orthonormal matrix, for example, U will produce new orthonormal matrix. Any column of U could be seen as a point and rotation according to R changes coordinates of a point. This kind of modification of coordinates of a point can be used to embed a bit.

Our method embeds each bit of a watermark in a square fragment of image which size is 4×4. Only the first column of U and the first column of V represent a watermark bit. Transforms that are necessary for watermarking can be defined as $T_L: U \to U'$, and $T_R: V \to V'$. New watermarked matrices $\{U', V'\}$ are defined using rotation matrices R_U and R_V:

$$U' = R_U U, \tag{4}$$

$$V' = R_V V. \tag{5}$$

A. Embedding Rule

Modified matrices $\{U', V'\}$ should satisfy some requirements necessary for proper extraction of a bit of a watermark. Those requirements can be expressed in a watermarking rule. Further we use a definition of transposed first columns of U' and V' respectively: $\boldsymbol{u}' = [U'(1,1), U'(2,1), U'(3,1), U'(4,1)]$, $\boldsymbol{v}' = [V'(1,1), V'(2,1), V'(3,1), V'(4,1)]$. Two main components of a rule are reference matrix Ref and a threshold Th. The rule is expressed as the following equation:

$$(-1)^{bit}\left(\boldsymbol{u}' Ref \boldsymbol{v}'^T - m\right) = Th, \tag{6}$$

where m is a mean of the term $\boldsymbol{u}' Ref \boldsymbol{v}'^T$. Higher threshold Th implies higher level of embedding distortions, but the robustness is also higher. To extract a bit of a watermark it is necessary to calculate the following expression:

$$bit = \left(2 + sign\left(\boldsymbol{u}' Ref \boldsymbol{v}'^T - m\right)\right) mod\ 3. \tag{7}$$

B. Minimization of Embedding Distortions

While robustness of a watermark depends on the parameters of embedding rule invisibility of a watermark is a subject for minimization of some criteria as, for example, a Residual Sum of Squares (RSS) between original and altered pixel values of a block. In this subsection we presume that the proposed embedding rule is used and the both matrices U and V are being modified.

The proposed goal function G for a watermarked fragment I'_k is:

$$G = \|I'_k - I_k\|_2^2. \tag{8}$$

The goal function can be rewritten in order to include rotational matrices R_U and R_V:

$$G = \|I'_k - I_k\|_2^2 = \|U'S'(V')^T - I_k\|_2^2 = \\ = \|US'V^T - R_U^T I_k R_V\|_2^2 . \tag{9}$$

If we define $S' = S + \Delta S$ where ΔS is also a diagonal matrix, expression (9) becomes:

$$G = \|U\Delta S V^T + I_k - R_U^T I_k R_V\|_2^2 . \tag{10}$$

In case we further denote

$$G^* = \|I_k - R_U^T I_k R_V\|_2^2, \tag{11}$$

becomes clear that it is always possible to adjust ΔS in (10) to provide $G \le G^*$. It is possible to modify on the first stage $\{R_U, R_V\}$ with the aim to minimize G^* and adjust ΔS on the second stage to minimize G. Such approach has its advantages and disadvantages. The advantage is that the approach is simpler because it does not require variables of ΔS to be taken into account and optimized on its first stage; optimization of ΔS on the second stage does not influence robustness; global minimum is easy to reach on the second stage. The disadvantage is that the solution is suboptimal in principle.

Taking into account that $\boldsymbol{u}' = (R_U \boldsymbol{u}^T)^T$ and $\boldsymbol{v}' = (R_V \boldsymbol{v}^T)^T$, first stage optimization task including embedding constraint can be defined as:

$$\begin{cases} G^* = \|I_k - R_U^T I_k R_V\|_2^2 \to min; \\ (-1)^{bit}(\boldsymbol{u} R_U^T Ref R_V \boldsymbol{v}^T - m) = Th. \end{cases} \quad (12)$$

Therefore rotational matrices R_U and R_V should be calculated according to optimization procedure.

C. Model for Rotations

Rotational matrix R in four dimensional space can be fully described according to Van Elfrinkhof's formulae [16]:

$$R = \begin{pmatrix} ap - bq - cr - ds & -aq - bp + cs - dr & -ar - bs - cp + dq & -as + br - cq - dp \\ bp + aq - dr + cs & -bq + ap + ds + cr & -br + as - dp - cq & -bs - ar - dq + cp \\ cp + dp + ar - bs & -cq + dp - as - br & -cr + ds + ap + bq & -cs - dr + aq - bp \\ dp - cq + br + as & -dq - cp - bs + ar & -dr - cs + bp - aq & -ds + cr + bq + ap \end{pmatrix} \quad (13)$$

where a, b, c, d, p, q, r, s are reals and $a^2 + b^2 + c^2 + d^2 = 1, p^2 + q^2 + r^2 + s^2 = 1$.

Rotational matrix R can be decomposed on matrices $\{R^L, R^R\}$ that describe left-isoclinic and right-isoclinic rotations:

$$R = R^L R^R \quad (14)$$

$$R^L = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}, \quad (15)$$

$$R^R = \begin{pmatrix} p & -q & -r & -s \\ q & p & s & -r \\ r & -s & p & q \\ s & r & -q & p \end{pmatrix}. \quad (16)$$

In general rotational matrices $\{R_U, R_V\}$ that figurate in the optimization task (12) are represented as compositions of left- and right-isoclinic rotations:

$$R_U = R_U^L R_U^R, \quad (17)$$

$$R_V = R_V^L R_V^R. \quad (18)$$

However, in some cases simpler model of rotational matrix is applicable.

In case Ref is an orthonormal matrix there are two consequences: a) Ref can be seen as some rotational matrix and can be decomposed on left- and right-isoclinic rotational matrices Ref^L and Ref^R:

$$Ref = Ref^L Ref^R; \quad (19)$$

b) term $R_U^T Ref R_V$ in (12) is also an orthonormal matrix and according to a) $R_U^T Ref R_V = R_U^T Ref^L Ref^R R_V$. In order to express any orthonormal matrix by term $R_U^T Ref^L Ref^R R_V$ it is enough that matrices R_U and R_V are left- and right-isoclinic respectively. Therefore utilization of orthonormal Ref for watermarking could significantly simplify goal function G^* and make embedding easier.

D. Criterion of Watermarking Performance

In order to provide high watermarking performance it is necessary to minimize embedding distortions and to adjust robustness. It would be much easier to judge a tradeoff between robustness and transparency for each block separately. Threshold value Th influences embedding distortions as well as robustness of a bit of a watermark for each particular block. Therefore several different values of Th for each block could provide sufficient variety of transparency-robustness pairs. A decision about the best Th for each block should be made according to some criterion.

Embedding distortions can be easily estimated according to, for example, RSS, but in order to estimate robustness we have to make some assumptions regarding distortion patterns. Those distortions are usually represented by signal processing or noise.

One possible way to check if an embedded bit is robust is to add each possible distortion pattern to a block and perform SVD to extract a bit. However, it would be computationally unreasonable. Therefore another kind of estimation of robustness is required.

According to the proposed watermarking rule a bit of a watermark can not be influenced by a distortion pattern that does not change the first column of orthonormal matrix. Therefore let us consider a special case of distortion that occurs when S' is being changed to S'', each column of U' and V' except the first is being rotated:

$$U'' = (R'_{\boldsymbol{u}'} U'^T)^T, \quad (20)$$

$$V'' = (R'_{\boldsymbol{v}'} V'^T)^T. \quad (21)$$

Such rotations are represented by rotational matrices $R_{\boldsymbol{u}'}$ and $R_{\boldsymbol{v}'}$ respectively where each matrix can be described by Euler-Rodrigues formulae [16]:

$$R' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a^2 + b^2 - c^2 - d^2 & 2(bc - ad) & 2(bd + ac) \\ 0 & 2(bc + ad) & a^2 - b^2 + c^2 - d^2 & 2(cd - ab) \\ 0 & 2(bd - ac) & 2(cd + ab) & a^2 - b^2 - c^2 + d^2 \end{pmatrix} \quad (22)$$

A special distortion pattern Dis_k^* of watermarked image fragment I'_k can be expressed in that case:

$$Dis_k^* = I'_k - I''_k = U'\left(S' - R'^T_{\boldsymbol{u}'} S'' R'_{\boldsymbol{v}'}\right)V'^T. \quad (23)$$

If we further define term $\left(S' - R'^T_{\boldsymbol{u}'} S'' R'_{\boldsymbol{v}'}\right)$ as SR^* it can be seen that:

$$SR^* = \begin{pmatrix} SR_{1,1} & 0 & 0 & 0 \\ 0 & SR_{2,2} & SR_{2,3} & SR_{2,4} \\ 0 & SR_{3,2} & SR_{3,3} & SR_{3,4} \\ 0 & SR_{4,2} & SR_{4,3} & SR_{4,4} \end{pmatrix}. \quad (24)$$

For general case distortion pattern for k-th fragment is denoted as Dis_k and general SR is defined:

$$SR = U'^T Dis_k V'. \quad (25)$$

The measure $\|\boldsymbol{dv}\|_2^2$ where

$$\boldsymbol{dv} = (SR_{1,2}, SR_{1,3}, SR_{1,4}, SR_{2,1}, SR_{3,1}, SR_{4,1}). \quad (26)$$

can be used as an indicator of changes in $\boldsymbol{u}'$ and $\boldsymbol{v}'$ for a single distortion pattern Dis_k, because no changes in $\boldsymbol{u}'$ and $\boldsymbol{v}'$ imply that $\|\boldsymbol{dv}\|_2^2 = 0$. If all the distortion patterns $\{Dis_k\}$ are taken into account then appropriate indicator of possible changes in $\boldsymbol{u}'$ and $\boldsymbol{v}'$ is $Var(\|\boldsymbol{dv}\|_2^2)$.

We further assume that random distortion pattern Dis can be approximated as $Dis = \sum_{i=1}^4 r_i \boldsymbol{dis}_i$, where $\{\boldsymbol{dis}_i\}$ is a set of four independent components, each represented as 4x4 matrix, and $\{r_i\}$ is a set of four independent normally distributed zero-mean random variables. This assumption is due to the nature of random distortion pattern for distortions caused by some popular image processing (for example JPEG). Usually such distortion patterns can be described by several high-frequency components.

The indicator of robustness for a particular pair $\{U', V'\}$ can now be defined as:

$$Var(\|\boldsymbol{dv}\|_2^2) = \sum_{i=1}^4 \|\boldsymbol{dv}_i\|_2^4 Var(r_i^2) + \\ +4\sum_{\substack{i=2 \\ j<i}}^4 \left[\left(\boldsymbol{dv}_i \boldsymbol{dv}_j^T\right)^2 Var(r_i) Var\left(r_j\right)\right], \quad (27)$$

where $\boldsymbol{dv}_i = (SR_{1,2}^i, SR_{1,3}^i, SR_{1,4}^i, SR_{2,1}^i, SR_{3,1}^i, SR_{4,1}^i)$ and $SR^i = U'^T \boldsymbol{dis}_i V'$. The main advantages of the proposed indicator of robustness are that it takes into account multivariate distribution of distortion patterns and can be easily computed for any pair $\{U', V'\}$.

It is necessary to estimate the watermarking performance in order to choose an appropriate threshold value Th for a particular block. To estimate the performance we united indicators of embedding distortions and robustness in a single criterion C that is determined as:

$$C = \alpha \frac{G}{\sum_{i,j=1}^4 I_k^2(i,j)} + \beta \sqrt{\frac{Var(\|\boldsymbol{dv}\|_2^2)}{(Th * S'_{1,1})^4}}, \quad (28)$$

where α and β are some positive constants defined empirically. Lower value of C corresponds to better watermarking performance. Depending on requirements to the tradeoff between invisibility and robustness different values of α and β can be used.

Therefore in order to provide lower value of C for a particular image fragment I'_k goal function G should be minimized several times, each time with different value of Th. The value of Th that provides the lowest C is the best for a particular block.

E. The Steps of Watermarking

The method of watermark embedding can be described as following:

1) Define a set of n different threshold values $\{Th_j\}$, $j = 1 \dots n$, that can be used in each block to embed a bit of a watermark;
2) Split the whole image I on fragments of size 4×4;
3) Select image fragments for watermark embedding according to some secret key;
4) For a particular selected image fragment I_k provide that watermarked fragment $I'_{k,j}$ satisfies embedding condition (12) and G_j is minimized for each Th_j, calculate C_j;
5) Replace each I_k by $I'_{k,j}$ that has the lowest C_j.

Watermark extraction can be specified by the steps:

1) Split the whole watermarked image I' on fragments of size 4×4;
2) Select image fragments for watermark extraction according to the key;
3) Apply SVD to each selected fragment I'_k and obtain $\{U', V'\}$;
4) Substitute $\{U', V'\}$ in equation (7) and calculate a bit.

IV. Experimental Results

The performance of the proposed watermarking method was compared with two different blind SVD-based methods proposed in [13] and [15]. Several tests were conducted in order to emphasize differences between the methods. First an influence of different orthonormal reference matrices Ref on the level of embedding distortions was explored without adaptation. Then some results of watermarking using the proposed method with adaptation were compared with the results of the other methods. Finally, results of watermarking with increased data payload were analyzed.

A. Different Reference Matrices

Reference matrix Ref is an important component for adjusting the proposed embedding rule. In order to select a matrix that provides better watermarking performance we have compared embedding distortions for different orthonormal reference matrices under condition with no adaptation e.g., equal threshold Th has been applied to all the blocks.

We presumed that all the considered orthonormal matrices-candidates provide equal robustness. Hence the level of embedding distortions is the only important characteristic that could be different for different matrices. Variance of the term $\boldsymbol{u}'Ref\boldsymbol{v}'^{T}$ influences embedding distortions. Lower embedding distortions correspond to a reference matrix that provides lower $Var(\boldsymbol{u}'Ref\boldsymbol{v}'^{T})$.

Five orthogonal normalized matrices were proposed as candidates for Ref.

The first matrix has just one non-zero element in each column (row):

$$Ref\_1 = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \quad (29)$$

The second matrix has two non-zero elements with equal absolute values in each column:

$$Ref\_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}. \quad (30)$$

The third matrix has three non-zero elements with equal absolute values in each column:

$$Ref\_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 1 & -1 & 0 \\ -1 & 0 & 1 & -1 \\ -1 & -1 & 0 & 1 \end{pmatrix}. \quad (31)$$

All the elements of the fourth matrix have equal absolute values:

$$Ref\_4 = 0.5 \begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \end{pmatrix}. \quad (32)$$

The fifth matrix has different number of non-zero elements in different columns (rows):

$$Ref\_5 = \frac{1}{3} \begin{pmatrix} 2 & -1 & 0 & -2 \\ 0 & 0 & -3 & 0 \\ -1 & 2 & 0 & -2 \\ 2 & 2 & 0 & 1 \end{pmatrix}. \quad (33)$$

All the five orthonormal matrices were used to collect five sets of indices. Each i-th set contains 262144 index values $\boldsymbol{u}'Ref\_i\boldsymbol{v}'^{T}$ calculated for each 4x4 block from 16 different grayscale images with resolution 512x512. The parameters of the distributions of index values for each set are given in Table I.

TABLE I. PARAMETERS OF INDEX DISTRIBUTION FOR DIFFERENT REFERENCE MATRICES

	Ref_1	Ref_2	Ref_3	Ref_4	Ref_5
Mean	-0.00030	0.00005	0.00086	-0.00047	0.00036
Variance	0.0818	0.0523	0.0913	0.1031	0.0981

From the table it can be seen that the second reference matrix Ref_2 provides that the variance of the set $\{\boldsymbol{u}'Ref\_2\boldsymbol{v}'^{T}\}$ is the smallest. Therefore the second reference matrix should be used in order to provide better watermarking performance.

B. Adjustment of the Proposed Criterion

A value of criterion C according to (28) depends on estimate of $Var(\|\boldsymbol{dv}\|_2^2)$ which in turn depends on a set of distortion patterns $\{Dis_k\}$. Each pattern in the set is approximated as $Dis_k = \sum_{i=1}^{4} r_{i,k}\boldsymbol{dis}_i$. However, for each pattern its complete (exact) representation should be obtained first: $Dis'_k = \sum_{i=1}^{16} r_{i,k}\boldsymbol{dis}_i$. Hence there are two important stages: collect distortion patterns $\{Dis'_k\}$; define the most important components $\{\boldsymbol{dis}_i\}$, $i = 1 \dots 4$.

In our tests all the 16 test images were split on blocks 4x4 which produced set $\{I_k\}$. Compression according to JPEG with quality factor 50 and 3x3 median filtering have been applied in turn to each of 16 test images. Therefore 32 distorted images were obtained. Each distorted image was again split on blocks 4x4 which produced set $\{I''_{k,g}\}$, where $g = 1$ corresponds to JPEG compression and $g = 2$ corresponds to median filtering. For each distorted block $I''_{k,g}$ distortion pattern $Dis'_{k,g}$ has been computed:

$$Dis'_{k,g} = I''_{k,g} - I_k. \quad (34)$$

Four the most important components $\{\boldsymbol{dis}_i\}$, $i = 1 \dots 4$ were defined using Principal Component Analysis (PCA) from the collection of $\{Dis'_{k,g}\}$, where $k = 1 \dots 524288$. For that purpose each distortion pattern $Dis'_{k,g}$ has been represented as a point in 16-dimensional space. First four eigenvectors (with the highest eigenvalues) returned by PCA have been obtained in a form of 1x16 vectors. Each vector has been rearranged to corresponding 4x4 (matrix) component and a set $\{\boldsymbol{dis}_i\}$ has been formed.

The set $\{Th_j\}$ for the adaptation was $\{0.002, 0.003, 0.004, 0.005, 0.006\}$, which means adaptation procedure required 5 iterations for each block.

C. Watermarking Results

The methods proposed in [13] and [15] provide quite different robustness-transparency tradeoffs and different data payloads. In order to make comparison fair the same watermark bit sequence consisted of 64 bits was used for all the methods. Each bit was embedded by each method redundantly (8 times) in randomly chosen blocks. Positions of chosen blocks were the same for the proposed method and the

method of Tehrani. Four grayscale images of size 512x512 were selected for comparison of the methods. The chosen images were Lena, Baboon, Cameraman and Livingroom. All the attacks mentioned in the experiment were simulated by StirMark Benchmark 4. For all the methods Bit Error Rates (BERs) of a watermark extracted from each image were calculated. For Gaussian Noise (GN) and Salt&Pepper attacks the rates were averaged over 100 runs. The results are represented in Table II.

TABLE II. RESULTS OF 64-BIT WATERMARK EXTRACTION

Image, Method, PSNR	**GN, PSNR=35 dB**	**Salt & Pepper, 3%**	**JPEG, Q=50**	**3x3 Median Filter**	**Cropping, 75%**	**Rotation, 0.25˚**
Lena, Tehrani, 52.76dB	5.58	6.35	4.68	9.38	10.35	9.38
Lena, Li, 42.58dB	**0**	**1.83**	**0**	**0**	13.20	**4.68**
Lena, proposed, 53.07dB	5.42	6.07	3.13	4.68	**9.81**	7.81
Baboon, Tehrani, 50.32dB	3.34	4.92	3.13	7.81	**9.39**	7.81
Baboon, Li, 41.95dB	**0**	**1.59**	**0**	**0**	14.46	**4.68**
Baboon, proposed, 51.50dB	3.81	5.47	1.56	4.68	11.60	9.38
Cameraman, Tehrani, 52.80 dB	6.28	6.23	3.13	9.38	11.67	10.94
Cameraman, Li, 41.75dB	**0**	**2.08**	**0**	**0**	12.53	**4.68**
Cameraman, proposed, 53.32dB	6.14	6.62	1.56	6.25	**11.03**	7.81
Livingroom, Tehrani, 50.59dB	3.51	5.82	3.13	10.94	12.72	9.38
Livingroom, Li, 42.26dB	**0**	**1.13**	**0**	**0**	15.09	**4.68**
Livingroom, proposed, 51.36dB	4.12	7.36	3.13	6.25	**11.83**	10.94

The payload in the particular test was just 64 bits which is very low. The proposed method and the method of Tehrani [15] use blocks of the same size 4x4 to embed a bit of a watermark. Therefore maximum payload of the both methods for 512x512 image is 16384 bit per image. However, for Li's method [13] the size of a macro-block is 32x32 and 2 bits are being embedded in each, which limits maximum payload by just 512 bit per image.

In order to compare the methods under a condition with the highest common payload the embedding redundancy for each method was adjusted in a different way. Then the methods were tested using the same 4 grayscale images. The method of Li has been used for embedding of 512 bit long sequence without redundancy. The method of Tehrani has been used for embedding of the same sequence with redundancy 6. The proposed method has been used for embedding with redundancy 8. The results are represented in Table III.

TABLE III. RESULTS OF 512-BIT WATERMARK EXTRACTION

Image, Method, PSNR	**GN, PSNR=35 dB**	**Salt & Pepper, 3%**	**JPEG, Q=50**	**3x3 Median Filter**	**Cropping, 75%**	**Rotation, 0.25˚**
Lena, Tehrani, 43.82dB	6.85	7.37	5.66	10.94	12.47	10.16
Lena, Li, 42.39dB	**1.98**	**5.15**	**2.73**	**1.37**	51.37	19.92
Lena, proposed, 44.07dB	5.56	6.07	3.32	4.88	**9.75**	**8.00**
Baboon, Tehrani, 43.19dB	4.35	5.96	4.69	11.91	12.25	9.38
Baboon, Li, 41.87dB	**2.13**	**4.84**	2.15	**1.56**	45.03	20.31
Baboon, proposed, 43.42dB	3.81	5.47	**1.76**	4.69	**11.60**	**9.18**
Cameraman, Tehrani, 43.91dB	7.21	6.85	4.30	10.35	12.03	11.33
Cameraman, Li, 41.85dB	**2.25**	6.78	2.54	**1.95**	48.52	21.09
Cameraman, proposed, 44.12dB	6.39	**6.52**	**1.56**	6.64	**10.92**	**8.20**
Livingroom, Tehrani, 42.95dB	4.31	6.92	5.47	11.72	13.82	**10.35**
Livingroom, Li, 42.39dB	**2.32**	**6.56**	**1.95**	**2.34**	50.26	21.88
Livingroom, proposed, 43.86dB	4.15	7.34	3.32	6.05	**11.71**	10.74

Even for increased data payload quality of images watermarked by the proposed method remains quite acceptable and is definitely the best among all the watermarked images in the test (Table III). It can be seen from Fig.1 that watermarked Lena image looks quite pure (PSNR=44.07dB).

Figure 1. Watermarked Lena image with PSNR=44.07dB.

V. DISCUSSION

The proposed method is blind and only blind methods [13] and [15] were selected to compare the performance. The reason why other well-known SVD-based non-blind or semi-

blind methods were rejected from the comparison is that they require additional information to be transferred.

From the watermarking results with low data payload (64 bit) it can be seen that there is no single method which performs better compared to others for all the kinds of common distortions. However, for non-geometrical attacks the method proposed by Li demonstrates extremely high robustness. For cropping attack the proposed and Tehrani's methods perform better because smaller blocks can be better spread in an image and smaller blocks are less likely to be cropped either. The quality of the images watermarked by the proposed and Tehrani's methods is much higher compared to Li's method. The proposed method provides slightly better quality of the watermarked images compared to Tehrani's method and its robustness toward JPEG and median filtering is better.

From the watermarking results with increased data payload (512 bit) it can be seen as previously that there is no absolute favorite. Each method embeds a watermark with different redundancy and the proposed method dominates in more positions while still providing the best quality. The method proposed by Li fully dominates in Gaussian noise and median filtering attacks even without redundant embedding. However, its performance in geometric attacks (cropping and rotation) is much worse. Another concern is that quality of images watermarked by Li's method is the worst. Because of the embedding with different redundancy the quality of images watermarked by the proposed and Tehrani's methods is comparable. Nevertheless the robustness of the proposed method is better than that of Tehrani's method except two kinds of distortion for Livingroom image. The advantage of the proposed method over Tehrani's method is especially high for JPEG and median filtering attacks and for some images BER is around 6% lower.

The proposed method and the method of Tehrani use the same SVD transform to embed a bit of a watermark in 4x4 block. Considerable advantage of the proposed method compared to the method of Tehrani in case of JPEG and median filtering attacks is mostly due to minimization of embedding distortions and proper adjustment of Th for each block.

Robustness of Li's method toward most kinds of attacks is very high even without redundant embedding. It is quite obvious that the ability to withstand noise and filtering attacks is better in case a bit of a watermark is embedded in larger block. The method proposed by Li uses 32x32 macro-block to embed 2 bit. In contrast to that the proposed method uses 4x4 blocks to embed a bit.

Popular image processing techniques usually process areas that are far larger than 4x4. A good example is JPEG-compression that process blocks 8x8. Therefore the result of JPEG-attack for a particular block 4x4 depends not only on that block, but also on some neighboring pixels, which makes a prediction of changes quite difficult based only on 4x4 block. Similar observation can be made regarding median filtering that uses adjacent pixels as well.

Nevertheless robustness-transparency tradeoff can be sufficient in case a bit is embedded in 4x4 block. In some instances compromise is required between robustness and data payload or between robustness and image quality. Quality of images watermarked by Li's method is usually around 42 dB which could be not enough for some demanding applications. Maximum payload provided by Li's method is 512 bit per 512x512 image which is only a half of required payload to embed 32x32 logo. Therefore redundant embedding is impossible for that method even for quite moderate payload which implies lower robustness toward some geometric attacks.

VI. CONCLUSIONS

New blind watermarking method based on SVD is proposed in this paper. The method embeds a bit of a watermark by modifying the first columns of the both orthonormal matrices of a transformed 4x4 image block. Multiple improvements implemented in respect to existing methods are: the both orthonormal matrices are used, model of rotations in 4D space is applied to modify orthonormal matrices, embedding distortions are minimized, the criterion of watermarking performance is proposed for adaptation.

Utilization of the both orthonormal matrices maintains better watermarking performance. Modification of the both matrices introduces lower embedding distortions compared to an approach that modifies just one. On the other hand such embedding is less affected by common image processing techniques.

Application of rotational model assures that the result of modification of orthonormal matrices is a matrix which is also orthonormal. The application guaranties that the result of the decomposition matches matrices used to compose a fragment. This is a considerable advantage over existing approaches. Rotational matrices are being adjusted in order to minimize goal function. Constraints necessary to embed a bit of a watermark are taken into account during the minimization procedure. Minimization of embedding distortions improves transparency of watermarked images without affecting robustness.

The proposed criterion of watermarking performance takes into account embedding distortions as well as robustness of a bit of a watermark for each particular block. Considered adaptation procedure on the basis of the proposed criterion chooses appropriate threshold value for each block. This reduces embedding distortions while keeps substantial robustness. Lower level of distortions enables embedding with higher redundancy which considerably increases total robustness of a watermark.

As the result of the proposed improvements BER for a watermark extracted after median filtering has been reduced up to 6% compared to the method proposed in [15]. On the other hand quality of watermarked images is higher. For some geometric attacks BER has been reduced more than 40% compared to the method proposed in [13].

ACKNOWLEDGMENT

The first author is thankful to Tampere Program in Information Science and Engineering for the support.

REFERENCES

[1] I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker, Digital Watermarking and Steganography (2 ed.), San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2007.

[2] C. Song, S. Sudirman, M. Merabti and D. Llewellyn-Jones, "Analysis of Digital Image Watermark Attacks," in *Proceedings of Consumer Communications and Networking Conference (CCNC)*, 9-12 Jan. 2010.

[3] H. R. Sheikh and A. Bovik, "Image information and visual quality," *IEEE Transactions on Image Processing*, vol. 15, no. 2, pp. 430-444, Feb. 2006.

[4] S. Lin and C.-F. Chen, "A robust DCT-based watermarking for copyright protection," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 3, pp. 415-421, Aug 2000.

[5] E. Fullea and J. Martinez, "Robust digital image watermarking using DWT, DFT and quality based average," in *Proceedings of the ninth ACM international conference on Multimedia (MULTIMEDIA '01)*, 2001.

[6] L. Trefethen and D. Bau, Numerical Linear Algebra, Cambridge University Press, 1997.

[7] V. Gorodetski, L. Popyack, V. Samoilov and V. Skormin, "SVD-based Approach to Transparent Embedding Data into Digital Images," in *Proceedings of the International Workshop on Information Assurance in Computer Networks: Methods, Models, and Architectures for Network Security (MMM-ACNS '01)*, 2001.

[8] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Transactions on Multimedia*, vol. 4, no. 1, pp. 121-128, Mar 2002.

[9] X.-P. Zhang and K. Li, "Comments on "An SVD-based watermarking scheme for protecting rightful Ownership"," *IEEE Transactions on Multimedia*, vol. 7, no. 3, pp. 593-594, June 2005.

[10] E. Ganic and A. Eskicioglu, "Robust DWT-SVD domain image watermarking: embedding data in all frequencies," in *Proceedings of the 2004 workshop on Multimedia and security (MM&Sec '04)*, 2004.

[11] P. Bao and X. Ma, "Image adaptive watermarking using wavelet domain singular value decomposition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 15, no. 1, pp. 96-102, Jan. 2005.

[12] H.-C. Wu, R.-J. Jang and Y.-C. Liu, "A robust watermarking scheme based on singular value decomposition and quantization technique," in *Proceedings of International Computer Symposium (ICS)*, Dec. 2010.

[13] Z. Li, K.-H. Yap and B.-Y. Lei, "A new blind robust image watermarking scheme in SVD-DCT composite domain," in *Proceedings of 18th IEEE International Conference on Image Processing (ICIP)*, Sept. 2011.

[14] C.-C. Chang, P. Tsai and C.-C. Lin, "SVD-based digital image watermarking scheme," *Pattern Recognition Letters*, no. 26, p. 1577–1586, 2005.

[15] I. O. Tehrani and S. Ibrahim, "An enhanced SVD based watermarking using U matrix," in *Proceedings of 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*, 2010.

[16] H. P. Manning, Non-Euclidean Geometry, HardPress, 2012.