SVD-Based Watermark with Quasi-One-Way Operation by Reducing a Singular Value Matrix Rank

Kazuo Ohzeki

Shibaura Institute of Technology
ISE, 3-7-5, Toyosu,
Koutou-ku, Tokyo 135-8548
+81-3-5859-8513

ohzeki@sic.shibaura-it.ac.jp

Masaru Sakurai

Nagoya Institute of Technology
CSE, Gokiso-cho, Showa-ku,
Nagoya 466-8555
Telephone number, incl. country code

sakurai.masaru@nitech.ac.jp

ABSTRACT

A new Singular Value Decomposition (SVD)-based watermarking method was developed in this study. Quasi-one-way operation is improved by reducing the rank of the singular value matrix. All diagonal elements of the singular value matrix are positive; all other off-diagonal elements are zeros. To add an element to the off-diagonal area is fundamentally a quasi-one-way operation because no value cannot be subtracted from zero. In adding elements to the off-diagonal area, a pair of linearly dependent vectors is produced. This modification reduces the rank of the singular value matrix. It is computationally difficult to find diminished singular values from the reduced rank matrix.

Categories and Subject Descriptors

H.1.1 [MODELS AND PRINCIPLES]: Systems and Information Theory -*Information theory*

General Terms

Security

Keywords

watermark, SVD, quasi-one-way function, inversion

1. INTRODUCTION

Watermarking is one of the prospective methods to enable forensic tracking in contents distribution [1]. Singular Value Decomposition (SVD) diagonalizes matrix elements by multiplying orthogonal matrices to obtain zero values for off-diagonal elements. To add watermarking elements to off-diagonal positions is a quasi-one-way functional operation. The quasi-one-way operation means, in this paper, that it is easy to get a forward operation result, but is difficult to find an inverse value from the result. It is discussed that the strict one-way function is not known [2]. The quasi-one way operation is one of methods to realize a very effective countermeasure against the so-called inversion attack. Many research papers have described inversion attacks, but the best method of dealing with them remains an open problem. Some embed a watermark into a random sequence instead of into normal images. One method theoretically embeds a watermark cryptographically and using a Zero-Knowledge detection method, which differs from an image watermark and is much too vulnerable to small attacks.

Gorodetski et al [3] introduced a watermarking method using SVD in 2001. Ganic [4] surveyed SVD-based watermarking methods in 2003. Many other papers have presented the use of SVD, but the problems of embedding methods remain. Features of SVD that have been discussed include robustness, combination with DCT, and wavelet transformation. A countermeasure to the inversion attack has not been achieved. We were unable to find an SVD watermarking method that features a quasi-one-way function to protect against inversion attacks.

In the study described in this paper, SVD is renovated from a mathematical perspective. Discussions of this matter are revised, and an improved SVD-based watermarking is developed with a quasi-one-way function to cope with inversion attacks. Data values of all steps are shown for verification of the proposed method for intuitive examination of the situation.

e-Forensics 2008, January 21-23, 2008, Adelaide, Australia.

2. RELATED STUDIES AND PROBLEMS

Liu and Tan presented a new SVD-based watermarking method [5]. Zhang and Li [6] explained that the extracted watermark is not the embedded watermark, but is determined by the reference watermark; the reference watermark generated the pair of SVD matrices used in the watermark detector. They concluded that, in the former method, the detection stage uses watermark-dependent information. That information is so improperly used that it does not guarantee an objective detection outcome and induces a false positive detection rate [6]. The SVD operation of the former method did not present a match between the decomposing and synthesis and could not prevent a successful inversion attack. The method is analyzed in the following paragraph; after embedding a watermark, SVD was calculated again to obtain an embedded diagonal singular value matrix. The second SVD did destroy an equivalent relation between the embedded watermark and the detected one.

The SVD method described in [5] is reconsidered here. For this analysis, "I" is an input image with a real number. Its matrix size is assumed to be square, N×N, for simplicity without loss of generality. The SVD of I is the following,

$$I=U*S*V^T$$

In that equation, U and V respectively denote orthogonal matrices diagonalizing I into S, where S is the diagonal matrix, T signifies the transpose of the matrix, and H is the Hermitian or conjugated transposition. For the real valued image I, autocorrelation of I is real and symmetric, therefore U, V and S are all real values. The SVD can be treated within real values and T is sufficient without H.

Then for watermark matrix W with weighted scalar value a, the watermark is added to S as
S+aW.

That S+aW is decomposed again in [5] as,

$S+aW = U_W S_W V_W^T$

In that equation, U_W, V_W^T is used for detection of the watermark later. Next, ignoring the embedded watermark W, the inverse of singular value decomposition is carried out as

$I_W = U * S_W * V^T$,

which is an embedded image. In the detection stage, for the embedded image I_W without any modification, SVD is again applied to obtain

$I_W = U^* * S_W^* * V^{*T}$.

For detected S_W^*, U_W, V_W^T are used to obtain

$D = U_W * S_W^* * V_W^T$

Then, subtracting S and using a,

$W^* = (D - S)/a$

where W^* differs from the original watermark W. In this inverse transformation, U, V and S_W are used instead of S+aW without consideration of the deformation caused by U_W, V_W^T. Because of this transformation, the embedded watermark was not be detectable correctly from a mathematical point of view, which causes a side effect that the embedded watermark is mixed into other data to produce a false watermark.

Here, basic characteristics of SVD will be reviewed for watermarking convenience. For N×N image data G, which serves the same role as image I, G can be diagonalized by matrices U and V as,

$U^T G V = S$

where S is a diagonal matrix. To get U and V for matrix G, the transpose of G is multiplied by G, as

$GG^T = G^T G$.

Putting eigenvectors of $GG^T = G^T G$ in a matrix in descending order of eigenvalues produces orthogonal transformation, U and V. Here, U is on the left for column transformation and V is on the right for row transformation. The product $GG^T = G^T G$ is symmetric and comprises real number elements. Therefore the U, V and S are all real values and the rank of U and V and S is depend on the rank of $GG^T = G^T G$.

The singular values in matrix S are positive; the root of the eigenvalues of $GG^T = G^T G$.

Figure 1 presents a flowchart of the method used in a previous study [5]. Wu presented a modification of [5] with a diagonal watermark to increase the rank of the watermark matrix, but the basic method is identical to that presented in [5]; an unmatched relation exists between an embedded watermark and a detected one [7].

3. Improved SVD-Based Method

3.1 Method 1

In consideration of the preceding section, after embedding a watermark into the singular value matrix S, there is no need to apply SVD again. In addition, a quasi-one-way characteristic of SVD lies in the fact that the off-diagonal positions values are zeros. Because there are no positive or negative values in the off-diagonal positions, to put a value on an off-diagonal position is a quasi-one-way operation. For that reason, adding watermark values at

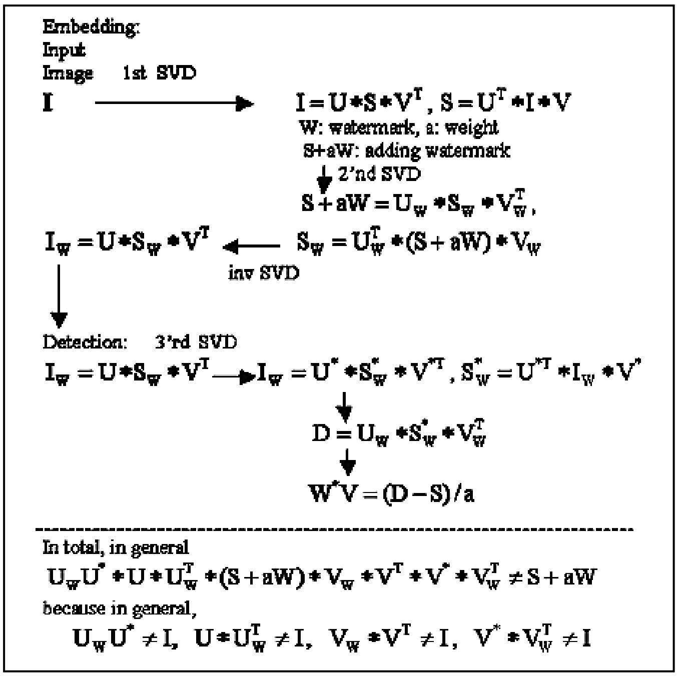

Figure 1. Conventional SVD Watermarking Method [5].

off-diagonal positions is an important quasi-one-way operation. As far as the quasi-one-way operation is effective, it is difficult to find another watermark with an appropriate pair of U and V of SVD for the embedded image, I_W.

To improve the SVD-based watermarking method, it is merely necessary to remove the operation of the second SVD. The embedded watermark is SS=S+aW. Then, the inverse SVD is performed to obtain an embedded image,

$I_W = U * SS * V^T$

If another SVD is applied to this I_W, then

$I_W = U_W * S_W * V_W^T$.

In general, $SS \neq S_W$, $U \neq U_W$, and $V \neq V_W$.

It is noteworthy that SS has off-diagonal elements other than zero, whereas S_W has only diagonal elements; from S_W, an embedded watermark cannot be detected.

On the other hand, the first and real embedder can detect SS and W using U, V and S. This is "Method 1" of improved SVD-based watermarking with a quasi-one-way function.

However, this Method 1 presents a problem. Although neither SS nor W can be derived directly from I_W, another effective U', V' and W', which might differ from the correct U, V and W, can be computed using basic linear algebra. Consequently, an inversion attack can be made on this Method 1. For example, after another SVD,

$I_W = U_W * S_W * V_W^T$

using a proper regular matrix T, $S_W = U_W^T * I_W * V_W$ can be modified, by multiplying T from the left and T^{-1} from the right, to

$T * U_W^T * I_W * V_W * T^{-1}$

Putting $T_U = T$, $T_V = T^{-1}$, we obtain

$$T_U * S_W * T_V = T_U * U_W^T * I_W * V_W * T_V . \qquad (3.1.1)$$

Using a pair of example matrices for T, as

$$T_U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ \varepsilon & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad T_U^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -\varepsilon & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = T_V$$

Then, (3.1.1) is modified to yield the following.

$$T_U * S_W * T_V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ \varepsilon & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} * \begin{bmatrix} s_1 & 0 & 0 & 0 \\ 0 & s_2 & 0 & 0 \\ 0 & 0 & s_3 & 0 \\ 0 & 0 & 0 & s_4 \end{bmatrix} * T_V$$

$$= \begin{bmatrix} s_1 & 0 & 0 & 0 \\ \varepsilon s_1 & s_2 & 0 & 0 \\ 0 & 0 & s_3 & 0 \\ 0 & 0 & 0 & s_4 \end{bmatrix} * \begin{bmatrix} 1 & 0 & 0 & 0 \\ -\varepsilon & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} s_1 & 0 & 0 & 0 \\ \varepsilon s_1 - \varepsilon s_2 & s_2 & 0 & 0 \\ 0 & 0 & s_3 & 0 \\ 0 & 0 & 0 & s_4 \end{bmatrix}$$

$$= \begin{bmatrix} s_1 & 0 & 0 & 0 \\ 0 & s_2 & 0 & 0 \\ 0 & 0 & s_3 & 0 \\ 0 & 0 & 0 & s_4 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 \\ \varepsilon s_1 - \varepsilon s_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$= S_W^* \qquad (3.1.2)$$

Subsequently, (3.1.2) is decomposed into a sum of two matrices as,

$S_W^* = S_W^D + W'$,

where S_W^D is a diagonal component and W' is an off-diagonal component.

On the other hand, (3.1.1) can be decomposed into a product of two matrices as follows;

Using $T_U * S_W * T_V = T_U * U_W^T * I_W * V_W * T_V$, we get

$(T_U * U_W^T)^{-1} * T_U * S_W * T_V * (V_W * T_V)^{-1} = I_W$.

Now we can find another SVD for the embedded image I_W with re-defined decomposition matrices as

$U^* = (T_U * U_W)^{-1} * T_U$, $V^{*T} = T_V * (V_W * T_V)^{-1}$.

In addition, the following can be inferred from the above. In fact, T_U is a versatile matrix for any watermarked image embedded by Method 1.

$$\begin{aligned} U^* V^{*T} &= (T_U * U_W{}^T)^{-1} * T_U * T_V (V_W * T_V)^{-1} \\ &= U_W{}^{T^{-1}} * T_U{}^{-1} * T_U * T_V * T_V{}^{-1} * V_W{}^{-1} \\ &= U_W{}^{T^{-1}} * (T_U{}^{-1} * T_U) * (T_V * T_V{}^{-1}) * V_W{}^{-1} \\ &= U_W{}^{T^{-1}} * I * I * V_W{}^{-1} \\ &= U_W{}^{T^{-1}} * V_W{}^{-1} \\ &= I \end{aligned}$$

3.2 Method 2

A further improved method is proposed to overcome the problem presented in the above section. This Method 2 is devised because Method 1 includes the defect that using an appropriate orthogonal matrix T, the diagonal matrix S can be transformed easily into another matrix with off-diagonal components, which removes the quasi-one-way function. The diagonal matrix S and watermark matrix W are first reviewed to formulate Method 2.

For image matrix I, SVD provides two orthogonal matrices, U and V, where U stands for column transformation and V is the row transformation. The watermark matrix W, which contains non-zero off-diagonal components, can be generated by multiplying an orthogonal matrix T by the diagonal singular matrix S. In fact, SS has two expressions,

SS=S+W

and

$SS = T_U * S$.

Then, from S+W= $T_U * S$,

$W = (T_U - I) * S$ or $T_U = (S + W) * S^{-1}$

are obtained. Observing the latter formula, in the case of matrices S and T_U in Method 1, W is not regular, and its diagonal components diminish. In the experiments described in [5], the number of random numbers for watermarking was shown to be limited. The rank of the watermark matrix W increases if the number of embedded watermarks increases. For this study, without the relation to the rank of W, embedding and detection of the watermark are carried out correctly. Increasing the rank of W tends to reduce the rank of T_U.

Based on these considerations, Method 2 proposes a non-regular matrix T_U. To reduce the rank of T_U, for example, a partial copy of S into W generates the linearly dependent matrix SS and consequently

$T_U = (S + W) * S^{-1}$

is also non-regular. In SVD, the rank of $U^* = T_U * U_W$ decreases and is not regular. By this operation, the embedded image I_W is decomposed as,

$I_W = U_W^{**} * S_W^{**} * V_W^{**}$.

The rank of S_W^{**}, U_W^{**} and V_W^{**} decreases and is computationally difficult to obtain regular matrices which

match the original I_W from these reduced rank matrices. The simplest example of W is,
W(i,i+1)=S(i,i), W(i+1,i)=S(i+1,i+1).
A flowchart of Method 2 is portrayed in Fig.2.

4. EXPERIMENTAL RESULTS

In this section, the proposed SVD-based watermarking algorithm is described using numerical data to confirm the operational methods in detail.

4.1 BASIC ANALYSIS

For a 4×4 image I, SVD is shown as the following.

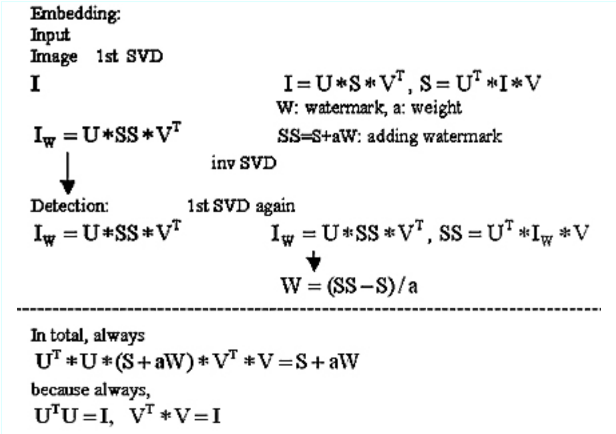

Figure 2. Proposed SVD-Based Watermarking.

I =

236	227	204	183
203	177	164	158
169	162	174	190
177	199	213	222

S=

767.6	0	0	0
0	63.2	0	0
0	0	17.9	0
0	0	0	0.25

U=

-0.554	-0.533	0.482	-0.420
-0.458	-0.434	-0.470	0.617
-0.452	0.354	-0.607	-0.549
-0.527	0.634	0.422	0.376

V=

-0.513	-0.664	-0.533	0.111
-0.502	-0.228	0.661	-0.509
-0.494	0.263	0.308	0.769
-0.491	0.662	-0.429	-0.370

Next, as a watermark matrix W, to make the second column of the singular value matrix conform to the third column,
W(2,3)=S(2,2), W(3,2)=S(3,3)
are processed. Then SS=S+W is obtainable.

W=

0	0	0	0
0	0	63.2	0
0	17.9	0	0
0	0	0	0

SS=

767.6	0	0	0
0	63.2	63.2	0
0	17.9	17.9	0
0	0	0	0.25

Next, the embedded image $I_W = U*SS*V^T$ is obtained by inverse SVD using SS, U, V.

I_W =

248.2	202.8	195.9	203.2
223.2	160.8	153.3	164.2
164.3	179.3	178.0	173.2
150.6	223.8	227.3	209.8

An attacker will attempt to find the singular value matrix SS to obtain the embedded watermark matrix W. To do so, I_W is decomposed as,

$$I_W = U_W^{**} * S_W^{**} * V_W^{**}$$

U_W^{**} =

-0.554	-0.381	-0.420	-0901
-0.458	-0.546	0.617	0.333
-0.452	0.175	-0.549	0.681
-0.527	0.725	0.376	-0.233

V_W^{**} =

-0.513	-0.846	0.111	0.091
-0.502	0.307	-0.509	0.629
-0.494	0.404	0.769	0.031
-0.491	0.164	-0.370	-0.771

S_W^{**} =

767.6	0	0	0
0	92.9	0	0
0	0	0.25	0
0	0	0	0.00

The rank of S_W^{**} is virtually 3, although it seems to be 4, but the fourth value is extremely small; it is almost zero.

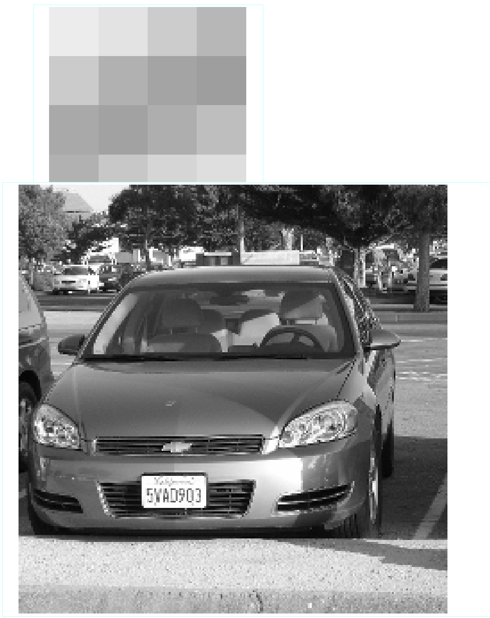

Figure.3 (a) 4×4 image (top) (b) 240×240 image (bottom)

Figure 3 shows parts of images used in these experiments. Figure3 (a) is a 4×4 monochrome image taken from the real world. Figure 3 (b) is a 240×240 monochrome image and its rank is actually 240. Most parts of singular values are sufficiently large, which indicates that Method 2 can be valid for use in general natural pictures.

Many other images were tested with application of SVD. Table 1 shows the maximum and minimum of the singular values of matrix S. The maximum values are from S(1,1) and the minimum values are from the last non-zero diagonal component. These images in Table 1 are all natural ones; the rank of S is the same values as the size of images, except for the circles image. It is not a natural image; it is artificial. Nevertheless, such images usually contain the same value in lines as background parts, and the rank might decrease. For all other images listed in Table 1, SVD operations are all well performed because the ranks of the singular matrix S are all the same value as the image size, which implies that the proposed method is stable in decomposition for many natural scene images.

Table 1 Ranks of Images and the Maximum and Minimum Values of Singular Values.

image name	size	rank of S	singular value	
			maximum	minimum
partial image	4		767.58	0.246
car	240	240	29761.3	0.382
girl	256	256	16511.0	0.252
couple		256	10002.5	0.0524
aerial		256	37267.6	0.353
mandrill		256	34517.9	0.0977
lena		256	31956.1	0.0148
peppers		256	27203.4	0.0692
circles(CG)		125	28508.9	40.3
mandrill	512	512	66463	0.0130
lena		512	38638	0.00270
peppers		512	60831	0.0475

4.2 EMBEDDING WATERMARKS

Based on the above considerations, watermark embedding experiments were carried out using Method 2. Figure 4 shows that the embedding was realized by multiplying a matrix $T_{k,k+1}$. The embedded images were modified using JPEG compression. Signal-to-noise ratios for both the embedded stage and that after the JPEG compression stage are shown in Fig. 5. Degradations are large for a compression ratio of 20. Detection ratios are shown in Fig. 6. Table 2 shows embedded positions and singular values for them. The detection rule for these experiments is that relevant singular values are all maintained at specified levels. The specified levels are half of the original values. The detection ratios shown in Fig.6 are normalized by the original values. The dotted line at 50% represents the borderline between detectable and non-detectable. Without JPEG compression, 100% detection is performed because there are only small fractional errors exist. Compression ratios of 11-13 are the maximum for detection. In the figure, SVD_min means the minimum value of two modified SVD values by JPEG at S(k,k) and S(k+1,k+1). These values are maintained larger than the borderline for JPEG compression ratio 30. In addition, WM_min means the minimum value of the embedded two watermarks modified by JPEG at S(k,k+1) and S(k+1,k). These values are critical and go below the borderline for JPEG compression ratio 11 or 13. Ripple_Max means the maximum value among all other elements in the neighboring area except the four elements; S(k,k), S(k,k+1), S(k+1,k) and S(k+1,k+1). Values for the Ripple_Max area are originally zeroes and modified by JPEG compression. The Ripple_Max is generally small. For JPEG compression ratio 30 the Ripple_Max is less than 15%.

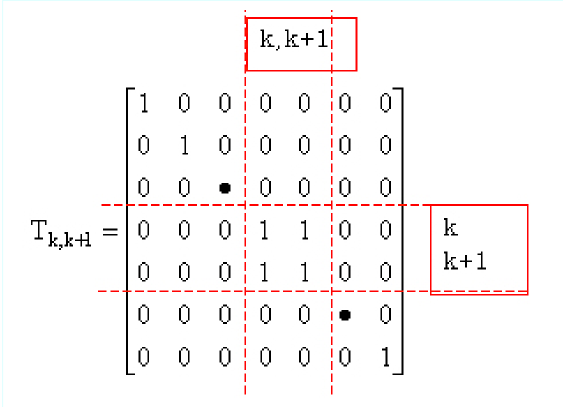

Figure 4. Embedding Matrix $T_{k,k+1}$.

Table 2. Embedded positions and Singular Values.

Image	Embedded Position(1) S(k,k)	SVD Value	Embedded Position(2) S(k+1,k+1)	SVD Value
girl	50	205.06	50	195.68
couple	51	197.62	51	189.70

5. CONCLUSIONS

Reorganizing the SVD-based watermarking system, a new improved SVD-based watermarking method with quasi-one-way function by reduced rank matrix is developed. The developed matrix with reduced-rank for watermark embedding in singular value decomposition cannot be restored using simple methods, such as simply multiplying a matrix. Embedded data are verified by a flowchart. The matrices were inspected using numerical values for all stages of transformation. Using the quasi-one-way function of the proposed method, inversion attacks cannot be activated. They would require computationally complex procedures to derive another set of singular value decomposition matrices. Regarding authentication, combination with a method proposed in a previous study, [8] might produce a promising system. Another modification to build the detection operation into a zero-knowledge proof procedure can be realized.

Experiments described in this paper have been pessimistic in relation to the detection rule. There is much room to improve the performance by setting a more optimistic detection rule.

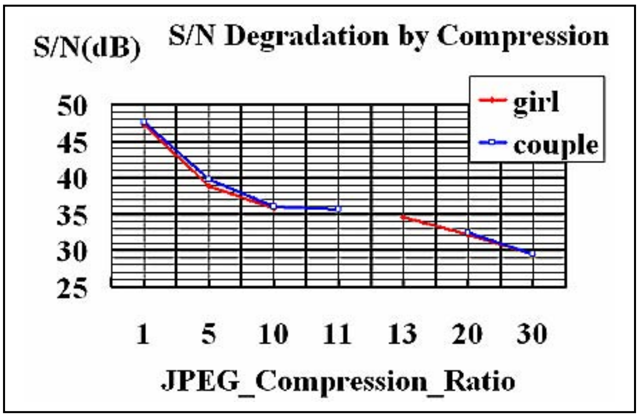

Figure 5. S/N Degradation by JPEG Compression.

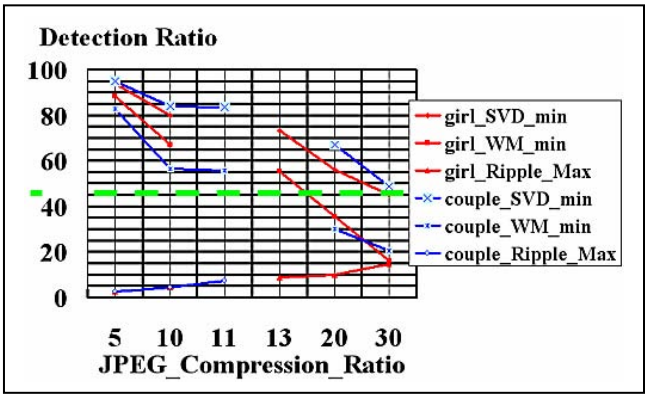

Figure 6. Detection Ratios Depending on Compression.

6. ACKNOWLEDGMENTS

The author thanks the Telecommunications Advancement Foundation (TAF) for supporting this research

7. REFERENCES

[1]Martin Schmucker ed., “First Summary Report on Forensic Tracking”, IST-2002-507932 ECRYPT, (European Network of Excellence in Cryptology) Jan. 2005.
http://www.ecrypt.eu.org/documents/D.WVL.7-1.1.pdf

[2]Goldreich, Oded, “Foundations of Cryptography: A Primer”, Now Publishers Inc 2005.

[3]Gorodetski, V. I, Popyack, L. J., Samoilov, V. and Skormin, V. A, “SVD-based Approach to Transparent Embedding Data into Digital Images,” Proceedings of the International Workshop on Information Assurance in Computer Networks: Methods, Models, and Architectures for Network Security (MMM-ACNS 2001),Pages: 263 - 274, May 21-23, 2001.

[4]Ganic, E., Zubair,N. and Eskicioglu, A.M. “An Optimal Watermarking Scheme Based on Singular Value Decomposition”. Proceedings of the IASTED International Conference on Communication, Network, and Information Security(CNIS). 85-90. 2003.

[5]Liu, Ruizhen, and Tan, Tieniu “An SVD-Based Watermarking Scheme for Protecting Rightful ownership”, IEEE Transactions on Multimedia, Vol. 4 No.1 pp.121-128, Mar. 2002.

[6]Zhang, Xiao-Ping, and Li, Kan ‘Comments on “SVD-Based Watermarking Scheme for Protecting Rightful ownership” ‘, IEEE Transactions on Multimedia, Correspondence, Vol. 7 No.2 pp.593-594, April 2005.

[7]Wu, Yongdong, " On the Security of an SVD-based Ownership Watermarking", IEEE Trans. on Multimedia, vol.7, no.4, pp. 624-627, Aug. 2005.

[8]Ohzeki, Kazuo, Cong, Li, and Igarashi, Kouhei, “Considering Knowledge of Watermarking Algorithm and Finding the Optimal Watermark Algorithm”, Wavilla Challenge WaCha06, . Sept. 2006.