International Journal of Computer Science and Applications
© Technomathematics Research Foundation
Vol. 7 No. 3, pp. 9 - 17, 2010

Discontinuity in SVD Embedding Mapping Used for Watermarks

Kazuo Ohzeki

Department of Information Science &Engineering, Shibaura Institute of Technology,
3-7-5, Toyosu Koutou-ku, 135-8548, Japan
ohzeki@sic.shibaura-it.ac.jp
http://www.alg.ise.shibaura-it.ac.jp

Yuki Seo

Fundamental Subjects in Mathematics and the Sciences, Common Core Subject Group,
College of Engineering,
307, Fukasaku Minumaku Saitama, 337-8570, Japan
seo@ sic.shibaura-it.ac.jp

Engyoku Gi

The Division of Electrical Engineering and Computer Science, School of Engineering.,
3-7-5, Toyosu Koutou-ku, 135-8548, Japan
m108048@ sic.shibaura-it.ac.jp

Abstract It is possible for Singular Value Decomposition (SVD) watermark embedding to have a quasi-one-way functionality. While basic SVD embedding has the drawback of being non-reversible, an advanced SVD method which uses a reversible relation only works one-way. When embedding takes place, the decomposing matrix obtained from the original image differs from the one obtained from the embedded image. This paper demonstrates that there is a distinct difference which shows discontinuity in the Euclidean Norm when evaluated numerically. This evidence points towards the probability that SVD embedding is resilient to inversion attacks.

Key words: inversion attack, SVD, one-way function, rank, mapping, norm, eigenvalue

1. Introduction

Digital watermarking systems are essential for protecting security, such as passport images. Freir (2006) has illustrated the gap between theoretical and practical security. Application-specific watermarking has the advantage of having fewer requirements, and a more robust system would broaden the application of this watermark.

Inversion attacks are a simple and fundamental problem for watermarking (Katzenbeisser, 2005). Let G be the original image and W a watermark. The owner

embeds the watermark W into the image G and obtains an embedded image Gw, as follows:

Gw=G+W

A typical inversion attack on this embedded image Gw is a declaration by an attacker that, "I embedded my own watermark W' in the image in question, Gw, x time ago." The declaration is always real because the attacker can decompose the image Gw as follows:

Gw=Gw-W'+W'=(Gw-W')+W',

where Gw-W' is the attacker's original image, and W' is the attacker's watermark. Though the attacker has only just acquired the image Gw, he can falsely claim that he has always owned both the original and the watermark.

Inversion attacks are made possible by the fact that embedding is an addition and the inverse of an addition is simply a subtraction. As long as watermark embedding is defined by a simple addition rule, an inversion attack can be carried out universally and easily. To avoid inversion attacks, simple addition needs to be replaced by more complex rules. Available devices include the hash function (which embeds hash values into the image) (Schmucker, 2006), non-linear quantisation methods (Chen, 2001), embedding multi-watermarks for verification such as the Zero-Knowledge Proof (Li, 2006) and using a one-way function which is not yet available through mathematical research. In this paper, we introduce some constraints to the addition rule in embedding, though the embedding itself remains an addition.

Given the considerations above, we introduced the Singular Value Decomposition (SVD) operation as a constrained condition for the addition rule. Normal usage effectively says, "A watermark was embedded in the image using SVD." If we decompose the image matrix using SVD, singular values all appear as positive data in a diagonal position. All other off-diagonal elements are zeros. If we add a watermarking value in an off-diagonal position, the embedded image is modified by an addition. However, the SVD results of the embedded image differ from those of the original SVD operation in that the decomposing matrices are different. The difference is not simply linear and continuous, but complex and discontinuous. Moreover, it is difficult to obtain a negative watermark for the embedded image through random, or trial and error searches. As a result, it is not easy to make an inversion attack on the SVD watermarking scheme.

Disabling an inversion attack requires the embedding process to have a type of one-way characteristic. In this case, it is important to evaluate the number of calculations involved in the one-way function with regard to forward and backward operations. Embedding a watermark by SVD is formalised as a function from an image to an embedded image through an SVD framework. The existence of an accurate one-way function defined by mathematical language has not yet been proved. In a practical sense, whether or not the number of operations is large or small is more relevant than accurate proof of behaviour in an infinite area. It is nevertheless difficult to prove the number of operations for a specific function in a mathematical way. It is possible to evaluate a given system numerically from an external engineering perspective. In this paper, the distance between matrices is examined. Some discontinuous phenomena are obtained which prove at the very least that the system is of a one-way type.

In the following sections, a basic SVD watermark relation is described. SVD watermarking is then revised for numerical analysis and in order to form a quasi-one-way function. The SVD method is revised by defining it accurately, and by explaining the behaviour of an inversion attack. Thereafter, the embedding process is defined as quasi-one-way mapping. Finally, numerical evaluations are carried out to highlight discontinuities and errors between the original data and the embedded data.

2. Basic SVD Watermarking System

Fig.1 shows a basic SVD watermarking framework. An input image G is decomposed by the SVD method. A watermark is embedded in the SVD domain and, using synthesised inverse decomposition, we obtain an embedded image Gw. The singular value matrix S is unique, while U and V are not unique. The embedding operation is represented by an addition "+W". This operation is reversible, which means the inverse of the addition is shown as a subtraction "-W". SVD is not reversible when watermarking is embedded. The SVD results for the embedded image Gw are different from the original decomposed data, S,U and V. The SVD of Gw is called the second SVD, SVD_b. Thin arrows with no changes in width represent one-to-one conversions. Arrows with width changes represent conversions one-to-n or n-to-one. Conventional SVD watermarking methods (Gorodetski, 2001) use SVD_b. In this paper we employ SVD in detecting the Gw watermark.

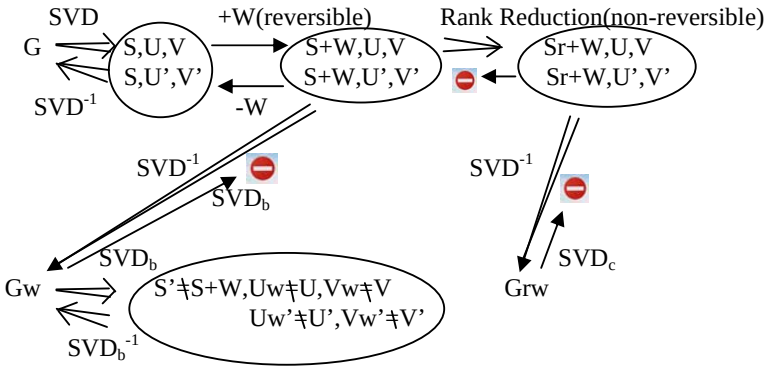


Fig.1 Basic SVD Watermarking Framework.

A watermarking system using this type of Singular Value Decomposition (SVD) was first proposed by Ohzeki (2005, 2008a, 2008b). In the current paper, it is revised and formulated with much stricter criteria regarding one-way characteristics. Let an image G be a square matrix. For a rectangular image, the method can easily be extended from the square matrix to a rectangular one by normal Singular Value Decomposition. We have observed that most square scenic image matrices are regular. For non-regular matrices, a partial matrix can be used up to the number of ranks after decomposition. G is represented in polar decomposition as:

$$G = |G| \cdot P , \tag{1}$$

where $|G|$ is a symmetric and positive matrix (positive definite), and P is an orthogonal matrix. $|G|$ is diagonalised as follows:

$$|G| = Q^T \cdot S \cdot Q \,. \tag{2}$$

S is a diagonal matrix with eigenvalues λ_i of $|G|$ in the diagonal position. Each of the λ_i are real and positive.

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N > 0$$

Combining (1) and (2), we obtain:

$$G = Q^T \cdot S \cdot Q \cdot P \,. \tag{3}$$

By making $U = Q^T$ and $V = P^T \cdot Q^T$ orthogonal matrices, we obtain:

$$G = U \cdot S \cdot V^T \,. \tag{4}$$

The above formula (4) is known as Singular Value Decomposition. S is a square root matrix of the eigenvalue matrix $G \cdot Gt = G \cdot G^T$. In terms of polar decomposition, $|G|$ and P are unique. Consequently, S is also unique, but U and V are not unique.

2.1 SVD Watermark Embedding (Ohzeki, 2008b)

The reason for introducing the SVD process to obtain one-way characteristics is so that all singular values in the diagonal position are positive, and all other off-diagonal elements are zeros after obtaining the singular value matrix S by an SVD. If we add a watermark element, W, in an off-diagonal position, as SS=S+W, and synthesise an embedded image Gw, then the added information will diminish during the second SVD of Gw as long as we adopt a rule for conducting SVDs. This produces a type of one-way characteristic with the ability to prevent inversion attacks.

In fact, the modified singular matrix SS=S+W is simply multiplied by the decomposing matrices U and V to synthesise image data in the following way:

$$G_W = U * SS * V^T \,. \tag{5}$$

Gw is an embedded image. Formula (5) and the above formulae are the definition of SVD watermarking, and we designate them as SVD1.

SVD1 has a problem. Ohzeki (2008a) has reported a type of inversion attack on SVD1. A revised version, SVD2, was proposed by reducing the rank of the matrix S (Ohzeki, 2008b).

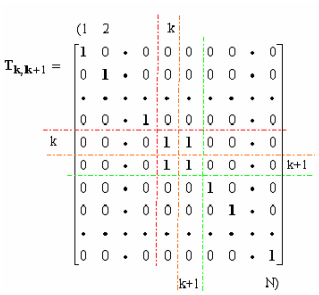
Decomposition by the SVD2 method was obtained using a special rank reduction matrix Tk (Ohzeki, 2008a, 2008b):

$$Gw2 = U * S * T_k * V^T \tag{6}$$

A typical example of W and Tk is:

$$W = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & w & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{7}$$

where w≠0 is a non zero watermark component.



The watermark "W" appears in a number of positions in the off-diagonal area. The pattern of the distributed watermarks in the off-diagonal area could be used by the owner as personal identification unknown to anyone else.

2.2 Mapping of the Embedding Procedure

We can now formalise the watermark embedding procedure using SVD as mapping. The embedding procedure is not a simple function which produces a single value. We therefore call the procedure mapping. Let m be a mapping procedure:

$$m : G \rightarrow G_w . \quad (8)$$

We have two types of mapping, one for SVD1 and one for SVD2. Let the difference between the original image G and the embedded image Gw be Emb_Diff. Then, Emb_Diff=Gw-G.

For G, Gw is simply an addition result. An inversion attack is run on Gw to find the -Emb_Diff',

which conforms to the SVD rule. However, there is no general-purpose -Emb_Diff. For Gw, if an attacker places –Emb_Diff in an off-diagonal position of Sw, the reproduced orthogonal matrices U' and V' will be different from the original matrices. At the very least, iterative operations may be necessary in order to find the decomposing matrices that conform to the SVD rule.

In other words, the embedding mapping procedure m, defined by (8), is not a simple addition with inverse elements of subtraction. It is an addition with a number of constrained conditions.

The degree of quasi-one-way mapping in this embedding process will be discussed in the following section.

2.3 Improvement of Quasi-One-Way Mapping for Embedding

The one-way function has been defined mathematically, but no real one-way function has been reported. However, many functions with one-way characteristics have been devised and used. Examples include the hash function and multiplication of prime numbers with decomposition of the factorisation of the product. Ohzeki (2008a) proposed a relaxed quasi-one-way mapping system (type-1) for watermark embedding. To evaluate quasi-one-way mapping, we propose another type (type-2) with a fixed criterion.

Definition of quasi-one-way mapping (type-2):
We can evaluate a fixed number of operations(C), where

$$C < \mathrm{Min}\left\{\mathrm{Num.of.Operations}(x = m^{-1}(y))\right\}$$

It is difficult to show directly the exact minimum number of reverse operations in SVD embedding mapping. Therefore, we will start by evaluating the distance between the orthogonal matrices U and V of the owner and the matrices Uw and Vw of the attacker. The specific distance between the distance measures will provide circumstantial evidence of non-trivial separate matrices. The measuring method we will use will involve evaluating changes of distance between U and Uw (also V and Vw) in terms of the watermark W, whose element value gradually changes from zero to a non-zero value. If the relation is continuous, the measured distance is also

continuous, but if it is discontinuous, the measured distance changes irregularly. We will, in fact, evaluate the distance in chapter 3, using a numerical calculation. We can at least see that the complexity of the inverse of SVD watermark mapping depends on the number of dimensions in the size of an image, and the number of reduced ranks produced by rank-reduction.

3. Numerical Evaluation

Numerical evaluations are carried out in this chapter for watermark embedding mapping by SVD, together with inverse mapping as quasi-one-way mapping. The distance between the matrices involved in both the diagonal decomposition of the image and quasi-one-way mapping are used for the evaluation.

3.1 Evaluation Using the Euclidean Norm

The distance between U and Uw and the distance between V and Vw are examined in SVD1 as a fundamental evaluation, but SVD1 is unable to resist the inversion attack. The Euclidean Norm, which is typically a unitarily invariant norm, is used for the distance evaluation. The Euclidean Norm is:

$$\|X\|_2 = \left(\sum_{j=1}^{n} \sum_{i=1}^{m} |x_{i,j}|^2 \right)^{1/2} = \left(\sum_{i=1}^{m} \sigma_i^2 \right)^{1/2}, \quad (9)$$

where $n \le m$, $X = (x_{i,j})$ is a unitary matrix, and its eigenvalues are $\sigma_1 \ge \sigma_2 \ge \cdots \ge \sigma_m \ge 0$

Elements of the watermark W vary in magnitude and position. For magnitudes of the elements, the values 1,2,4,8,16,32 are tested. In terms of position, because of the small size of the matrix, a single element is tested for all positions in the upper-right half of SS, as well as two and four elements for a specific position in the upper-right half, and eight elements for a specific position on both sides of SS. Fig. 2 shows all six positions in the upper-right half of SS for a single element case. The results are shown in Fig. 3(a)-(c). The embedded watermarks affect the singular values obtained from the embedded Sw. The effects on the lower parts of SS, where eigenvalues are smaller, are slightly greater than the effects on the other parts, and these are shown in Fig. 3(a). The simple difference between the original and the embedded image is proportional, as shown in Fig. 3(b) by the signal-to-noise ratio (SNR). Fig. 3(c) shows the Euclidean Norm difference between each of the decomposing matrices U and Uw, which depend on the embedding magnitudes. Although the difference increases as the magnitude of the watermark increases, the tendency is not proportional. Instead,

$$W = \begin{bmatrix} \bullet & 1 & 2 & 3 \\ \bullet & \bullet & 4 & 5 \\ \bullet & \bullet & \bullet & 6 \\ \bullet & \bullet & \bullet & \bullet \end{bmatrix}$$

Fig. 2: Embedding position for the upper right-hand part of the watermark matrix. The singular values are in the diagonal position. The size of the image is 4×4. W is added to S as SS=S+W.

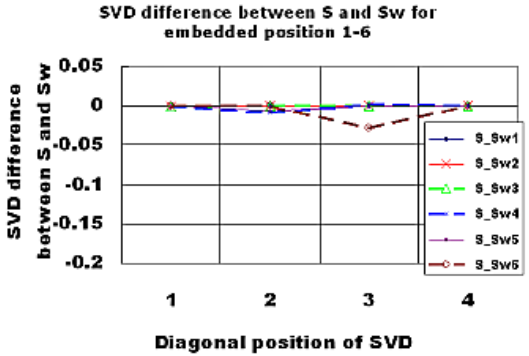


Fig.3 (a) The SVD difference between S and Sw vs. SVD values. SVD values are arranged in descending order. Six embedding positions are investigated. The size of the image is 4×4.

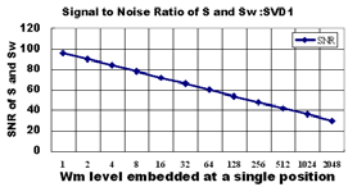


Fig. 3(b) Signal to nise ratio of an embedding error against the magnitude of the watermark. The size of the image is 4x4.

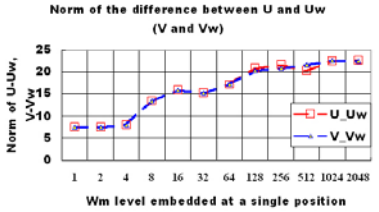


Fig 3(c) Norm difference between U and Uw against the magnitude of the watermark. The size of the image is 4×4.

a staircase pattern can be seen as the magnitude of the watermark increases. This result indicates that, because the Euclidean Norm of formula (9) is continuous since it is a root of the sum of the squared differences of the elements, the diagonal process causes discontinuity. Up to this point, these experiments were carried out for a small 4×4 piece of the real image data in order to be able to see the data directly.

Next, an evaluation of the norm is carried out for a large real image 256×256. Fig.4 shows the Euclidean Norm of the difference between U and Uw against the small difference in the watermark component. The embedded watermark is in the 100^{th} row of the singular matrix S. The 100^{th} singular value is at (100,100) of S. The embedded watermark elements are at (100, P), where P=101, 102,…,256. The embedded watermark magnitudes are at 0.01, 0.1, 1.0, 10.0, and 100.0 in order to observe the detail of the continuity. In Fig. 4, the lowest line represents the case W=0.01. Thereafter, cases W=0.1, 1, 10, and 100 follow from bottom to top in order. For cases W=0.1 and W=1, there are great variations in many parts of the norm differences. These variations should be interpreted as the same watermark position seen vertically at different magnitudes. These cases of discontinuity take place in a specific position of the singular value domain with a large norm difference at a small watermark magnitude difference. This is a symptom of discontinuity in SVD embedding mapping. In the case of W=10 and W=100, the variations are not considered outstanding when seen on the graphs. However, a logarithmic scale graduates the vertical axis, and the differences could be masked out by larger difference values. Another interpretation is that the difference might not be influenced by the magnitude of the watermark and could, in fact, be independent of it, but it could be sensitive to the image or the SVD structure.

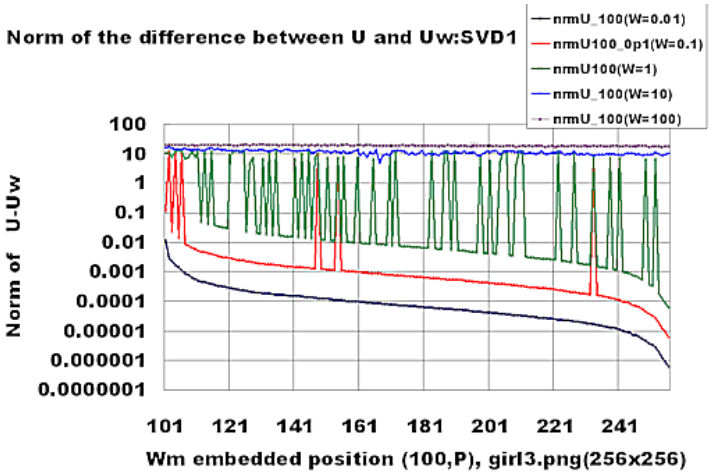


Fig. 4 The Euclidean Norm of the difference between U and Uw vs. the embedded position. The magnitudes of the watermarks are 0.01, 0.1, 1, 10, and 100 from the bottom line to the top respectively. The embedded positions are on the 100th row of the watermark matrix. The size of the image is 256×256.

We shall now describe SVD2. Fig. 5 shows the embedding degradation, the SNR versus the embedding positions, the differences between U and Uw and the differences between V and Vw. In the case of this SVD2, embedding magnitudes are determined by the singular values of the positions. This implies a decrease of embedding magnitudes along the horizontal axis, and an increase of the SNR along the same axis, whereas the norms of the differences decrease along the horizontal axis.

Next, we examine an integrated case of combining the SVD1 and SVD2 methods. The watermarks are embedded as SVD1 and the eigenvalues as SVD2. “LV” indicates the magnitude of the watermark for the SVD1 method. “Num” indicates the number of embedded watermarks using the SVD1 method. Fig. 6 shows the amalgamation of both methods, SVD1 and SVD2. The horizontal axis shows the graduated SNR of the errors between the original image and the watermarked image. On the whole, the relation between errors, and the norm of the difference between the decomposing matrices remain the same, regardless of embedding methods.

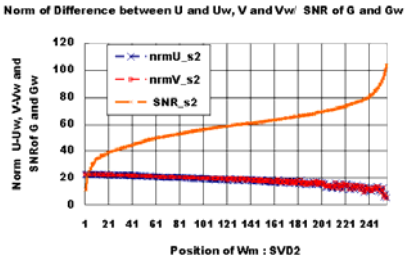


Fig. 5 The SNR of G and Gw vs. the embedding position at the uppermost line. The Euclidean Norm of the difference between U and Uw (V and Vw). Both graphs are for the SVD2 method. The image “girl3.png”is monochrome. The size of the image is 256×256.

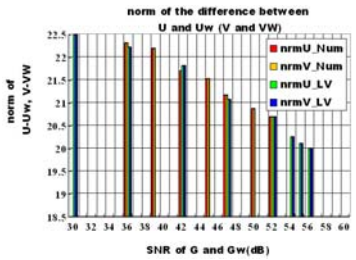


Fig. 6 The Euclidean Norm difference between U and Uw and (V and Vw) vs. the SNR of G and Gw. The image “girl3.png” is monochrome. The size of the image is 256×256.

4. Conclusions

This paper gives a detailed description of how the SVD watermarking system can be revised using a new protocol. A new numerical evaluation is proposed for decomposing SVD matrices in order to make use of quasi-one-way mapping. Although SVD1 is vulnerable to inversion attacks, SVD2 has not yet been subject to an attack.

Numerical evaluation shows that SVD embedding mapping has discontinuous elements in many cases, in the sense that there has to be a large number of differences to make only a small difference in the watermark. This indicates that SVD embedding mapping should create a type of quasi-one-way mapping, thanks to its discontinuity.

The number of calculations in SVD watermarking depends on the size of the image, which means that, at the very least, any attackers will be forced to do more calculations in order to infiltrate the embedding system.

References

1. Freir, L. P. et al., 2006, Watermarking Security: A Survey: Trans on Data Hiding and Multimedia Security I, pp. 41-72.
2. Katzenbeisser, S. ed., 2005, First Summary Report on Hybrid Systems: ECRYPT, D.WVL.5-1.0.pdf
3. Schmucker, M. ed., 2006, Applications, Application Requirements and Metrics, ECRYPT, D.WVL.12-1.0.pdf, Feb.
4. Chen, B. et al., 2001, Quantization Index Modulation: a class of provably good methods for digital watermarking and information embedding, IEEE Trans. IT, Vol. 47 no. 4, pp.1423-1443, May.
5. Li, Q., Chang, E. C., 2006, Zero-knowledge Watermark Detection Resistant to Ambiguity Attacks, Proc. ACM MMSec. Workshop, pp. 158-163, Sept.
6. Ohzeki, K., Cong, L., 2005, Consideration of Variable Embedding Framework for Image Watermark against Collusion Attacks, Wavilla Challenge (WaCha), 2005, Proc. of the WAVILA Workshop D.WVL.2-1.0.pdf, pp.54-62. June 8-9,
7. Ohzeki, K., Sakurai, M., 2008a, SVD-Based Watermark with Quasi-One-Way Operation by Reducing a Singular Value Matrix Rank, Proc. of The First International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia (e-forensics 2008), Technical session B4. Watermarking, 1. Jan 22.
8. Ohzeki, K., Gi, E., 2008b, Quasi-One-Way Function and its Applications to Image Watermarking, Proc. of the First International Symposium on Multimedia - Applications and Processing (MMAP in IMCSIT), pp. 501-508, Oct.
9. Gorodetski, V., Popyack, L., Samoilov, V., Skormin, V., 2001, 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, pp.263-274.