Secured Data Hiding Technique: Dual Watermarking

Lekhashri H. Mahajan
Department of Electronics & Telecommunication Engineering,
R. C. Patel Institute of Technology,
Shirpur, Maharashtra, India

Shailaja A. Patil
Department of Electronics & Telecommunication Engineering,
R. C. Patel Institute of Technology,
Shirpur, Maharashtra, India

ABSTRACT

Watermarking is a major technology to achieve copyright protection. The combinations of different mathematical tools such as Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) are used to embed watermark in the host image. In this dual watermarking scheme, to improve the robustness and protection of an image, number of watermarks embedded in the host image are two. These watermarks are known as primary and secondary watermark. The host image contains primary and secondary watermarks, in which secondary is embedded into primary and the resultant image is used as watermark for the host image. In this scheme, the images which are used as a watermark are visible gray scale images.

General Terms:

Attacks, Authentication, Watermarking.

Keywords:

Correlation Coefficient, Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD).

1. INTRODUCTION

Watermarking is a technique for inserting information (the watermark) into an image, which can be later extracted or detected for variety of purposes [1, 2, 4, 5, 10]. Watermarking is very important for copyright protection which is applied to various objects like bills, papers, garment labels, product packing. Watermarking serve for many purposes like copyright protection, broadcast monitoring and data authentication [7, 8, 10]. There are so many different watermarking algorithms have been proposed in the literature. Mainly, there are two categories of watermarking technique, spatial domain and transform or frequency domain [7, 8, 10, and 11]. Watermarking in transform domain is more robust and secure to different attacks as compared to spatial domain [3, 6, 10]. The combination of DWT and SVD are used to achieve high robustness against attacks like compression, cropping, rotation, resizing etc [8, 10, and 11].
The watermark is hidden from view during normal use, only become visible by adopting a special viewing process. e.g. Hold the bill up to light. The watermark carries information about the object in which it is hidden [12, 13, 14]. e.g. Authenticity of the bill, the trademark of the paper manufacturer. Watermarking can also be applied to digital signals. A watermark may be fragile, semi- fragile, robust. The requirements for watermarking are transparency, capacity and robustness. Figure 1 shows the procedure for watermarking [9].

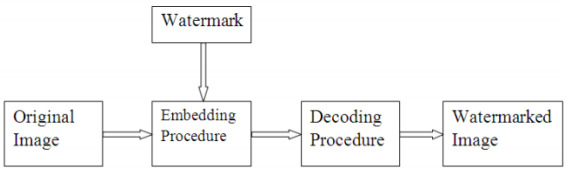

Fig. 1. Watermarking Procedure

The procedure of embedding and retrieval of watermark from watermarked image is shown. Take the original image on which watermark should apply and then use some appropriate watermark embedding technique using which watermark can safely apply on original image[22, 23]. After that the decoding procedure at the other end, in which using some decoding algorithm on that image the watermarked can easily obtain. Meanwhile some attack may apply on watermarked image by some unknown party. So choose such watermark embedding technique which is robust to such attacks[15, 16, 17, 18].

2. DISCRETE WAVELET TRANSFORM (DWT)

DWT is a multiresolution decomposition of a signal[19, 20, 21]. DWT uses filer banks for the construction of the multiresolution time frequency plane. The DWT uses multiresolution filter banks and special wavelet filters for the analysis and reconstruction of signals. Wavelets are also playing a significant role in many image processing applications. The 2-D wavelet decomposition of an image is performed by applying the 1-D DWT along the rows of the image first and then the results are decomposed along the columns. The following figure shows the image and its subband in DWT domain. This operation results in four decomposed sub band images such as Low-Low (LL), Low-High (LH), High-Low (HL), and High-High (HH). The frequency components of those sub bands cover the full frequency spectrum of the original image.

3. SINGULAR VALUE DECOMPOSITION (SVD)

SVD is one of the most powerful numeric analysis techniques with various applications including watermarking [17, 20, 21]. SVD is a linear algebra technique used to solve many mathematical problems. Decompose a matrix that is not symmetric by considering a

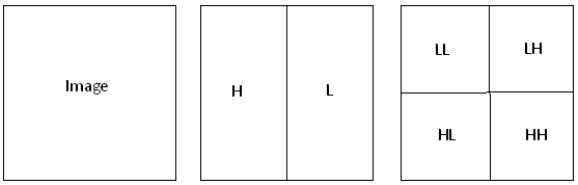

Fig. 2. DWT Transform

matrix A which is of dimension $m \times n$ where $m \geq n$. The vectors in the expansion of a are the eigen vectors of the square matrices AA^T and A^TA. The singular values are non zero square roots of the square matrices AA^T and A^TA. The singular value decomposition of A is given by,

$$A = USV^T \tag{1}$$

Where U is an $m \times m$ real or complex unitary matrix and (the conjugate transpose of V) is an $n \times n$ real or complex unitary matrix such that,

$$U \times U^T = I \tag{2}$$

$$V \times V^T = I \tag{3}$$

Where, I represents an Identity matrix and S is the diagonal matrix of order $m \times n$ having elements $S1, S2, S3, ..., Sn$.

Where,

$$S1 > S2 > ... > Sn \tag{4}$$

The singular values of A are represented by the diagonal elements of S. The columns of U matrix are known as the left singular values of A and the columns of V are known as the right singular values of A. Such a factorization is called the singular value decomposition of A.

4. DUAL WATERMARKING SCHEME

In this watermarking scheme, the watermarks embedded in the host image are two. These watermarks are known as primary and secondary watermark. The host image contains primary and secondary watermarks, in which secondary is embedded into primary and the resultant image is used as watermark for the host image. This watermarking scheme is for gray scale digital images. The secondary watermark is embedded into primary watermark and the resultant watermark image is used as watermark for the host image. Secondary watermark is easy to detect but primary is harder sometimes. To improve the robustness of the scheme, dual watermarking is used.

4.1 Watermark Embedding for Dual watermarking scheme

Firstly, secondary watermark image is embedded in the primary watermark image by using following algorithm.

4.1.1 Embedding Secondary Watermark for Dual Watermarking

(1) Perform 1-level wavelet transform on the primary watermark.
(2) Perform SVD transform on secondary watermark.
(3) Perform SVD transform on all parts.
(4) Modify the singular values of all parts with the singular values of the another watermark i.e. secondary watermark.
(5) Obtain all modified approximation and all the detail parts of an image.
(6) Perform 1-level inverse DWT to get the watermarked primary watermark.

4.1.2 Embedding Primary Watermark for Dual Watermarking. The host image contains primary and secondary watermarks, in which secondary is embedded into primary and the resultant image is used as watermark for the host image and the embedding algorithm of which is as follows.

(1) Perform 1-level wavelet transform on the host image.
(2) The sub-images of the host image is segmented into non overlapping rectangles using ZIG-ZAG sequence.
(3) Perform SVD transform on new primary watermark.
(4) Perform SVD transform on each and every non overlapping rectangles.
(5) Modify the singular values of each and every non overlapping rectangles with the singular values of the new primary watermark.
(6) Obtain all modifies non overlapping rectangles.
(7) After embedding the watermark, reconstruct approximation and each and every detail parts.
(8) Perform single level inverse discrete wavelet transform to obtain watermarked image.

4.2 Watermark Extraction for Dual Watermarking

For watermark extraction from watermarked image, both watermark and host images are needed. The extraction process is as follows.

4.2.1 Extracting Primary Watermark for Dual Watermarking

(1) Perform single level wavelet transform on the host and watermarked image.
(2) The sub-images of the host and watermarked image is segmented into non-overlapping rectangles for which ZIG-ZAG sequence is used.
(3) Perform SVD transform on each and every non-overlapping rectangles of both the images.
(4) singular values of primary watermark are extracted from all non-overlapping rectangles.
(5) Obtain all estimate of primary watermark.
(6) Select the primary watermark which has the greatest correlation coefficient.

4.2.2 Extracting Secondary Watermark for Dual Watermarking

(1) In this section, we have to extract secondary watermark from the image which we got from previous section.
(2) Perform 1-level wavelet transform on the primary watermark.
(3) Perform SVD transform on approximation and each and every detail parts of both images.
(4) Extract singular values of secondary watermark from approximation and all detail parts.
(5) Obtain all estimate of secondary watermark.
(6) Sum up all these after detecting all estimate of secondary watermark.

In this watermarking scheme, we have taken gray scale Lena image of size 512 X 512 and for primary and secondary watermark we have taken 8 bit gray scale image and logo image of sizes 128 X 128 and 64 X 64 respectively.

5. RESULTS

To check the similarity between embedded watermark and extracted watermark, correlation coefficient is given by,

$$NC = \frac{\sum_{Y=1}^{M}\sum_{X=1}^{N}[I(X,Y)I^{'}(X,Y)]}{\sum_{Y=1}^{M}\sum_{X=1}^{N}[I(X,Y)]^2} \quad (5)$$

Where $I(i,j)$ is the original image and $I'(i,j)$ is the modified image. X is the height and Y is the width of the image. The value of NC is lies between 1 and -1. If the value of NC is equal to 1 then extracted logo is just equal to original one. The correlation coefficient of extracted primary and secondary watermarks is given in table 1.

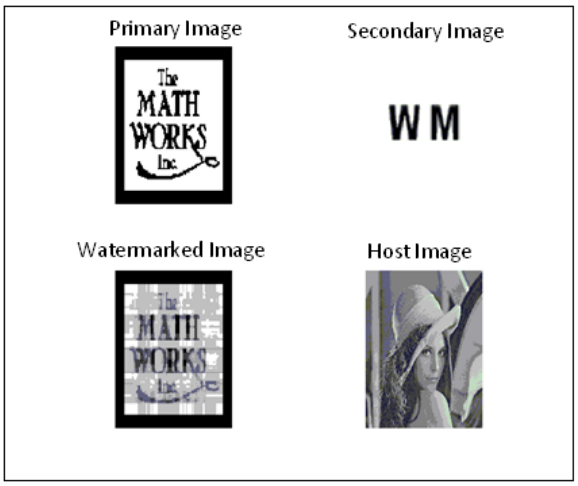

Fig. 3. Dual level watermark Embedding

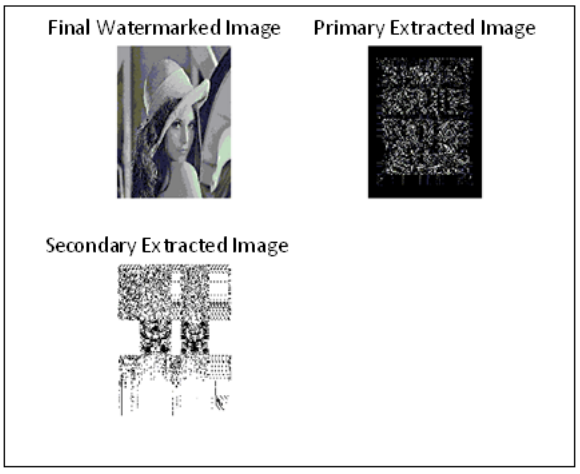

Fig. 4. Dual level watermark Extraction

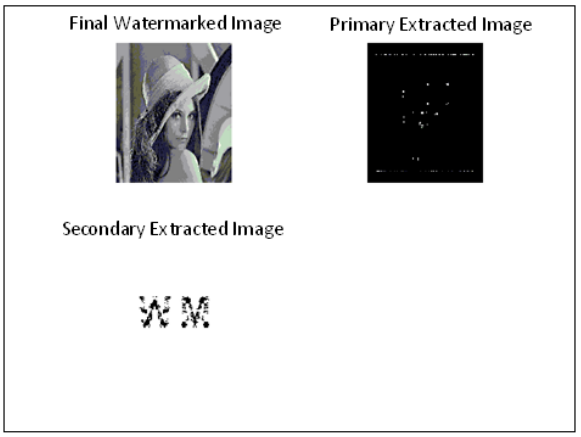

Fig. 5. Extracted logo after applying Salt and Pepper noise attack

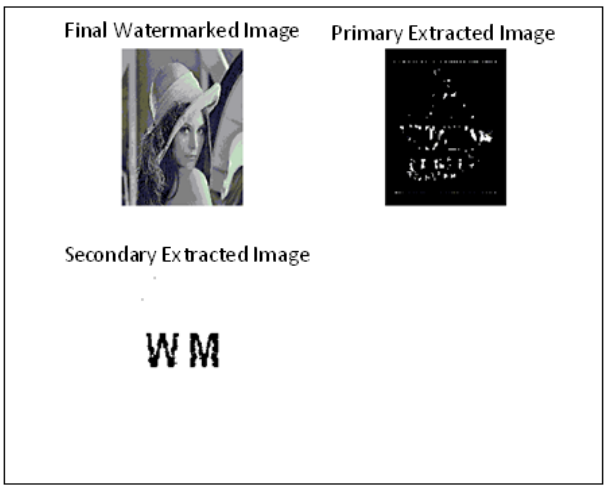

Fig. 6. Extracted logo after applying cropping attack

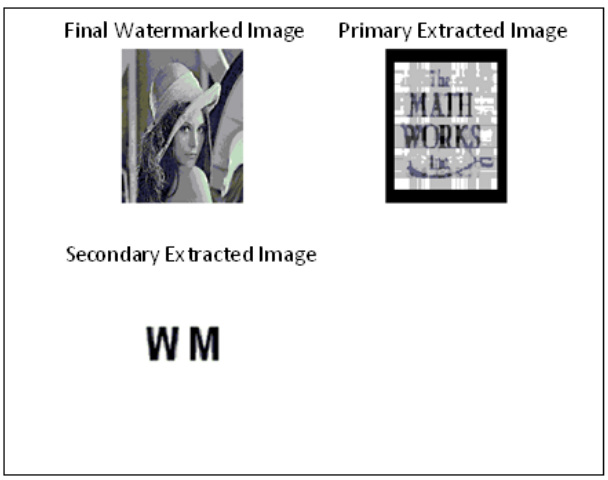

Fig. 7. Extracted logo after applying resizing attack

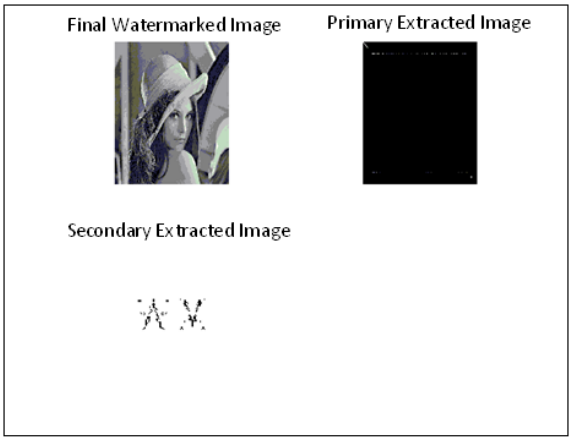

Fig. 8. Extracted logo after applying rotating attack

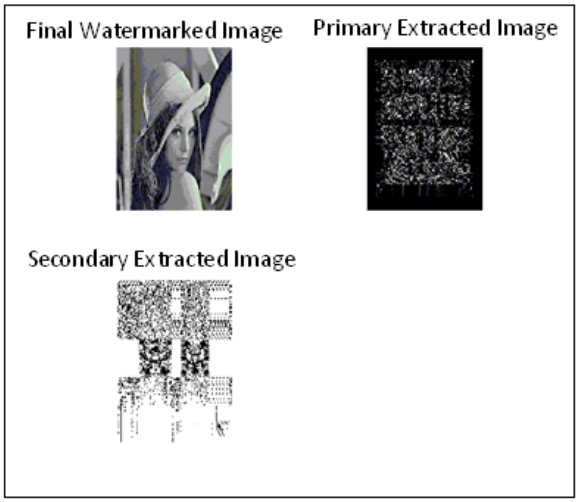

Fig. 9. Extracted logo after applying Median Filtering attack

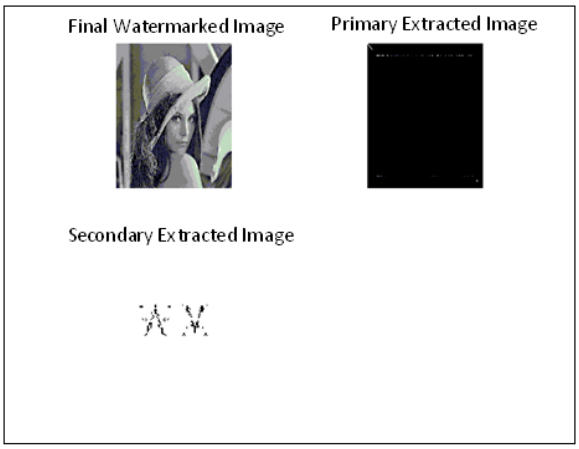

Fig. 10. Extracted logo after applying compression attack

Correlation Coefficient		
Attacks	Dual Level Watermarking	
	Primary	Secondary
Before Attacking	0.9407	1
Salt and Pepper	-0.9892	0.8018
Cropping	-0.6634	0.8321
Compression	-0.0240	0.3163
Resizing	0.9407	1
Rotate	-0.6278	0.9318
Median Filtering	-0.1646	0.2613

Table 1 Correlation coefficient between embedded and extracted watermarks of single level and dual level watermarking schemes.

6. CONCLUSION

This dual watermarking scheme is very useful to establish ownership of an image. Both images are used gray scale images. In this scheme, visible watermarking is used for embedding watermark in the host image. DWT-SVD have been used for the protection and robustness of an image which is used as a mathematical tool to image the data in the host image. The secondary watermark is easy to detect and extract form the host image in all cases. Both watermarks used are invisible.

7. REFERENCES

[1] R. Schyndel, A. Tirkel and C. Osborne, “A Digital Watermark”, Proceedings of International Conference on Image Processing, IEEE, Vol. 02, pp. 86-90, 1994.

[2] B. M. Macq and J. J. Quisquater, “Cryptology for digital TV broadcasting, Proceedings IEEE, Vol. 83, pp. 944-957, 1995.

[3] G. B. Rhoads, “Identification/authentication coding method and apparatus”, Word Intellectual Property Organization, WIPO, 1995.

[4] Bender et. al, “Techniques for data hiding”, IBM systems Journal, Vol. 35, pp. 313-336, 1996.

[5] J. Ruanaidh, W. J. Dowling and F. M. Bolad, “Watermarking digital Images for copyright protection”, Image Processing, Proceedings of International Conference on Digital Object Identifier, pp. 239-242. 1996.

[6] M. Swanson, B. Zhu and A. Tewfik, “Transparent Robust Image Watermarking”, Proceedings of International Conference on Image Processing, IEEE, Vol. 03, pp. 211-214, 1996.

[7] I. Pitas, “A Method for Signature Casting on Digital Images, International Conference on Image Processing, Vol. 3, pp. 215-218. September 1996.

[8] I. Cox, J. Kilian, F. Leighton and T. Shamoon,“Secure Spread Spectrum Watermarking for Multimedia”, IEEE Transactions on Image Processing, Vol. 06, pp. 1673-1687, 1997.

[9] X. Xia, C. Boncelet, and G. Arce, “A Multiresolution Watermark for Digital Images”, Proceedings of International Conference on Image Processing, IEEE, Vol. 01, pp. 548-551, 1997.

[10] D. Kundur and D. Hatzinakos, “A Robust Digital Image Watermarking Method Using Wavelet based Fusion”, Proceedings of International Conference on Image Processing, IEEE, Vol. 01, pp. 544-547, 1997.

[11] F. Bartolini, M. Barni, V. Cappellini and A. Piva, “Mask Building for Perceptually Hiding Frequency Embedded Wa-

termarks", Proceedings of International Conference on Image Processing, IEEE, Vol. 01, pp. 450-454, 1998.

[12] L. Marvel, C. Retter, and C. Boncelet, "Hiding Information in Images", Proceedings of International Conference on Image Processing, IEEE, Vol. 02, pp. 396-398, 1998.

[13] V. S. Craver, N. Memon, B. Yeo, and M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications", IEEE Journal on Selected Areas in Communications, Vol. 16, pp. 573-586, 1999.

[14] M. Ramkumar and A. N. Akansu, "A robust data hiding scheme for image using DFT", Proc. International Conference on Image Processing, Vol. 02, pp. 211-215, 1999.

[15] M. Barni, F. Bartolini, A. De Rosa and A. Pivai, "Optimum Decoding and Detection of Multiplicative Watermarks", IEEE transactions, pp. 1118-1123, 2003.

[16] G. Bhatnagar, B. Raman and K. Swaminathan, "DWT-SVD based Dual Watermarking Scheme", Proc. IEEE, Vol. 01, 2008.

[17] B. Jagadeesh, S. Srinivas Kumar and K. Raja Rajeswari, "A Genetic Algorithm Based Oblivious Image Watermarking Scheme using Singular Value Decomposition (SVD)", 2009.

[18] Lintao Lv, Liang Hao ad Hui Lv, "Resisting RST Watermarking Algorithm for Image Content Authentication", pp. 5-10, 2010.

[19] B. Jagadeesh, S. Srinivas Kumar and K. Raja Rajeswari, "Image Watermarking Scheme Using Singular Value Decomposition, Quantization and Genetic Algorithm", Vol. 03, pp. 7-10, 2010.

[20] N. V. Dharwadkar, B. B. Amberker and A.Gorai, "Non-blind Watermarking scheme for color images in RGB space using DWT-SVD", Proceedings IEEE, Vol. 04, November 2011.

[21] S. kumar, A. kumar saini and P. kumar, "SVD based Robust image digital watermarking using DWT", IEEE, Vol. 45, 2012.

[22] J. Delaigle, C. De Vleeschouwer and B. Macq, "Psychovisual Approach to Digital Picture Watermarking", Journal of Electronic Imaging, Vol. 7, pp. 628-640, 1998.

[23] P. Bas, J. Chassery and F. Davoine, "Using the Fractal Code to Watermark Images", Proceedings of IEEE International Conference on Image Processing, Vol. 01, pp. 469-473, 1998.

[24] www.mathworks.com