Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7739200

ROBUSTNESS OF IMAGE AGAINST AMBIGUITY ATTACK FOCUSING ON SINGULAR VALUE DECOMPOSITION AND REDUNDANT DISCRETE WAVELET TRANSFORM WATERMARKING TECHNIQUES

Priyanka Mishra[1], Rakesh Ahuja[1]
[1]Chitkara University, Institute of Engineering and Technology, Chitkara University, Punjab, India

Abstract
Digital image watermarking technique is being used for confirmation of proprietorship and copyright protection. A novel resilient image watermarking approach that relies on the Redundant Discrete Wavelet Transform and Singular Value Decomposition techniques for these applications were first suggested by Khoo and Makbol (2013). In this research, we provide two ambiguity attacks on this approach to show that it is ineffective for robustness concerns including transaction monitoring, proprietor identification, and ownership assurance.
Keywords: Redundant discrete wavelet transform; Singular Value Decomposition; Ambiguity attack

Introduction

among the most significant benefits of the mathematical period, which is ubiquitous usage of the network that technology, which has made transfer of computerized information a simple task. Furthermore, a large number of associated metadata can easily swappable using Mentoring technique. The astounding digital advancement from analogue to arithmetical innovation did not occur without causing concern about the safeguard of researchers' privileges and the battle against hacker attacks, because those records can be easily reproduced and altered by anybody with no worsening. As a result, it is critical for authors of digital content to defend themselves and protect their own records because they have suffered severe liquidity problems. Digital watermarking was presented in this frame of reference to ensure the authority and authenticity of digitized information to incorporate watermark to such records[1-2]. The fundamental concept behind watermarking is to embed hidden confidential message into secured multimedia data.

The suggested watermarking systems in the literature may be categorized in two groups predicated on the transform and spatial domain. Original pixel of cover image is altered in spatial domain to insert watermark. In contrast, the transform domain includes image of watermark to embed it with actual picture frequency domain coefficients. Decomposing a picture into It is not always advantageous to use a standard basis set in the frequency domain. As a result, utilizing linear algebra techniques like SVD-based approaches, several transform representations for watermarking were examined. (Tan and Liu, Raman and Bhatnagar, Hu et a1., 2012 2009, 2012;). Additionally, It has been proven that SVD watermarking techniques have a very high resistance to many different types of attacks. Some SVD-based watermarking techniques are ineffective and have unacceptably large rates of false positive detections as

described by Liu and Tan, 2002; Shieh et al(2006), Eskicioglu(2005), Ganic,and Lai(2011) and Abdallah et al(2007) and these are reported in the literature by Rykaczewski (2007), Loukhaou (2009), Zhang et al. (2005) and Loukhaoukha and Loukhaoukha (2012, 2013).

This article examines the method suggested by Makbol and Khoo's(2013) for watermarking techniques RDWT and SVD for digital images[4-6]. We demonstrate that this system is inefficient for transaction monitoring, validating ownership, and identifying ownerss since it does not connect an original picture to a watermark. The topic notion of singular value decomposition is briefly discussed in Section 2. Also, Section 3 provides a description of algorithm of watermarking developed by author Makbol and Khoo in 2013. Two ambiguity attacks on this watermarking approach are given in Section 4 of the paper. Also Section 5 presents the experimental findings about these attacks. Section 6 wraps up the project completely[7-10].

Singular Value Decomposition Technique

The watermarking technique SVD may be used to break down any matrix of size M x N, however we will only discuss square matrices in this exposition (SVD). The SVD method is described in the following way for image of size N x N:

$$I = U.S.V^T \quad \text{.....} \quad (1)$$

where $U \in \mathfrak{R}^{N \times N}$ and V $\in \mathfrak{R}^{N \times N}$ are left and right singular vectors used to describe orthogonal matrices.

Also $S \in \mathfrak{R}^{N \times N}$ is a diagonal matrix with nonnegative terms that has a single valued. The following gives a basic illustration of the SVD operation[11-12]:

$$A = \begin{bmatrix} 156 & 157 & 158 & 159 \\ 157 & 157 & 158 & 158 \\ 159 & 158 & 156 & 155 \\ 159 & 158 & 156 & 155 \end{bmatrix} = \begin{bmatrix} -0.5008 & -0.6225 & 0.6014 & 0 \\ -0.5008 & -0.3584 & -0.7879 & 0 \\ -0.4992 & 0.4920 & 0.0935 & -0.7071 \\ -0.4992 & 0.4920 & 0.0935 & 0.7071 \end{bmatrix}$$

$$\text{x} \begin{bmatrix} 629.0028 & 0 & 0 & 0 \\ 0 & 4.8302 & 0 & 0 \\ 0 & 0 & 0.4394 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \text{x} \begin{bmatrix} -0.5016 & 0.6366 & -0.3053 & 0.5000 \\ -0.5008 & 0.3040 & 0.6378 & 0.5000 \\ -0.4992 & -0.3065 & -0.6379 & 0.5000 \\ -0.4984 & -0.6391 & 0.3052 & -0.5000 \end{bmatrix}$$

A number of the singular value decomposition's properties include:

Singular values represent the image's brightness. Assuming that the SVD is used to decompose the picture shown in Figure 1, the principal components are first multiplied by 2 and afterwards divided by 2. The pictures that were acquired are shown in Fig. lb and 1c, respectively[13]. It is obvious that as the pictures' single values change, their brightness also does.

(a) Original Picture (b) Regenerated Picture: SVs (c) Regenerated Picture:: SVs

Fig. 1. Effects of changing Singular Values of images

(a) Host image (b) Regenerated Picture:

Fig. 2. Changes in Singular Vectors' Effects.

Single-vector systems describe the image's innately geometrical characteristics. The single-vector systems of identical picture are substantially modified as in Fig. la. The matrix U is increased by 0.025, and the matrix V is decreased by the same amount. The resulting picture is shown in Fig. 2, where the image's geometry has been drastically altered.

• The great stability of single values suggests that even a little alteration has no effect on how the image is visually perceived. In Fig. 3, a case of the constancy of the singular values is illustrated by the addition of a minor disturbance having a value of 5. The value of PSNR of both the original and rebuilt images are identical to 63.29 dB, demonstrating that this disturbance has no effect on how the reproduced image is perceived visually[14-15].

Singular Value Decomposition Watermarking Technique

In this part, the robust blind picture watermarking method is discussed. This method is developed by Makbol and Khoo using SVD and RDWT watermarking techniques[16-19]. The following steps make up the embedding of a watermark:

(1) To split the original image into the four sub-bands LL, LH, HL, and HH, use the RDWT one level approach.

(2) Use the following watermarking SVD procedure on each of the four sub-bands:

$I^i = U^i \cdot S^i \cdot V^{iT}$

(a) Host Image (b) Regenerated Image

Fig. 3. Impact on images

(3) Add watermark to single values S^i for every sub-band.

$$S_M^i = S^i + \alpha \cdot W \tag{3}$$

(4) Execute the following SVD operation on the matrix S_M^i for each sub-band:

$$S_M^i = U_W^i \cdot S_W^i \cdot V_W^i \tag{4}$$

where *i* shows the sub-bands *and* α indicates the scaling factor. Here the value of α is 0.05 to insert watermark into the LL sub-band and α is 0.005 for the other sub-bands.

(5) Execute each coefficients of each sub-bands of RDWT.

$$I^{inew} = U^i \cdot S_W^i \cdot V^{iT} \tag{5}$$

(6) To produce watermarked picture I_W, the reversed watermarking method RDWT with the four pairs of altered coefficients are used.

By effectively reverse processing embedding procedure for distorted watermark image W*, a potentially deformed watermark I^*_W is recovered by potentially deformed watermarked picture i in the extraction step[20-23]. It should be noted

that U_W^i and V_W^i will be preserved and required while removing the watermark as described in following steps:

(1) RDWT technique is applied on the most likely deformed image to separate it into its four sub-bands.
(2) Use the following SVD procedure on all sub-bands.

$$I_W^* = U^{i*} \cdot S^{i*} \cdot V^{i*} \tag{6}$$

where the sub-bands are indicated by i.

(1) Calculate

$$D^{*i} = U_W^{*i} \cdot S^{*i} \cdot V_W^{*iT} \tag{7}$$

where I is shown for four sub-bands.

Calculates

$$W^{*i} = \frac{D^{*i} - S^i}{\alpha} \tag{8}$$

where W^{*i} is recovered watermark.

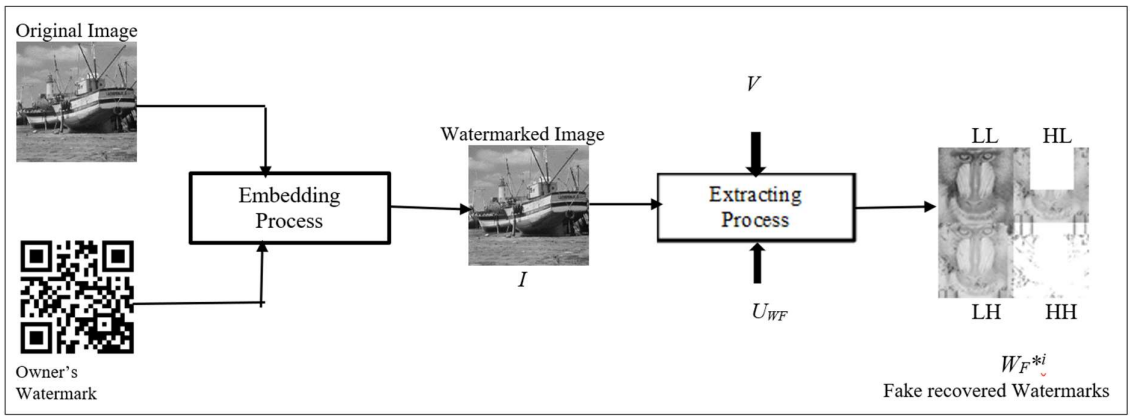


Fig. 4. Diagram depicting first attack

Ambiguity Attack

The groundwork for the ambiguity attack has been shown by Craver et al in 1998. This approach allows the owner to separate his watermark from the watermarked information. Similar to how the attacker may remove his own watermark, no client can establish which of them is correct, leading to uncertainty and the inability for anybody to assert ownership[24-27]. The digital watermarking technique developed by author Makbol and Khoo in 2013 and subject to attacks in this section. It proves that it is not suitable for identification and authentication. These attacks are based on Redundant Discrete Wavelet Transform and Singular Value Decomposition watermarking techniques.

First attack

Assume that Alice, the proprietor, followed steps 1 to 6 to and insert personalized watermark named W into the host picture named I, resulting in the watermarked image designated by I. Alice completes the extraction procedures in order to assert her ownership of picture I. (from 1 to 4). She is regarded as the true owner if her watermark is effectively removed from the watermarked imageI_WO^ . The SVD watermarking technique is then claimed to Bob's private image of watermark, which provides the result UWF and VWF., Now step 4 is performed Bob. Following are the measures he takes while extracting the watermarked picture I in order to demonstrate his ownership of it[28-32]:

(1) With the watermark's singular values S^{*i}, steps 1 and 2 are finished that were obtained via estimate and all specified components.
(2) Steps 3 can be completed as follows by providing U_{WF} and V_{WF}:

$$D_F^{*i} = U_{WF}^{*i} \cdot S^{*i} \cdot V_{WF}^{*iT} \tag{9}$$

where I stand for the sub-bands.
(3) W^{*i} is the recovered watermark, where i denotes the sub-bands.

$$W^{*i} = \frac{D^{*i} - S^{i}}{\alpha} \tag{10}$$

The watermark W^{*i} is watermark image of Bob and it is successfully extracted from watermarked image I for each sub-band. Figure 4 displays a schematic diagram for this kind of attack[33-36].

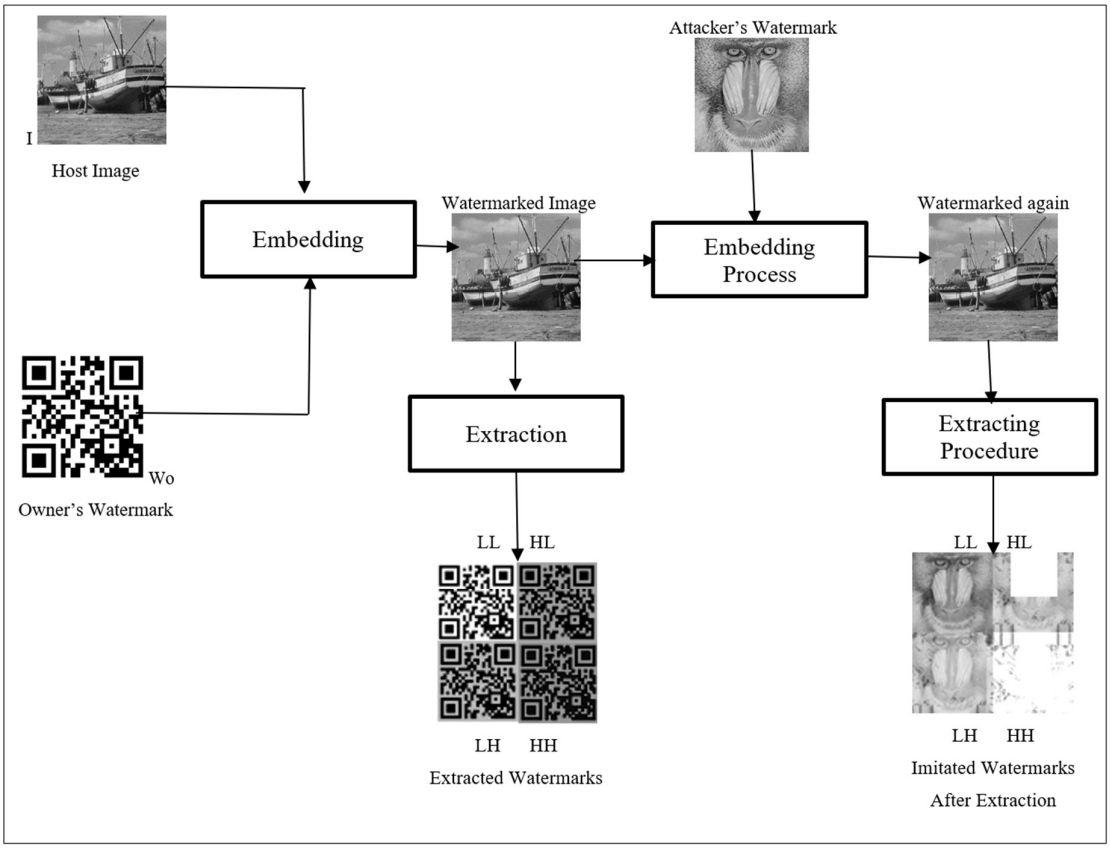


Fig. 5. The second attack's diagram.

Second attack

Imagine that the image I belongs to Alice and watermark is now inserted to it, making it the original watermarked image rather than I. Because Alice and Bob each have the ability to remove their own watermarks, they are both equally able to claim possession of the actual picture in this circumstance, which raises questions about who exactly the rightful owner is. In the end, nobody is sure if Alice or Bob are communicating the truth. In Fig. 5, the attack's block diagram is shown[37-42].

Outcomes of Experiments

Experiments are conducted in this part to demonstrate the potency of the attacks suggested in Section 4. The original pictures Lena and Peppers are utilized The size of images are 256 x 256

as shown below. Owner and attacker watermarks, also listed below in same size, are shown in Fig. 6[43-44].

We assume the role of Bob in this part and two experiments are run in response to each attack. First, Proprietor of the actual pictures is Alice. Image Lena is designated as I1 and the image Peppers represented as I2. . Also, her owner watermark WO is added in the image by using the embedding method just as described in Section 3[45]. Now I_Wo^1 and I_Wo^2 are the current watermarked pictures respectively.

(a) Image of Lena (b) Image of Boat (c) Watermark of owner (d) Attacker's watermark

Fig. 6. Host Images and Watermark Images.

Table 1

Watermarks are retrieved from sub-bands and watermark image of attacker, with a normalized correlation.

Watermarked Pictures	Recovered watermark	NC of Extracted Watermark
I_{Wo}^{1}	W_{1F}^{*LL} W_{1F}^{*HL} W_{1F}^{*LH} W_{1F}^{*HH}	0.9812 0.9102 0.8702 0.8832
I_{Wo}^{2}	W_{2F}^{*LL} W_{2F}^{*HL} W_{2F}^{*LH} W_{2F}^{*HH}	0.9825 0.9216 0.9017 0.8654

(a) (b) (c) (d) (e)

Fig. 7. Preliminary Observation: (a) Watermark embedded, (b) to (e)Watermark extracted

First attack

The extraction procedure outlined in Section 3 is carried out to remove the watermark from the watermarked pictures I1Wo and I2Wo. If UWF and VWF, which are calculated from the attacker watermark WF, are not employed as opposed to the singular vectors UW and VW based on owner's watermark WO as shown in Fig. 6d. The extracted watermarks are W*i1F and W*i2F, where i is corresponding to the watermarked image sub-bands. I1Wo and I2Wo

are false watermarks which resemble the attacker watermark both geometrically and visually. The attacker watermark WF and the watermarks that were retrieved from the watermarked picture, I1Wo and I2Wo ,are correlated in Table 1 using normalized correlation values (NC)[46-48].

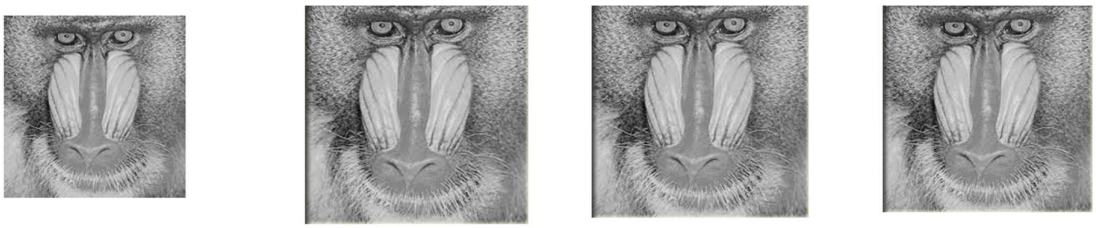
Figures 7 and 8 shows embedded and extracted watermarks respectively. Although the watermark that is included in the original pictures is the watermark of the owner. The recovered watermarks are obviously geometrically and visually same as watermark of an attacker[49].

(a) (b) (c) (d) (e)

Fig. 8. Secondary Observation: (a) Watermarked Image, (b) to (e) Images of watermark extracted

(a) I^1_{Wo} $(b)\ I^1_{WOF}$ (c) I^2_{Wo} (d) $(b)\ I^2_{WOF}$

Fig. 9. Watermarked and re-watermarked images.



(a) W^{*LL}_{1OF} (b) W^{*HL}_{1OF} (c) W^{*LH}_{1OF} (d) W^{*HH}_{1OF}

Fig. 10. Extracted watermarks from watermarked images I_WOF^1

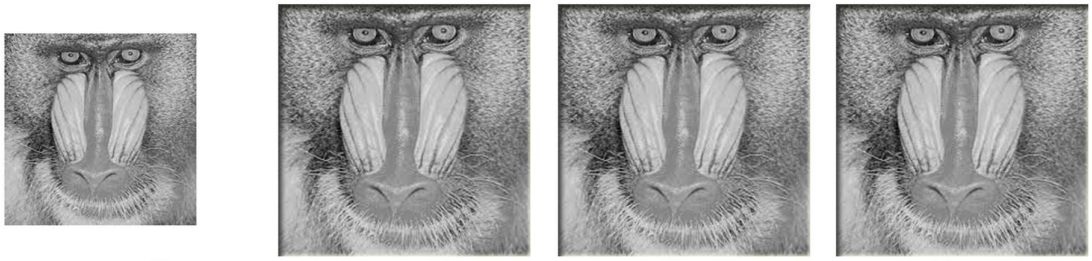
Second attack

The watermark W_F of the attacker, as described in Section 3, is added to the watermarked images $I^1_{Wo}\ and\ I^2_{Wo}$to create pictures with watermarks named I^1_{WOF} and I^2_{WOF} as shown in Fig. 9b and 9d. Theses have PSNR values that are identical to 48.26 dB and 49.18 dB for their original images respectively.

The watermarked pictures $I^1_{Wo}\ and\ I^2_{Wo}$ accordingly in Figures 9a and 9c. These are extracted to provide the watermark $W^{*i}_1\ and\ W^{*i}_2$ of Alice, in accordance with the scenario described in Section 4.2. It is evident from looking at Figs. 10 and Fig.11 that recovered watermarks are aesthetically and geometrically comparable with owner's watermark W_O.

The watermarks that were retrieved as well as the owner's W_O watermark W_1^{*i} *and* W_2^{*i}have normalized correlation (NC) values of 0.9989, 0.9942, 0.9939, and 0.9975, and 0.9982, 0.9946, 0.9940, and 0.9922 respectively [50-52].

Additionally, we can also eradicate the watermarks W_{1O}^{*i} from the watermarked images I_{WOF}^{1}. These extracted water- marks are introduced in Fig. 10, when they resemble the watermark of the attacker named W_F both geometrically and visually.



(a) W_{2OF}^{*LL} $(b)W_{2OF}^{*HL}$ $(c)W_{2OF}^{*LH}$ (d) W_{2OF}^{*HH}

Fig. 11. Extracted watermarks

Additionally, we are able to recover the watermarks WF from the I_Wo^1 and I_Wo^2 watermarked pictures. It is clear from Fig. 10 that these recovered watermarks are geometrically and visually identical to the attacker's watermarks I_WOF^1 and I_WOF^2. They have a normalised correlation (NC) of 0.9993, 0.9970, 0.9965, and 0.9934 with the intruder watermark OF, where I denote the sub-bands of image[53].

Additionally, we can recover watermarks W2'QF from the watermarked pictures. These retrieved watermarks are shown in Fig. 11, where it is obvious that they share many visual and geometrical characteristics of attacker's watermark OF. Along with the attacker watermark, a normalized correlation value is also available. These values are 0.9991, 0.9967, 0.9972, and 0.9918, where I stand for the sub-bands of image[54].

Retrieved watermarks are shown in research observations above which create a scenario. Due to the fact that it is impossible to tell if Alice or Bob are telling the truth, it is unclear who the real owner of original photograph I is. Accordingly, it is not recommended to utilize the watermarking techniques SVD and RDWT suggested by Makbol and Khoo (2013) for proving ownership and owner verification[55-60].

Conclusion

The study presents an image watermarking technique based on redundant discrete wavelet transform and singular value decomposition developed by Makbol and Khoo in 2013 to be ineffective against the two ambiguity attacks. During the separation process, an attacker possibly asserts that using the precise vectors of any false watermark, the watermark is implanted so the user may take possession of the watermarks. Every watermarked image in the massive attack is visible to the public and is eligible for re-watermarking with the attacker's watermark. The implanted watermark can be claimed by this individual. According to testing results, Use of this technique for authentication and identification purposes is not advised.

References

- Ganic, E., Eskicioglu, A., 2005. Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition. J. Electron. Imaging 14 (October (4)), 043004–043004-9.
- Lai, C.-C., 2011. A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. Dig. Signal Process. 21 (July (4)), 522–527.
- Loukhaoukha, K., Chouinard, J.-Y., 2010. On the security of ownership watermarking of digital images based on SVD decomposition. J. Electron. Imaging 19 (March (1)), 013007, 9pp.
- Loukhaoukha, K., 2012. On the security of digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. J. Inf. Hiding Multimed. Signal Process. 3 (April (2)), 135–141.
- Loukhaoukha, K., 2013. Comments on "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm". Dig. Signal Process. 23 (July (4)), 1334
- Shieh, J.-M., Lou, D.-C., Chang, M.-C., 2006. A semi-blind digital watermarking scheme based on singular value decomposition. Comput. Stand. Interfaces 28 (April (4)), 428–440
- Abdallah, E., Hamza, A.B., Bhattacharya, P., 2007. Improved image watermarking scheme using fast Hadamard and discrete wavelet transforms. J.Electron. Imaging 16 (July (3)), 1–9.
- Bhatnagar, G., Raman, B., 2009. A new robust reference watermarking scheme based on DWT-SVD. Comput. Stand. Interfaces 31 (September (5)),1002–1013.
- Craver, S., Memon, N., Yeo, B.-L., Yeung, M.M., 1998. Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks,and implications. IEEE J. Sel. Areas Commun. 16 (May (4)), 573–586.Ganic, E., Eskicioglu, A., 2005. Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition. J.Electron. Imaging 14 (October (4)), 043004–043004-9.
- Hu, W.-C., Chen, W.-H., Yang, C.-Y., 2012. Robust image watermarking based on discrete wavelet transform-discrete cosine transform-singular value decomposition. J. Electron. Imaging 21 (July–Sept (3)), 033005, 7pp.
- Lai, C.-C., 2011. A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. Dig. Signal Process. 21 (July(4)), 522–527.
- Liu, R., Tan, T., 2002. A SVD-based watermarking scheme for protecting rightful ownership. IEEE Trans. Multimed. 4 (March (1)), 121–128.
- Loukhaoukha, K., Chouinard, J.-Y., 2010. On the security of ownership watermarking of digital images based on SVD decomposition. J. Electron. Imaging 19 (March (1)), 013007, 9pp.
- Loukhaoukha, K., 2012. On the security of digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. J. Inf. Hiding Multimed. Signal Process. 3 (April (2)), 135–141.368 K. Loukhaoukha et al. / Journal of Electrical Systems and Information Technology 4 (2017) 359–368
- Loukhaoukha, K., 2013. Comments on "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm". Dig. Signal Process. 23 (July (4)), 1334.

- Makbol, N.M., Khoo, B.E., 2013. Robust blind image watermarking scheme based on Redundant Discrete Wavelet Transform and Singular Value Decomposition. Int. J. Electron. Commun. 67 (February (2)), 102–112.
- Rykaczewski, R., 2007. Comments on "an SVD-based watermarking scheme for protecting rightful ownership". IEEE Trans. Multimed. 9 (February (2)), 421–423.Shieh, J.-M., Lou, D.-C., Chang, M.-C., 2006.
- Xiao, L., Wei, Z., Ye, J., 2008. Comments on "Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition" and theoretical analysis. J. Electron. Imaging 17 (October (4)), 040501–040501-3.
- Zhang, T., Zheng, Z.L.W.M., Liu, B., 2008. Comments on "A semi-blind digital watermarking scheme based on singular value decomposition". In: Proceedings of International Conference on Intelligent Systems Design and Applications, November, pp. 123–126.
- J. Cox, F. Kilian, F. T. Leighton, and T. G. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673–1687, Dec. 1997.
- Adelsbach, B. Pfitzmann, and A. R. Sadeghi, "Proving ownership of digital content," in Proc. IHW, Lecture Notes Comput. Sci., 2000, vol. 1768, pp. 126–141.
- Nikolaidis, S. Tsekeridou, A. Tefas, and V. Solachidis, "A survey on watermarking application scenarios and related attacks," in Proc IEEE Int. Conf. Image Processing, Oct. 2001, vol. 3, pp. 991–994.
- S. Voloshynovskiy, T. Pun, J. J. Eggers, and J. K. Su, "Attacks on digital watermarks: Classification, estimation-based attacks, and benchmarks," IEEE Commun. Mag., vol. 39, no. 8, pp. 118–126, Aug. 2001.
- S. Craver, N. Memon, B. Yeo, and M. Yeung, "Resolving rightful own- ership with invisible watermarking techniques: Limitation, attacks, and implications," IEEE J. Sel. Areas Commun., vol. 16, no. 4, pp. 573–586, May 1998.
- M. Ramkumar and A. N. Akansu, "Image watermarks and counterfeit attacks: Some problems and solutions," presented at the Content Secu- rity and Data Hiding in Digital Media, Newark, NJ, 1999.
- Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," IEEE Trans. Inf. Theory, vol. 47, no. 4, pp. 1423–1443, Jul. 2001.
- P. Moulin and R. Koetter, "Data hiding codes," Proc. IEEE, vol. 93, no. 12, pp. 2083–2126, Dec. 2005.
- Adelsbach, S. Katzenbeisser, and A. Sadegi, "On the insecurity of non-invertible watermarking schemes for dispute resolving," presented at the IWDW, Seoul, Korea, 2003.
- S. Craver, N. Memon, B. Yeo, and M. Yeung, "Can invisible water- marks resolve rightful ownerships," IBM Res. Inst., Tech. Rep. RC 20509, 1997.
- W. Zeng and B. Liu, "On resolving rightful ownerships of digital im- ages by invisible watermarks," in Proc. ICIP, 1997, pp. 552–555.
- L. Qiao and K. Nahrstedt, "Watermarking methods for MPEG encoded video: Towards resolving rightful ownership," in Proc. ICMCS, 1998, vol. 9, no. 3, pp. 194–210.

- R. B. Wolfgang and E. Delp, “A watermarking technique for digital imagery: Further studies,” in Proc. SPIE: Voice, Video Data Commun., 1997, pp. 297–308.
- M. Ramkumar and A. N. Akansu, “A robust protocol for proving own- erhsip of multimedia content,” IEEE Trans. Multimedia, vol. 6, no. 3, pp. 469–478, Jun. 2004.
- S. Katzenbeisser and H. Veith, “Securing symmetric watermarking schemes against protocol attacks,” in Proc. SPIE: Security Water- marking Multimedia Contents, 2002, vol. 467, pp. 260–268.
- Adelsbach, S. Katzenbeisser, and H. Veith, “Watermarking schemes provably secure against copy and ambiguity attacks,” presented at the ACM CCS-10 Workshop on Digital Rights Management, Washington, DC, 2003.
- Adelsbach and A. R. Sadeghi, “Advanced techniques for dispute resolving and authorship proofs on digital works,” in Proc. SPIE: Security Watermarking Multimedia Contents V, 2003, vol. 5020, pp. 677–688.
- Coskun and N. Memon, “Confusion/diffusion capabilities of some robust hash functions,” presented at the CISS, Princeton, NJ, 2006.
- Coskun, B. Sankur, and N. Memon, “Spatio-temporal trans- form-based video hashing,” IEEE Trans. Multimedia, vol. 8, no. 6, pp. 1190–1208, Dec. 2006.
- V. Monga and M. K. Mihcak, “Robust image hashing via non-negative matrix factorizations,” in Proc. ICIP, Genoa, Italy, Sep. 2005.
- J. S. Seo, J. Haitsma, T. Kalker, and C. D. Yoo, “A robust image finger- printing system using the radon transform,” Elsevier Signal Process.: Image Commun., vol. 19, no. 4, pp. 325–339, 2004.
- Z. Yang, W. T. Ooi, and Q. Sun, “Hierarchical non-uniform locally sensitive hashing and its application to video identification,” presented at the Int. Conf. Image Processing, Singapore, Oct. 2004.
- M. B. Villarino, Sharp bounds for the harmonic numbers. (2005) [Online]. Available: http://www.citebase.org/cgi-bin/cita- tions?id=oai:arXiv.org:math/0510585.
- M. Agoyi, E. Celebi, and G. Anbarjafari, “A watermarking algorithm based on chirp z-transform, discrete wavelet transform, and singular value decomposition,” Signal, Image and Video Processing, vol. 9, no. 3, pp. 735–745, March 2015.
- R. Liu and T. Tan, “A SVD-based watermarking scheme for protecting rightful ownership,” IEEE Transactions on Multimedia, vol. 4, no. 1, pp. 121–128, March 2002.
- E. Ganic and A. M. Eskicioglu, “Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition,” Journal of Electronic Imaging, vol. 14, no. 4, p. 043004âA˘ S¸ 043009, December 2005.
- 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.
- G. C.-W. Ting, “Ambiguity Attacks on the Ganic-Eskicioglu Robust DWT-SVD Image Watermarking Scheme,” in
- Proceedings of International Conference on Information Security and Cryptology, vol. 3935, December 2005, pp. 378–388.

- R. Rykaczewski, “Comments on "an SVD-based watermarking scheme for protecting rightful ownership",” IEEE Transactions on Multimedia, vol. 9, no. 2, pp. 421–423, February 2007.
- P. Bao and X. Ma, “Image adaptive watermarking using wavelet domain singular value decomposition,” IEEE Transaction on circuits and systems for video technology, vol. 15, no. 1, pp. 96–102, January 2005.
- J.-M. Guo and H. Prasetyo, “Security analyses of the watermarking scheme based on redundant discrete wavelet transform and singular value decomposition,” International Journal of Electronics and Communications, vol. 68, no. 9, pp. 816–834, September 2014.
- R.-S. Run, S.-J. Horng, J.-L. Lai, T.-W. Kao, and R.-J. Chen, “An improved SVD based watermarking technique for copyright protection,” Expert Systems with Applications, vol. 39, no. 1, pp. 673–689, 2012.
- H.-C. Ling, R. C.-W. Phan, and S.-H. Heng, “On the security of a hybrid watermarking algorithm based on singular value decomposition and Radon transform,” International Journal of Electronics and Communications, vol. 65, no. 11, pp. 958–960, November 2011.
- L.Xiao, Z. Wei, and J. Ye, “Comments on “Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition” and theoretical analysis,” Journal of Electronic Imaging, vol. 17, no. 4, October 2008.
- K. Loukhaoukha and J.-Y. Chouinard, “On the security of ownership watermarking of digital images based on SVD decomposition,” Journal of Electronic Imaging, vol. 19, no. 1, p. 013007 (pp. 9), March 2010.
- K. Loukhaoukha, “Comments on "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm",” Digital Signal Processing, vol. 23, no. 4, p. 1334, July 2013.
- W. Yongdong, “On the security of an SVD-based ownership watermarking,” IEEE Transactions on Multimedia, vol. 7, no. 4, pp. 624–627, August 2005.
- Malek, M., Dhiraj, B., Upadhyaya, D., Patel, D. “A Review of Precision Agriculture Methodologies, Challenges, and Applications”. Lecture Notes in Electrical Engineering, vol 875, p.285. April 2022. Springer, Singapore. https://doi.org/10.1007/978-981-19-0284-0_25
- Malek, M.S., Gohil, P., Pandya, S., Shivam, A., Limbachiya, K. “A Novel Smart Aging Approach for Monitor the Lifestyle of Elderlies and Identifying Anomalies”. Lecture Notes in Electrical Engineering, vol 875, p. 278. April 2022. Springer, Singapore. https://doi.org/10.1007/978-981-19-0284-0_13
- Gohil P., Malek M., Bachwani D., Patel D., Upadhyaya D., Hathiwala A. “Application of 5D Building Information Modeling for Construction Management”, ECS Transactions, Vol. 107, no. 1, p. 2637, April 2022. DOI: 10.1149/10701.2637ecst