DWT-SVD BASED SECURED IMAGE WATERMARKING FOR COPYRIGHT PROTECTION USING VISUAL CRYPTOGRAPHY

Sushila Kamble[1], Vikas Maheshkar[2] , Suneeta Agarwal[3] , Vinay K Srivastava[4]

[1, 2, 3] Department of Computer science & Engineering, MNNIT, Allahabad, India
Sushila@mnnit.ac.in , v_maheshkar@yahoo.com , Suneeta@mnnit.ac.in
[4]Electronics & Communication Engineering, MNNIT, Allahabad, India
vinay@mnnit.ac.in

ABSTRACT

In this paper, a new robust watermarking technique for copyright protection based on Discrete Wavelet Transform and Singular Value Decomposition is proposed. The high frequency subband of the wavelet decomposed cover image is modified by modifying its singular values. A secret key is generated from the original watermark with the help of visual cryptography to claim the ownership of the image. The ownership of the image can be claimed by superimposing this secret key on the extracted watermark from the watermarked image. The robustness of the technique is tested by applying different attacks and the visual quality of the extracted watermark after applying these attacks is good. Also, the visual quality of the watermarked image is undistinguishable from the original image.

KEYWORDS

Image watermarking; Visual Cryptography; Singular Value Decomposition; Discrete Wavelet Transform; Robustness

1. INTRODUCTION

Introduction Digital information is easy to distribute, duplicate and modify which leads to the need for copyright protection techniques. Digital watermarking technique is one of the solutions to avoid unauthorized copying or tampering of multimedia data. Recently many watermarking schemes have been proposed to address this problem. The watermarking schemes are broadly categories into two main domains i.e. spatial domain and the transform domain. In spatial domain watermarking the watermark is embedded by directly modifying the intensity values of the cover image. The most popular technique is the least significant bit (LSB) method. In transform domain the watermark is embedded by modifying the frequency coefficients of the transformed image. The common methods in the transform domain are Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT), etc. Recently, singular value decomposition (SVD) was explored for watermarking. It is one of the most useful numerical analysis techniques having property that the singular values (SVs) of an image do not change significantly when a small perturbation is added to an image. [1-4]

Natarajan Meghanathan, et al. (Eds): ITCS, SIP, JSE-2012, CS & IT 04, pp. 143–150, 2012.
© CS & IT-CSCP 2012 DOI : 10.5121/csit.2012.2113

With the rapid development of internet technology, transmission of multimedia information over the Internet becomes convenient. While transmitting these data security of multimedia data is a prime concern. The hackers may steal information to misuse this important data. Hence secret images are generated before this transmission. One of the solutions to deal with this security problems is Visual cryptography. Naor and Shamir had introduced Visual cryptography [5]. In this paper the authors had proposed encoding scheme to share a binary image into two shares Share1 and Share2. If pixel is white one of the above two possibilities is chosen to generate Share1 and Share2. Similarly If pixel is black one of the below two probabilities is chosen to generate Share1 and Share2. Each share pixel is encoded into two white and two black pixels. Only one cannot give any clue whether the pixel is white or black. The secret image can be revealed only when both the shares are superimposed on each other.

The two major considerations in visual cryptography are pixel expansion and number of shares encoded. If the pixel expansion is smaller then it may results in smaller size of the share. If the multiple secret images are encoded then the same share images requires less overhead while sharing multiple secrets.

Chin-Chen Chang et al [6] also suggested spatial-domain image hiding schemes to hide a binary watermark into two shares. The two different gray level cover images are used to embed these secret shares. Embedding images can be superimposed to decode the hidden messages. To balance the performance between pixel expansion and contrast, Liguo Fang [7] proposed scheme based on combination. Xiao-qing and Tan [8] has suggested a threshold visual secret sharing schemes based on binary linear error correcting code. The author has mixed XOR and OR operation with reversing. VC-based repeating watermarking scheme is proposed by Wang, Tai, and Yu [9]. The authors add some parts of the watermark into edge blocks of the host image. It results in enhance robustness of the scheme. The limitation of the scheme is that the host image must be altered to embed a watermark.

Chang and Chuang [10] proposed a scheme based on torus automorphism and visual cryptography. Watermark is embedded without altering the host image. Lou, Shieh, and Tso [11] developed a copyright protection scheme based on chaos and VC techniques. The limitation of the scheme is that it does not provide the main characteristic of VC and uses the Human Visual System to decrypt secret messages. The watermark is retrieved by performing an XOR operation between the shadow images. In 2005 Hsu and Hou [12] proposed a copyright protection based on sampling distribution of means and Visual Cryptography to achieve the requirements of robustness and security. The secret message can be identified by the HVS directly without the aid of computers.

In this paper, we apply the concept of Singular Value Decomposition to embed a watermark into the cover image and to extract this watermark from the watermarked image. The watermark to be embedded is encrypted using visual cryptography. The watermark is first split into two shares. However, only the first share acts as a watermark while the second share acts as the secret key. Thus, the other share is the key to reconstruct the watermark. The visually crypted watermarks can be transmitted on the internet and the secret key share is hold by the copyright owner of watermarked image as the secret key. In this sense, it is very easy and fast to perform the image authenticate by just superimposing the key share over the decrypted watermark image. Since these two shares are mutually dependent, the watermark will not be revealed if one of these two shares is modified. The scheme is robust after several attacks are performed on the watermarked image. Section 2 gives preliminaries used for the proposed technique. Section 3 presents the technique for splitting a watermark using visual cryptography and embedding and extraction of the share. The experimental results and discussion is given in Section 4 followed by conclusion in Section 5.

2. Proposed Technique

The proposed technique is divided in two sections, embedding technique and the extraction technique as described below:

2.1 Embedding Technique

1. Apply 1-level DWT on the cover image. It gives four subbands LL, LH, HL, and HH. The HH subband is selected for the embedding of watermark as the high frequency coefficient changes are responsible for the changes in the edges only.
2. SVD is calculated for HH subband only. This will reduce the computational overhead as we are not considering the whole cover image.
   $CD1 = CU + CS + CV'$
3. The watermark is now encrypted to increase the security of the scheme. For this we applied the visual cryptography on the watermark. This will divide the watermark into two shares, viz., share 1 and share 2. The original watermark can be obtained if both the shares of the encrypted watermark are superimposed on each other. Hence we will use share1 of the watermark for the embedding purpose while share 2 of the watermark is provided as the secret key.
4. Apply SVD on the share1 of the watermark
   $W_{share1} = WU + WS + WV'$
5. Modify the singular values of the HH subband of cover image and apply inverse SVD.
   $W1 = CS + \alpha WS$
   Where, CS is the SV's of the cover image and WS are the SV's of the watermark. α is the embedding strength.

   $CD1' = CU + W1 + CV'$
6. Perform the inverse DWT by combining the subbands with the modified one to get the watermarked image.

The embedding technique is shown in following figure 1.

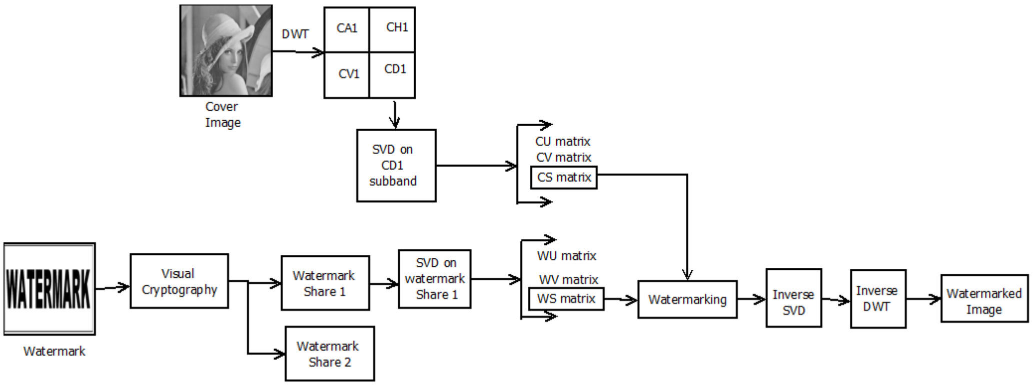


Figure 1. Embedding Technique

2.2 Extraction Technique

The extraction technique is exactly the reverse of the embedding technique.

1. Perform level-1 DWT on watermarked image.
2. Perform SVD on the HH subband.
3. Extract the singular values of the watermark.
   $WS_{extract} = (W1 - CS)/\propto$
4. Perform inverse SVD to get the share 1 of the decrypted watermark1 i.e. share 1 of the watermark.
5. Share 2 which acts as secret key is superimposed on the decrypted watermark share 1 to get the extracted watermark.

The extraction technique is shown in figure2.

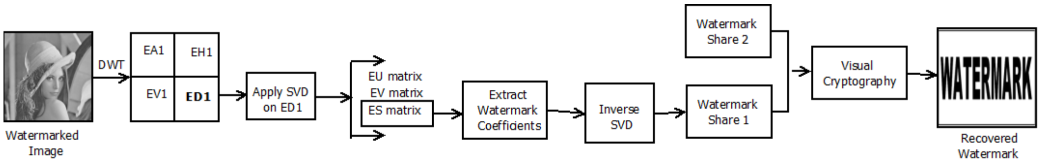


Figure 2. Extraction Technique

3. Experimental Results and Discussion

In order to authenticate the performance of the proposed technique, simulation is done on wide set of cover images and watermarks using MATLAB10. The cover image is of size 512X512 gray scale images as shown in figure 3 and watermark is of size 256X256 as shown in figure 4. As indicated in figure 4 the watermark is divided into two shares after applying visual cryptography. This is represented as visual crypt watermark 1 and 2 respectively. The decrypted watermark 1 is the share 1 of the watermark extracted from the watermarked images. This is combined with the visual crypt watermark 2 to get the extracted watermark.

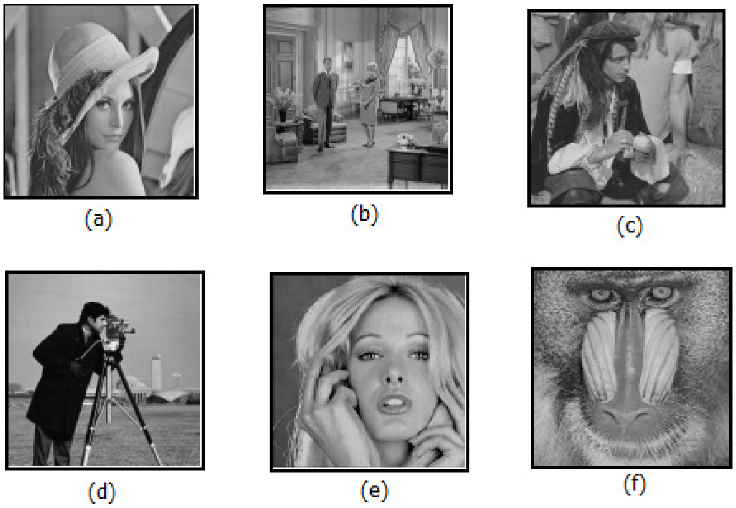
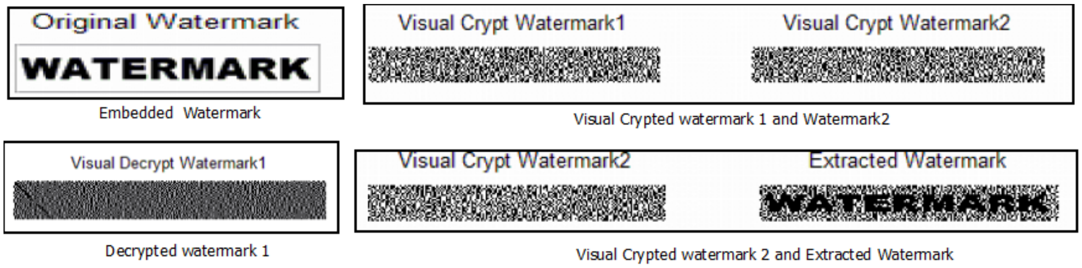


Figure 3. Cover Images (a) Lena (b) Living room (c) Pirate (d) Cameraman (e) Woman (f) Mandrill



Embedded Watermark

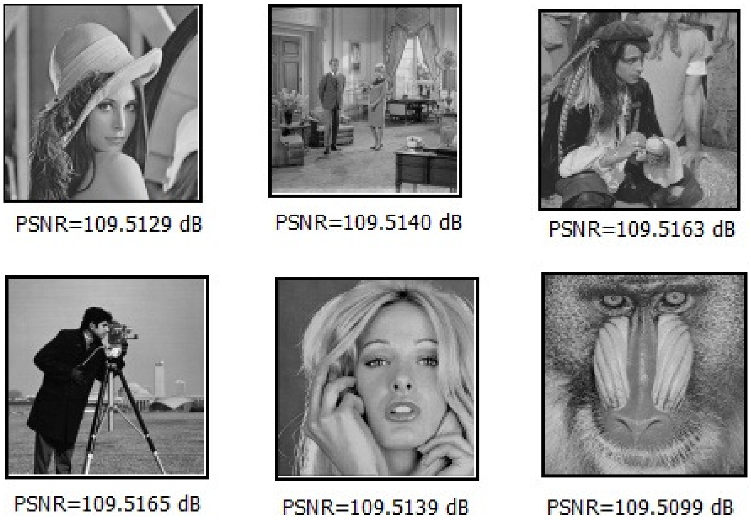
Visual Crypted watermark 1 and Watermark2

Decrypted watermark 1

Visual Crypted watermark 2 and Extracted Watermark

Figure 4. Embedded and Extracted Watermark

Figure 5 shows the PSNR obtained between cover image and watermarked image for all standard test images. The PSNR indicates that the imperceptibility of the watermarked image is good and the watermarked image is indistinguishable from the cover image.



PSNR=109.5129 dB

PSNR=109.5140 dB

PSNR=109.5163 dB

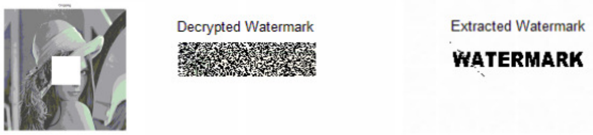
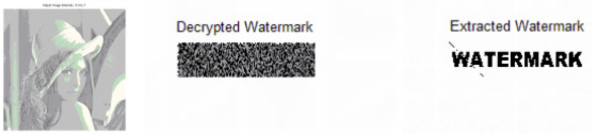
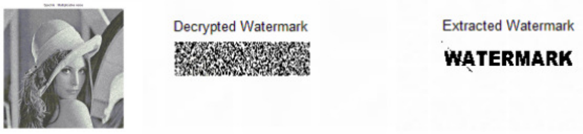
PSNR=109.5165 dB

PSNR=109.5139 dB

PSNR=109.5099 dB

Figure 5. Watermarked Images with PSNR

To check the robustness of our algorithm we applied a wide set of attacks on the test images. The effect of these attacks on the watermark images with corresponding extracted decrypted watermark and extracted watermark by combining the share 2 of the watermark is shown in following figure.

Cropping	
Image Intensity (0.4 to 1)	
Speckle Noise	

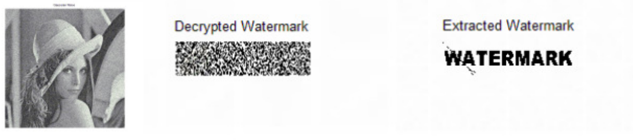
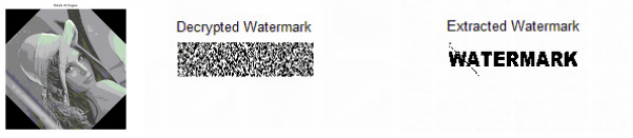
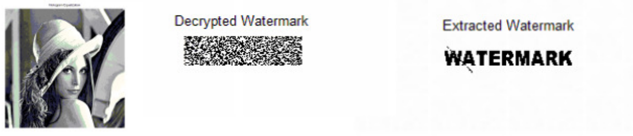
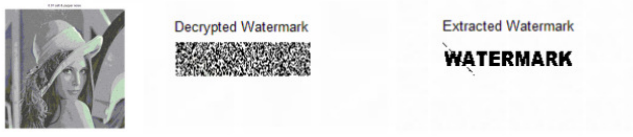
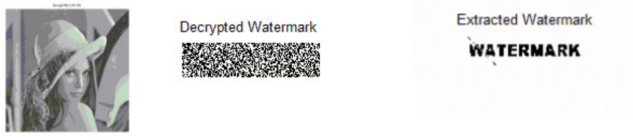
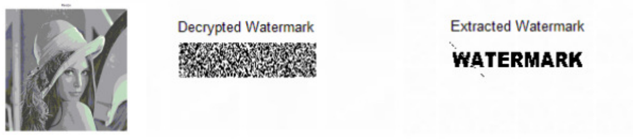
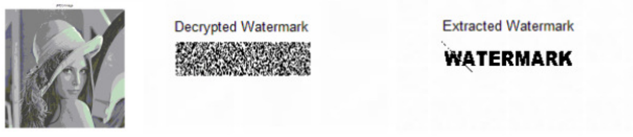
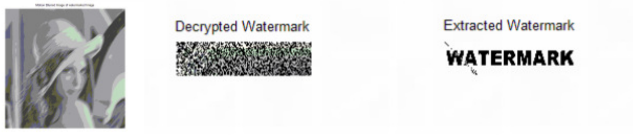
Gaussian Noise	
Rotation	
Histogram Equalization	
Salt & Paper Noise	
Gaussian Filter	
Resize	
JPEG	
Motion Blurred	

Figure 6. Analysis of attacks on Watermarked Images

The visual quality of the extracted watermark is good after applying the different attacks. This acceptable performance is measured with the help of normalized correlation measured between embedded and extracted watermark. Table 1 shows the normalized correlation values after applying different attacks on the watermarked images.

Table1. Normalized correlation between embedded and extracted watermark

Image Attacks	Lena	Living room	Pirate	Cameraman	woman	Mandrill
Cropping	0.9865	0.9833	0.9777	0.9865	0.9869	0.9914
Image Intensity	0.9872	0.9866	0.9859	0.9872	0.9909	0.9929
Speckle Noise	0.9924	0.9898	0.9885	0.9911	0.9894	0.9874
Gaussian Noise	0.9885	0.9885	0.9860	0.9885	0.9864	0.9859

Rotation	0.9872	0.9879	0.9809	0.9847	0.9834	0.9760
Histogram Equalization	0.9898	0.9841	0.9898	0.9879	0.9864	0.9874
Salt & Pepper Noise	0.9885	0.9853	0.9866	0.9879	0.9889	0.9884
Gaussian filter	0.9872	0.9878	0.9872	0.9866	0.9859	0.9909
Resize	0.9885	0.9872	0.9872	0.9885	0.9929	0.9934
JPEG	0.9898	0.9930	0.9917	0.9904	0.9904	0.9934
Motion Blurred	0.9815	0.8177	0.9838	0.9140	0.9864	0.8980

6. CONCLUSIONS

In this paper a new robust watermarking technique for copyright protection has been proposed. We applied the singular value decomposition along with the Discrete Wavelet Transform. Since the technique utilizes the properties of both DWT and SVD the proposed technique is more robust against different attacks. The innovation of this paper is that the security of the algorithm is increased with the help of visual cryptography on the watermark image. If the second share of the watermark which acts as the key is not present then it is not possible to extract the exact watermark information. It is very difficult to change or remove the watermark without knowing the secret key share as the watermark is split into two shares with random patterns. The robustness of the technique is justified by giving analysis of the effect of attacks and still we are able to get good visual quality of the embedded watermark.

REFERENCES

[1] R. Sun, H. Sun, and T. Yao, “A SVD and quantization based semifragile watermarking technique for image authentication,” in Proc.Int. Conf. Signal Process., pp. 1592–1595, (2002)

[2] C. C. Chang, P. Y. Tsai, and M. H. Lin, “SVD-based digital image watermarking scheme,” Pattern Recogn. Lett. 26, 1577–1586, (2005).

[3] J. M. Shieh, D. C. Lou, and M. C. Chang, “A semi-blind digital watermarking scheme based on singular value decomposition,” Comput. Stand. Inter. 28, 428–440, (2006).

[4] R. Liu and T. Tan, “An SVD-based watermarking scheme for protecting rightful ownership,” IEEE Trans. Multimedia 4, 121–128, (2002).

[5] Moni Naor and Adi Shamir, “Visual Cryptography”, advances in cryptology– Eurocrypt, pp 1-12, (1995).

[6] Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin , “Sharing A Secret Two-Tone Image In Two Gray-Level Images”, Proceedings of the 11th International Conference on Parallel and Distributed Systems , ICPADS'05, (2005).

[7] Liguo Fang, BinYu, “Research On Pixel Expansion Of (2,n) Visual Threshold Scheme”, 1st International Symposium on Pervasive Computing and Applications, pp 856-860, (2006)

[8] Xiao-qing Tan, “Two Kinds Of Ideal Contrast Visual Cryptography Schemes”, International Conference on Signal Processing Systems, pp. 450-453,(2009)

[9] C. C. Wang, S. C. Tai, and C. S. Yu, “Repeating image watermarking technique by the visual cryptography,” IEICE Trans. Fundamentals E83-A_8_, 1589–1598, (2000).

[10] C. C. Chang and J. C. Chuang, “An image intellectual property protection scheme for gray-level images using visual secret sharing strategy,” Pattern Recogn. Lett. 23, 931–941, (2002).

[11] D. C. Lou, J. M. Shieh, and H. K. Tso, “Copyright protection scheme based on chaos and secret sharing techniques,” Opt. Eng. 44_11_, 117004, (2005).

[12] C. S. Hsu and Y. C. Hou, “Copyright protection scheme for digital images using visual cryptography and sampling methods,” Opt. Eng.44_7_, 077003, (2005).

Authors

Sushila Kamble received B.E. in Computer Technology from MIET Gondia, Maharashtra, India in 2003, M. Tech in Computer Science & Engineering from SATI Vidisha, MP, India in 2007 and presently pursuing Ph.D from Motilal Nehru National Institute of Technology, Allahabad, UP, India. She is having 4 years of teaching experience. Her current research interest includes Digital watermarking, Pattern Recognition, Computer Vision, Algorithms, Compression, Biometrics, Face recognition.

Vikas Maheshkar received B.E. in Computer Technology from MIET Gondia, Maharashtra, India in 2002, M. Tech in Computer Science & Engineering from SATI Vidisha, MP, India in 2007 and presently pursuing Ph.D from Motilal Nehru National Institute of Technology, Allahabad, UP, India. He is having 7 years of teaching experience. His current research interest includes Pattern Recognition, Computer Vision, Algorithms, Compression, Biometrics, Face recognition, Digital watermarking.

Suneeta Agarwal received B. Sc degree in 1973 from university of Allahabad, M.Sc degree in 1975 from university of Allahabad, Ph. D in 1980 from IIT Kanpur and M. Tech degree in 2007 from AAIDU. She is having 31 years of Teaching Experience and currently professor in the Computer Science and Engineering Department, Motilal Nehru National Institute of Technology, Allahabad. Her current research interest includes Pattern Recognition, Computer Vision, Theory of Computation Science, Algorithms, Automata Theory, Compression, Patten matching, Finger print recognition.

Vinay Kumar Srivastava received the BE in ETC from GEC Rewa, MP, India in 1989, the M Tech in Communication from IT-BHU, Varanasi, India in 1991 and PhD in Electrical Engineering from IIT Kanpur, India in 2001. Presently he is a Professor in the department of ECE, MNNIT, Allahabad, India. He has about 18 years of teaching and research experience in the area of signal and image processing. He has chaired many sessions in conferences. He has authored or coauthored around 20 publications. His current research interest includes image compression, digital watermarking, stability 2D PSV system, DSP methods for identification of protein-coding regions, design and analysis of IDMA systems.