On the Security of a Hybrid SVD-DCT Watermarking Method Based on LPSNR

Huo-Chong Ling[1], Raphael C.-W. Phan[2], and Swee-Huay Heng[1]

[1] Research Group of Cryptography and Information Security,
Centre for Multimedia Security and Signal Processing,
Multimedia University, Malaysia
{hcling,shheng}@mmu.edu.my
[2] Loughborough University, LE11 3TU, United Kingdom
r.phan@lboro.ac.uk

Abstract. Watermarking schemes allow a cover image to be embedded with a watermark, for diverse applications including proof of ownership and covert communication. In this paper, we present attacks on watermarking scheme proposed by Huang and Guan. This scheme is hybrid singular value decomposition (SVD) based scheme in the sense that they employ both SVD and other techniques for watermark embedding and extraction. By attacks, we mean that we show how the designers' security claim, related to proof of ownership application can be invalidated. Our results are the first known attacks on this hybrid SVD-based watermarking scheme.

Keywords: singular value decomposition, watermarking, attacks, proof of ownership, ambiguity, discrete cosine transform.

1 Introduction

Nowadays, information is mostly stored in digital format. This results in widespread duplication of digital content and as a consequence, infringement of copyright has become an important issue that needs to be addressed. Digital watermarking has emerged as an efficient method to curb copyright protection issue. A digital watermarking scheme works by embedding the content owner's watermark into the content without significantly degrading the quality of the content. This watermark could be company's logo or any other text that identifies the owner. Once the case of copyright infringement is found, the owner takes the case of ownership claim to the authority, and proves ownership by performing the watermark extraction process on the claimed content to extract his watermark. Therefore, robustness of the watermarking scheme is an important factor, i.e. it should be infeasible for an attacker to remove, modify or prevent the extraction of an embedded watermark without visible distortions of the image.

In this paper, we concentrate on singular value decomposition(SVD)-based watermarking schemes. SVD is a linear algebra scheme that can be used for many applications, particularly in image compression [1], and subsequently for

Y.-S. Ho (Ed.): PSIVT 2011, Part I, LNCS 7087, pp. 257–266, 2011.

image watermarking [2–13]. For an N-by-N image matrix A with rank $r \leq N$, the SVD of A is defined as $A = USV^T = \sum_{i=1}^{r} u_i s_i v_i^T$ where S is an N-by-N diagonal matrix containing singular values (SVs) s_i satisfying $s_1 \geq s_2 \geq \ldots \geq s_r > s_{r+1} = \ldots = s_N = 0$, and U and V are N-by-N orthogonal matrices. V^T denotes the adjoint (transpose and conjugate) of the N-by-N matrix V. Since the SVs are arranged in decreasing order, the last terms will have the least affect on the overall image.

In past years, several SVD-based watermarking schemes [2–13] have been proposed. The most popularly cited scheme is due to Liu and Tan [12] that makes sole use of SVD for watermarking. They proposed to insert the watermark into the SVs of the cover image and demonstrated its high robustness against image distortion. However, Zhang and Li [14] and Rykaczewski [15] proved that the Liu-Tan scheme suffers from false-positive detection problem, i.e. the case where a watermarked image I_W^* does not contain a particular watermark W_A and yet it can be shown by an attacker that the watermarked image I_W^* does contain the watermark W_A. Therefore, the Liu-Tan scheme was not suitable to be used for proof of ownership application. In 2008, Mohammad et al. [13] proposed an improved variant of the Liu-Tan scheme and claimed that the improved version was able to solve the false-positive detection problem in the Liu-Tan scheme. However, their scheme was fundamentally flawed as proven by Ling et al. [16]. Other attacks on SVD-based watermarking schemes were found in [17–21].

In this paper, we furthermore show attacks on the hybrid SVD-based watermarking scheme proposed by Huang and Guan [9] that uses not just SVD but also discrete cosine transform (DCT) and local peak signal-to-noise ratio (LPSNR). By attacks, we mean that we show how the designers' security claim, related to proof of ownership application can be invalidated.

In Sect. 2, we recall the basics of the scheme proposed by Huang and Guan. We then present attacks on the scheme in Sect. 3 that invalidate the security claim of the designers. Experimental results verifying our attacks are given in Sect. 4, and Sect. 5 proposes countermeasure to the scheme. Finally, Sect. 6 concludes the paper.

2 Hybrid SVD-Based Watermarking Scheme

Huang and Guan [9] proposed a hybrid watermarking method that employs singular value decomposition (SVD), discrete cosine transform (DCT) and local peak signal-to-noise ratio (LPSNR). The SVD transform is performed on the watermark to get its singular values which are then embedded into selected DCT coefficients of the cover image based on Logistic mapping [22]. LPSNR is then applied to the watermarked image to exclude the block artifacts. The watermark embedding steps of the scheme are as follows:

E1. Denote cover image I as an N-by-N matrix and watermark W as an M-by-M matrix. I is divided into non-overlapping 8×8 sub-blocks I_k ($1 \leq k \leq \frac{N}{8} \times \frac{N}{8}$).

E2. Perform SVD on watermark W as:

$$W = USV^T. \tag{1}$$

E3. Select sub-blocks for watermark embedding using Logistic mapping [22], $X_{n+1} = \mu X_n$ (1 - X_n) which maps the unit interval into itself for $\mu \in [0, 4]$. Select initial value $X_0 \in (0, 1)$ as the key and then drop the first 100 iterations to get a chaotic sequence

$$X_{101}, X_{102}, ..., X_{100+\frac{N}{8}\times\frac{N}{8}}. \tag{2}$$

where $\frac{N}{8} \times \frac{N}{8}$ is the length of the chaotic sequence (i.e. the number of 8×8 sub-blocks of cover image I).

E4. Construct another sequence $m_1, m_2, ..., m_{\frac{N}{8}\times\frac{N}{8}}$ from the sequence of (2) to index the sub-blocks in which the S in (1) is going to be embedded. If X_{100+i} is the jth bigger number in the sequence of (2), then $m_i = j$ where $(1 \leq i \leq \frac{N}{8} \times \frac{N}{8})$.

E5. Only sub-blocks with indices m_i are selected for embedding. DCT is performed on these sub-blocks as:

$$F^{m_i}(u, v) = DCT(I^{m_i}(r, c)). \tag{3}$$

where $1 \leq i \leq M$, $1 \leq u, v \leq 8$, $1 \leq r, c \leq 8$. $F^{m_i}(u,v)$ is the coefficient value at position (u,v) in DCT domain, whereas $I^{m_i}(r,c)$ is the coefficient value at position (r,c) in spatial domain.

E6. In each sub-block, one position (u_e,v_e) is selected for embedding S in (1) as:

$$F^{*m_i}(u_e, v_e) = F^{m_i}(u_e, v_e) + \alpha^{m_i} s_i. \tag{4}$$

where $(1 \leq i \leq M)$. Position (u_e,v_e) is chosen under the following rules:

- If s_i belongs to group A (which contains most energy of watermark), then $(u_e,v_e) = (1,1)$.
- If s_i belongs to group B (which contains remaining energy of watermark), then (u_e,v_e) is chosen from set $C = \{(u, v) \mid 1 \leq u \leq 3, 1 \leq v \leq 3, u + v \leq 3\}$.

α^{m_i} is a scaling factor that determines the watermark strength, and it is determined by LPSNR value given in the following equation.

$$\text{LPSNR} = 10\ log_{10} \frac{(L-1)^2}{\frac{1}{8^2}\sum_{r=1}^{8}\sum_{c=1}^{8}[I^*_{m_i}(r,c) - I_{m_i}(r,c)]^2} \tag{5}$$

where L is the number of gray levels, $I^*_{m_i}(r, c)$ and $I_{m_i}(r, c)$ are the spatial coefficient values of the unwatermarked sub-block and the corresponding watermarked sub-block at the position (r, c), respectively.

E7. Perform inverse DCT on all the watermarked sub-blocks and substitute them for the corresponding sub-blocks in the cover image I to obtain the watermarked image I_W.

In order to perform the watermark extraction from the possibly distorted watermarked image I_W^*, the content owner needs to keep U and V (from Step E2), μ and X_0 (from Step E3) and α^{m_i} (from Step E6). The watermark extraction steps are as follows:

X1. Denote the possibly distorted watermarked image I_W^* as an N-by-N matrix. I_W^* is divided into non-overlapping 8×8 sub-blocks I_{Wk}^* $(1 \leq k \leq \frac{N}{8} \times \frac{N}{8})$.
X2. Repeat Steps E3 till E5 using μ and X_0 to find watermarked image's sub-blocks in which the SVs of watermark are embedded.
X3. Based on (4), the SVs of the watermark are extracted by:

$$s^*{}_i = \frac{(F^{*m_i}(u_e, v_e) - F^{m_i}(u_e, v_e))}{\alpha^{m_i}}. \tag{6}$$

The extracted sequence is described as $s^*{}_1$, $s^*{}_2$,...,$s^*{}_M$. $F^{*m_i}(u_e, v_e)$ and $F^{m_i}(u_e, v_e)$ are the DCT coefficient values of watermarked image's and cover image's sub-blocks at position (u_e, v_e) of index m_i respectively.
X4. The watermark is restored by:

$$W^* = US^*V^T. \tag{7}$$

where $S^* = \text{diag}(s^*{}_1, s^*{}_2,...,s^*{}_M)$.

Note that in the watermark embedding Step E2, the content owner needs to keep U and V so that he can use it later in the extraction Step X4.

2.1 On the Security Claim of the Huang-Guan Scheme

Huang and Guan claimed that their scheme was robust since the bigger singular values (SVs) which comprised most energy of the watermark were embedded into the DC components of the sub-blocks of the original cover image and LPSNR method was used. Therefore, their scheme was claimed to be usable in proof of ownership application. Nevertheless, in the next section, we present attacks on this scheme that violate the designers' claims.

3 Attacks on the Huang-Guan Scheme

We show in this section, how attacks can be mounted that invalidate the security claim made by Huang and Guan [9], namely that the scheme can be used for proof of ownership application. For the rest of the section, we will use Alice as the content owner and Bob as the attacker.

3.1 Attack 1

Our first attack invalidates the designers' claim that the Huang-Guan scheme can be used for proof of ownership application. We first recall the fact that in the embedding steps, Alice needs to keep the orthogonal matrices U and V of her watermark W, the parameters μ and X_0 and the scaling factor α^{mi} so that she can use it later in the extraction steps.

In order to launch the attack, Bob needs to obtain the watermarked image I_W^* and performs the embedding Steps E1 - E7 with I_W^*, his own watermark W_B, his own parameters μ_B and X_{B0} and his own scaling factor α^{Bmi} to obtain the watermarked image O. Both watermarked images I_W^* and O are perceptually correlated with each other since the same embedding steps are repeated. A dispute arises when Bob claims that he is the owner of O since he can extract his watermark W_B from O by supplying his own parameters μ_B and X_{B0}, and orthogonal matrices U_B and V_B of his watermark W_B. Alice could also lay equal claim to O since she too can extract her own watermark W from O by supplying her own parameters μ and X_0, and orthogonal matrices U and V of her watermark W. This leads to ambiguity because Bob lays equal claim as Alice, and therefore, no one can prove who the real owner of image O is.

This attack works because for an image I, its orthogonal matrices U and V due to SVD can preserve major information of the image [14, 15]. Therefore, if Bob uses his own U_B and V_B regardless of what the extracted singular matrix S^* is (as in (7)), he can still obtain a good estimate of the watermark W_B during the extraction process.

Besides that, the parameters μ and X_0 do not actually influence the robustness against this ambiguity attack. Their purpose is just to determine the cover image's sub-blocks that are used to embed the SVs of the watermark. Therefore, Bob can use his own parameters μ_B and X_{B0} to determine the sub-blocks that can be used to embed the SVs of his own watermark. Furthermore, Bob can use his own scaling factor α^{Bmi} to determine the strength of his embedded watermark in the watermarked image O.

This attack shows that the Huang-Guan scheme cannot be used for proof of ownership claim, directly invalidating the designers' claim that it can.

3.2 Attack 2

The second attack is another type of ambiguity attack described in Sect. 3.1. In this attack, an attacker can directly prove that the watermarked image I_W^* belongs to him also. The steps of our attack are as follows:

C1. Denote the possibly distorted watermarked image I_W^* as an N-by-N matrix and watermark W_B as an M-by-M matrix. I_W^* is divided into non-overlapping 8×8 sub-blocks I_{Wk}^* $(1 \leq k \leq \frac{N}{8} \times \frac{N}{8})$.

C2. Perform SVD on watermark W_B as:

$$W_B = U_B S_B V_B^T. \tag{8}$$

C3. Repeat Steps E3 - E6 using Bob's parameters μ_B and X_{B0}, his scaling factor α^{Bm_i} and his SVD components from Step C2. However, in Step E6, modify $F^{*m_i}(u_e, v_e)$ as follows:

$$F^{*m_i}(u_e, v_e) = F^{m_i}(u_e, v_e) - \alpha^{Bm_i} s_i. \tag{9}$$

The major change here is that the '+' operation in (4) is being replaced with the '−' operation.

C4. Perform inverse DCT on all the watermarked sub-blocks and substitute them for the corresponding sub-blocks in the image I_W^* to obtain the fake watermarked image O.

Now, instead of using O as the watermarked image, it is used as the cover image in the extraction process. The watermark extraction steps are as follows:

D1. Denote watermarked image I_W^* as an N-by-N matrix. I_W^* is divided into non-overlapping 8×8 sub-blocks I_{Wk}^* $(1 \leq k \leq \frac{N}{8} \times \frac{N}{8})$.

D2. Repeat Steps E3 - E5 using μ_B and X_{B0} to find I_W^*'s sub-blocks in which the SVs of watermark are embedded.

D3. The SVs of the watermark are extracted by:

$$s^*{}_i = \frac{(F^{*m_i}(u_e, v_e) - F^{m_i}(u_e, v_e))}{\alpha^{Bm_i}}. \tag{10}$$

The extracted sequence is described as $s^*{}_1$, $s^*{}_2$,...,$s^*{}_M$. $F^{*m_i}(u_e, v_e)$ and $F^{m_i}(u_e, v_e)$ are the DCT coefficient values of watermarked image I_W^*'s and cover image O's sub-blocks at position (u_e, v_e) of index m_i respectively.

D4. The watermark is restored by:

$$W_B^* = U_B S^* V_B^T. \tag{11}$$

where $S^* = \text{diag}(s^*{}_1, s^*{}_2,...,s^*{}_M)$.

In this attack, Bob uses the fake watermarked image O as the cover image, and proves that the watermarked image I_W^* belongs to him by extracting his watermark W_B from I_W^*. Alice, on the other hand, is also able to extract her watermark W from I_W^*. Therefore, a deadlock has resulted and no one can prove more than the others.

One may argue that Alice can also extract her watermark W from the fake watermarked image O because I_W^* is used as the cover image during the embedding steps and it contains Alice's watermark W. However, Bob can also extract his watermark W_B from Alice's original cover image I due to the properties of SVD [14, 15] as discussed in Sect. 3.1. Bob can just supply his watermark W_B and his fake watermarked image O to extract his watermark from Alice's original cover image I. This is illustrated in the experimental results section.

In either Attack 1 or Attack 2, Huang and Guan concentrated on ensuring that false negatives do not occur, i.e. the case where the watermarked image does indeed contain a watermark and yet it has been modified (while still maintaining perceptual similarity) such that the watermark can no longer be extracted.

Unfortunately, the designers did not treat the case of false positives, i.e. the case where the watermarked image does not contain a particular watermark and yet it can be shown by an attacker that the watermarked image does contain that particular watermark, which has never been embedded in the first place.

4 Experimental Results

In this section, we describe experiments that are carried out to further support our attacks in Sect. 3. Figure 1 shows a cover image, an owner's watermark, the watermarked image after going through the embedding Steps E1 - E7 and the extracted watermark, respectively. The values μ and X_0 used in Step E3 are 3.8 and 0.5 respectively.

Attack in Sect. 3.1 is carried out using the attacker's watermark in Fig. 2(a) and the watermarked image in Fig. 1(c). The values μ_B and X_{B0} used in Step E3 are 3.9 and 0.8 respectively. Figure 2(b) shows the watermarked image after the attack. The peak signal-to-noise ratio (PSNR) and the correlation coefficient (CC) between the watermarked image in Figs. 2(b) and 1(a) are 42.488 dB and 0.999 respectively. The closer the CC value is to either 1 or -1, the stronger the correlation between both images. This shows that both images are perceptually correlated, and the quality of the watermarked image after the attack is still in a very good condition. When no attack is introduced, the PSNR and the CC values between the cover image and the watermarked image are 45.389 dB and 0.999 respectively.

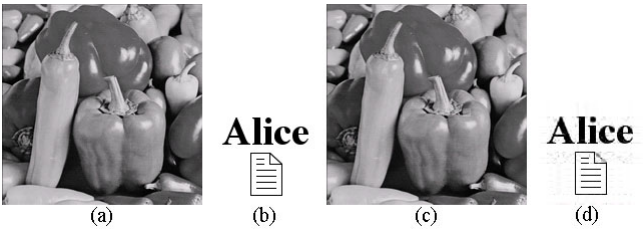

Fig. 1. (a)Original cover image with the size 200 × 200 (b)Owner's watermark with the size 100 × 100 (c)Watermarked image (d)Extracted watermark

Extraction process is then carried out on Fig. 2(b). Figures 2(c) and 2(d) show the extracted watermarks using the attacker's parameters and the owner's parameters respectively. Both attacker's watermark (PSNR = 25.665 dB, CC = 0.991) and owner's watermark (PSNR = 25.563 dB, CC = 0.985) can be extracted successfully.

Attack in Sect. 3.2 is then carried out, and Fig. 3(a) shows the watermarked image after the attack (PSNR = 42.488 dB, CC = 0.999). This watermarked image will then be used as the cover image in the extraction process. The result of the extraction process is that the attacker's watermark as shown in Fig. 3(b)

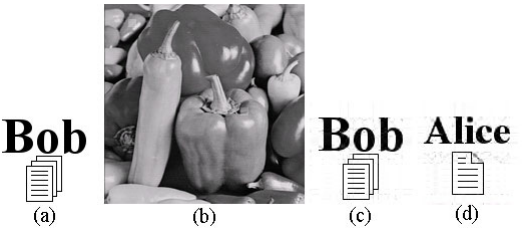

Fig. 2. (a)Attacker's watermark (b)Modified watermarked image after attack. (c)Extracted watermark using attacker's parameters (d)Extracted watermark using owner's parameters

(PSNR = 25.665 dB, CC = 0.991) can also be extracted out, besides the owner's watermark.

One may argue that Alice can also extract her watermark from Fig. 3(a) because the watermarked image in Fig. 1(c) is used as the cover image during the embedding steps and it contains Alice's watermark. However, Bob can also extract his watermark from Alice's original cover image in Fig. 1(a) due to the properties of SVD [14, 15]. In other words, Bob can just supply his watermark's U_B and V_B components and his modified watermarked image in Fig. 3(a) to extract his watermark from Alice's original cover image. This arguement is demonstrated and Figs. 3(c) and 3(d) show the results, where Alice's watermark and Bob's watermark can be extracted successfully.

Therefore, the Huang-Guan scheme is not suitable for protection of rightful ownership.

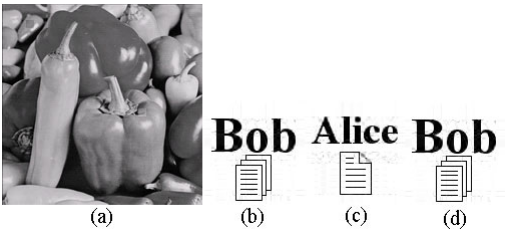

Fig. 3. (a)Modified watermarked image after the attack in Sect. 3.2 (b)Extracted watermark (c) Owner's extracted watermark from Fig. 3(a) (d) Attacker's extracted watermark from Fig. 1(a)

5 Countermeasure

One of the possible countermeasures is to embed the whole watermark into the DC coefficient of cover image's sub-blocks instead of using the SVs of the watermark. This will solve the dependant of orthogonal matrices U and V that influence the watermark being extracted from the watermarked image, at the expense of dropping the SVD in the embedding stage. Huang [23] has proposed

a similar block-based watermarking scheme as in Huang and Guan scheme [9] using DCT and LPSNR. He suggested that other block-based transform domain, such as DFT, DWT and SVD can be used in the proposed scheme. However, as illustrated in the attacks in Sect. 3, it is not feasible to use SVD in the proposed scheme [23].

6 Conclusions

We have presented attacks on a watermarking scheme which is based on a hybrid use of SVD, DCT and LPSNR. These attacks work due to designers' oversight related to properties of the SVD, further supported by our experimental results. Huang and Guan [9] have neglected the fact that an image's orthogonal matrices U and V due to SVD can preserve major information of the image [14, 15]. Our attacks directly invalidate the security claim made by the scheme designers, namely use for proof of ownership application. Our results are the first known attacks on this scheme.

References

1. Andrews, H.C., Patterson, C.L.: Singular Value Decomposition(SVD) Image Coding. IEEE Trans. Commun. 24(4), 425–432 (1976)
2. Aslantas, V.: A Singular-Value Decomposition-Based Image Watermarking using Genetic Algorithm. AEU - Int. J. Electron. Commun. 62(5), 386–394 (2008)
3. Chang, C.C., Tsai, P., Lin, C.C.: SVD-Based Image Watermarking Scheme. Pattern Recognit. Lett. 26, 1577–1586 (2005)
4. Chang, C.C., Hu, Y.S., Lin, C.C.: A Digital Watermarking Scheme Based on Singular Value Decomposition. In: Chen, B., Paterson, M., Zhang, G. (eds.) ESCAPE 2007. LNCS, vol. 4614, pp. 82–93. Springer, Heidelberg (2007)
5. Chang, C.C., Lin, C.C., Hu, Y.S.: An SVD Oriented Watermark Embedding Scheme with High Qualities for the Restored Images. Int. J. Innov. Comput. Inf. Control. 3(2), 609–620 (2007)
6. Ganic, E., Eskicioglu, A.M.: Robust DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies. In: 2004 Workshop on Multimedia and Security, pp. 166–174. ACM, Magdeburg (2004)
7. Ganic, E., Eskicioglu, A.M.: Robust Embedding of Visual Watermarks using Discrete Wavelet Transform and Singular Value Decomposition. J. Electron. Imaging. 14(4), 43004 (2005)
8. Ghazy, R., El-Fishawy, N., Hadhoud, M., Dessouky, M., El-Samie, F.: An Efficient Block-by-Block SVD-Based Image Watermarking Scheme. Ubiquitous Comput. Commun. J. 2(5), 1–9 (2007)
9. Huang, F., Guan, Z.H.: A Hybrid SVD-DCT Watermarking Method Based on LPSNR. Pattern Recognit. Lett. 25, 1769–1775 (2004)
10. Lai, C.C.: A Digital Watermarking Scheme Based on Singular Value Decomposition and Tiny Genetic Algorithm. Digital Signal Processing 21(4), 522–527 (2011)
11. Lagzian, S., Soryani, M., Fathy, M.: A New Robust Watermarking Scheme Based on RDWT-SVD. Int. J. Intell. Inf. Process. 2(1), 22–29 (2011)

12. Liu, R., Tan, T.: An SVD-Based Watermarking Scheme for Protecting Rightful Ownership. IEEE Trans. Multimedia. 4(1), 121–128 (2002)
13. Mohammad, A.A., Alhaj, A., Shaltaf, S.: An Improved SVD-Based Watermarking Scheme for Protecting Rightful Ownership. Signal Processing 88, 2158–2180 (2008)
14. Zhang, X.P., Li, K.: Comments on "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership". IEEE Trans. Multimedia. 7(2), 593–594 (2005)
15. Rykaczewski, R.: Comments on "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership". IEEE Trans. Multimedia. 9(2), 421–423 (2007)
16. Ling, H.C., Phan, R.C.W., Heng, S.H.: Analysis on the Improved SVD-Based Watermarking Scheme. In: Kim, T.H., Adeli, H. (eds.) AST/UCMA/ISA/ACN 2010. LNCS, vol. 6059, pp. 143–149. Springer, Heidelberg (2010)
17. Ling, H.C., Phan, R.C.W., Heng, S.H.: Attacks on SVD-Based Watermarking Schemes. In: Yang, C.C., Chen, H., Chau, M., Chang, K., Lang, S.-D., Chen, P.S., Hsieh, R., Zeng, D., Wang, F.-Y., Carley, K.M., Mao, W., Zhan, J. (eds.) ISI Workshops 2008. LNCS, vol. 5075, pp. 83–91. Springer, Heidelberg (2008)
18. Ling, H.C., Heng, S.H., Goi, B.M.: Attacks on a Block Based SVD Watermarking Scheme. In: 6th Int. Conf. Inf. Technol.: New Generations (ITNG 2009), Las Vegas, Nevada, vol. 1-3, pp. 371–375 (2009)
19. Ting, G.C.W.: Ambiguity Attacks on the Ganic-Eskicioglu Robust DWT-SVD Image Watermarking Scheme. In: Won, D., Kim, S. (eds.) ICISC 2005. LNCS, vol. 3935, pp. 378–388. Springer, Heidelberg (2006)
20. Xiao, L., Wei, Z., Ye, J.: Comments on "Robust Embedding of Visual Watermarks using Discrete Wavelet Transform and Singular Value Decomposition" and Theorectical Analysis. J. Electron. Imaging. 17(4), 40501 (2005)
21. Xing, Y., Tan, J.: Mistakes in the Paper Entitled "A Singular-Value Decomposition-Based Image Watermarking using Genetic Algorithm". AEU - Int. J. Electron. Commun. 64(1), 80–81 (2010)
22. Peitgen, H.O., Jurgens, H., Saupe, D.: Chaos and Fractals: New Frontiers of Science. Springer, New York (1992)
23. Huang, F.: A New General Transparency Model for Block-Based Watermarking Method. Int. J. of Network Secur. 7(2), 235–239 (2008)