International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Authentication of Meddle watermarks with Revocable Data Hiding and Retrieving for RGB Color Images

K.SOWJANYA

Asst.Professor Department of ECE Anubose Institue of Technology,

K.S.P Road,New Paloncha,Khammam(Dist),Telangana,India-507115

sowjanya.kavuturu@gmail.com

Abstract

In this paper, a Revocable watermark is used for meddle watermarks for color images . A Revocable watermark is embedded in to robust watermark in the discrete wavelet transform (DWT) domain using feature map and location map. Generally, the robust watermark is used to verify the owner ship, but if the robust watermark is tampered or faked by the malicious attacker, then it cannot prove the ownership when it is extracted from the original image.. In this, we focus on authentication and reversibility of the robust watermark because the purpose of Revocable data embedding is to authenticate the robust water mark. This technique provides not only the authentication of robust watermark but also restoration, when Revocable data is exactly extracted bit by bit.

I. INTRODUCTION

With the result of advancement in today's technology, digital content can be easily copied, manipulated and distributed. Copy right protection and content authentication of digital content has become an urgent problem to content owner ship and distributors. Digital watermarking has provided a valuable solution to this problem. In recent years digital watermarking has become a very active research field and been widely accepted as a promising technique for multimedia security .Generally digital watermarking is divided in to two categories: robust watermarking and fragile watermarking. As a special subset of fragile watermark, Revocable watermark (which is also called lossless watermark) enables the recovery of the original, unwatermarked content after watermark content has been detected to be authentic. If an embedded watermark is tampered or faked by
malicious attacker, an extracted watermark is not enough to verify the owner ship.

The Revocable watermark is used to confirm authenticity of a digital content. In this paper a Revocable watermark is embedded in to the robust watermark for the purpose of ownership proof.
With Revocable data embedding, one can restore the original robust watermark after it is authenticated. Digital rights management (DRM) systems are built from several components that allow setting efficient electronic commerce of intangible goods [1].

Watermarking is the core technology and it is most closely associated with DRM [2].Fragile watermarks can be used to confirm authenticity of a digital content [4]. They can also be used in applications where it is important to figure out how the digital content was modified or which portion of it has been tampered with. Semi-fragile watermarks [5] are designed to survive standard transformations, such as lossy compression, but they will become invalid if a major change [6] occurs.

The paper organized as follows: in the section 2 follows about Revocable watermarking and old methods for watermarking techniques. In section3 about DWT(Discrete Wave Let Transform) .In section4 presents embedding and verification methods, using the DWT domain. In section 5 simulation results are given. In section 6 conclusion is given.

II. WHAT IS REVOCABLE WATERMARKING

Revocable watermarking (lossless or invertible watermarking) enables us to recover the image which is same as the original image pixel by pixel after the content is authenticated. This type of lossless recovery is compulsory in sensitive imagery applications like medical and military purposes because every bit of information is important

The motivation of Revocable watermark is distortion-free data embedding [7, 8, 9, and 10]. In sensitive images such as military and medical images, Revocable data embedding provides the original data when the digital content is authenticated.

Revocable watermark is a special subset of fragile watermark [11].Like fragile watermarks; it can be used for digital content authentication. But Revocable watermark is much more than content authentication. It has an additional

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

advantage that when watermarked content has been detected to be authentic, one can remove the Revocable data to retrieve the original robust watermark

A. Ownership Verification

Image authentication is one of the application fields of digital watermarking, which allows us to recognize manipulations in images.Robust watermarks are designed to resist against heterogeneous manipulations. This type of watermark is used in the applications having presupposing security of the watermarking systems. Fragile watermarks are embedded with very low robustness. Therefore, this type of watermark can be destroyed even by the slightest manipulations. In this sense they are comparable to the hidden messages in steganographic methods. They can be used to check the integrity of objects.

When the robust watermark is tampered by malicious attacker then the Revocable watermark can be used to prove the ownership .i.e. whether the robust watermark modified or not. The conventional cryptography cannot prove the ownership shown in fig 1. Because even one bit is changed, the watermark cannot be decrypted. Therefore the Revocable watermark exactly extracted from robust watermark is not only the authentication of the robust watermark but also restoration of the original robust watermark after it is authenticated.

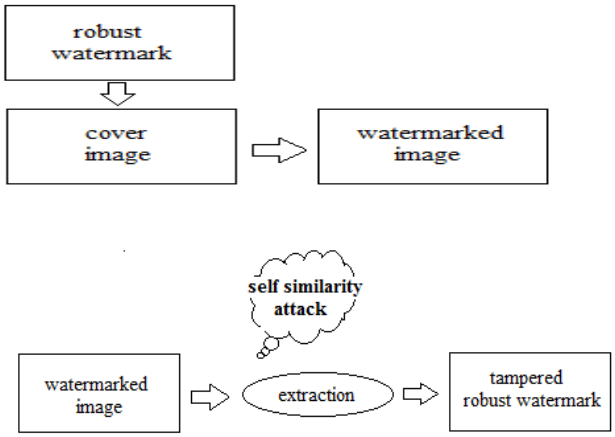

Figure 1.Shows general watermarking technique

In addition, Revocable data embedding provides high capacity data embedding without increasing the storage space of the digital content [10].

III.THE DISCRETE WAVELET TRANSFORM

In this section, it is an authentication technique in the DWT domain for meddle watermarks of still images like JPEG-2000.The standardization of this image is used in the wavelet transform domain. The advantages of watermarking techniques in the wavelet transform domain are an inherent robustness of the scheme to the JPEG-2000 lossy compression and the possibility of minimizing computation time by embedding watermarks inside of a JPEG-2000 encoder.

Compared to other transform domains, the DWT domain has many advantages. The wavelet functions have better space frequency localization characteristic, thus they provide the capability to localize information both in space and frequency, which makes the wavelet based methods more robust against geometric attacks such as cropping and scaling.

The DWT decomposes a digital signal into different sub bands (LL, LH, HL, and HH), so that the lower frequency sub bands have finer frequency resolution and coarser time resolution compared to the higher frequency sub bands.

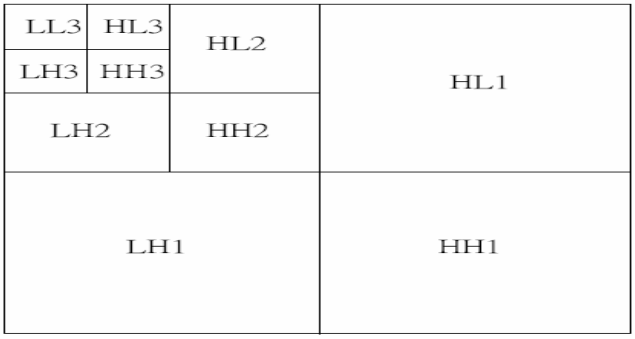

Figure 2.Shows illustration of Wavelet Decomposition

The DWT is being increasingly used for image compression due to the fact that the DWT supports features like progressive image transmission (by quality, by resolution), ease of compressed image manipulation] region of interest coding, etc. Because of these characteristics, the DWT is the basis of the new JPEG2000 image compression standard .Also they are hierarchical and suitable for the human visual system (HVS). Similarly, the inverse DWT is applied which is just opposite to the forward DWT to get back the reconstructed image.

The idea of meddle watermarking is shown in fig.3

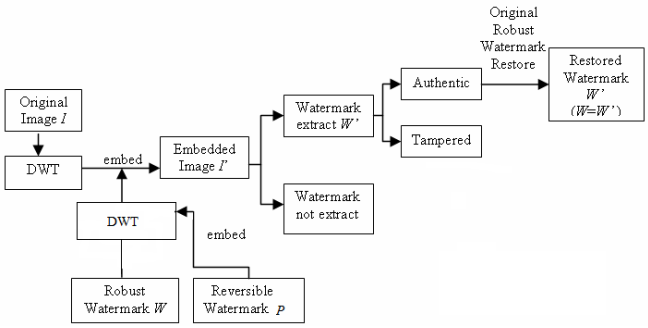

Figure 3. A block diagram for meddle watermarking

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IV.MEDDLE WATERMARKS WITH EMBEDDED REVOCABLE DATA FOR COLOR IMAGES

A. Feature Map Generation

The reason to generate the feature map from the image is in order to make watermarks based on contextual information. it is generated at LL4 band after a 4-level wavelet transform by taking the difference between a coefficient of the LL4 band. The feature map is constructed as' 1'and' 0'. If the difference between a coefficient and a neighboring is positive, the value of corresponding position for feature map is recorded to '1' otherwise'0'.

$$C_{41}(m,n) > C_{41}(m,n+1) : '1'$$
$$C_{41}(m,n) < C_{41}(m,n+1) : '0' \quad (1)$$

' C 'is the coefficient of wavelet transform, the first index subscript '4' means a 4-level wavelet transform and the second index subscript '1' means LL band. (m, n) is the location of the coefficient

B. Location Map Generation

The location map is generated from the coefficients of the robust watermark to embed the Revocable watermark in to robust watermark the LSB bit of coefficient made '0' then in that LSB bit it is embedded. It is important to identify the location of '1ible watermark ' value of the LSB.Since '1' is changed to '0' before the Revocable watermark is embedded. Because the value'1'is removed

C. Coefficient Adjustment at Level 3 and Level 2

In frequency-domain watermarking, if the robust watermark is inserted into the low-frequency sub bands, the image quality is largely impaired. On the other hand, if the robust watermark is inserted into the high-frequency sub bands, the robust watermark can be removed by image compression. Therefore, the robust watermark is usually inserted into the mid-frequency sub bands.

The robust watermark is embedded in to 3-level wavelet transform. The wavelet coefficients are adjusted according to the corresponding bit value of the robust watermark. if the robust watermark bit is '1',we adjust the coefficient value of LH3 to larger than that of HL3.otherwise we adjust the coefficient value of HL3 vice versa.

$$'1': C_{32}(m,n) > C_{33}(m,n)$$
$$'0': C_{32}(m,n) < C_{33}(m,n) \quad (2)$$

If the difference 'd' between the coefficients LH3 and HL3 is less than 't' ,it is adjusted at least to that extent 't' .if the t value larger makes the watermark stranger. But it increases degradation of the image. So the 't' value adjusted to match the purpose our application.

$$d < t \Rightarrow C_{32}(m,n) = C_{32}(m,n) + d + t : '1'$$
$$C_{33}(m,n) = C_{33}(m,n) + d + t : '0' \quad (3)$$

The above procedure will be implemented for adjusting the coefficients in 2-level wavelet domain for embedding of location map.

D. Watermark Embedding Procedure

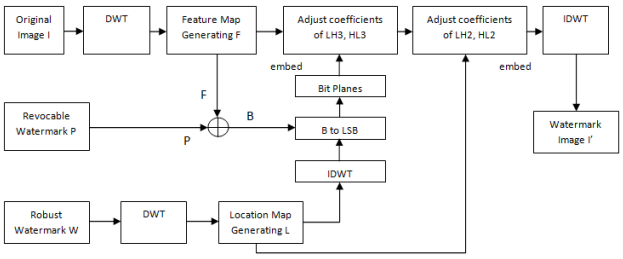

Figure 4.A block diagram for Watermark Embedding

E. Watermark Verification Procedure

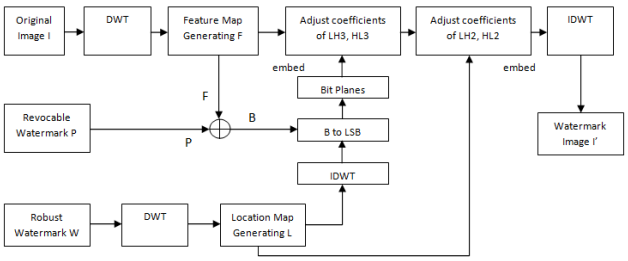

Figure 5.A block diagram for Watermark Verification

V. EXPERIMENTAL DISCUSSIONS

Here the proposed method can be applied to different test images like" leaf", "Lena", "pepper" and "lake". Here the test image is "Lena" shown in fig 6.The test image is "Lena" of size 512x512(256 grayscale levels per pixel).the robust watermark size is 64x64(256 grayscale levels per pixel) and the Revocable watermark is a binary logo and its size is 32x32.

5.1. Experimental Results

In the Fig .6 shows the cover image ,Fig.7(a) shows the Robust watermark and (b) shows the Revocable watermark. Fig. 8 Shows watermarked image and its PSNR is 36.67dB. Fig 9(b) shows the extracted Robust watermark from the watermarked image and the Revocable watermark shows in (a) has authentic result. Fig.10 shows the attacked watermarked image by malicious-attacker.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

The attack on the watermarked image is a geometrical[14] attack which is a self similarity attack[13]. In this the right side eye is replaced with left side eye Fig. 11(a) shows the extracted Revocable watermark from the tampered robust watermark and location of tampered area. Fig 10(b) shows the tampered robust watermark. In Revocable watermarking because both the payload and original information are embedded into the image, an embedder has to consider the embedding capacity. In the previous methods [5, 10], a compression or expansion for capacity is generally used for Revocable data embedding. In this proposed algorithm, the location map for the restore to the original is not embedded into the robust watermark but embedded into the original image. Therefore our algorithm has efficiency for the capacity

Figure6. Test image

Figure 7. (a) Robust Watermark (b)Revocable watermark

Figure 8. watermarked image

Figure 9. (a) Recovered Revocable watermark is Authentic (b) Restored Robust Watermark

Figure 10. self-similarity attack watermarked image

Figure 11. (a) Non authentic Revocable Watermark (b)Tampered Robust Watermark

VI .CONCLUSION

In this paper, a Revocable data embedded for meddle watermarks for color images is used. The Revocable watermark is embedded into the robust watermark in wavelet domain using the feature map and the location map. Though the robust watermark is extracted exactly from watermarked image, if it is tampered or faked by malicious attacker, then it cannot exactly verify the ownership. By using Revocable watermark we can verify the ownership and also using Revocable watermark which is embedded into the robust watermark for the restoration of original robust watermark . For the future work, we will concentrate in various multimedia applications using this.

REFERENCES

[1] W. Rosenblatt, W. Trippe, and S. Mooney, Digital Rights Management, New York, 2002.

[2] E. T. Lin, A. M. Eskicioglu, and R. L. Lagendijk,"Advances in Digital Video Content Protection, "Proceedings of the IEEE vol. 93, issue 1 pp. 171-183, Jan. 2005.

[3] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia,"IEEE Trans. Image Process., vol. 6, pp. 1673-1687, Dec.1997.

[4] P. W. Wong, "A watermark for image integrity and ownership verification," Proceedings of IEEE Int. Conf.Image Processing, pp. 455-459, 1998.

[5] M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp,"Hierarchical watermarking for secure image authentication with localization," IEEE Trans. Image Processing, vol. 11, No. 6, pp. 585- 595, 2002.

[6] Cox, I. J., Miller, M. L., and Bloom, J.A.: Digital Watermarking, Morgan Kaufmann, San Francisco, 2001.

[7] M. J. Gormish, E. L. Schwartz, A. Keith, M. Boliek, and A. Zandi, "Lossless and nearly lossless compression for high quality images, "Proceedings of SPIE, vol. 3025, pp. 62-70, 1997.

[8] M. Goljan, J. Fridrich, and R. Du, "Distortion-free data embedding for images," in 4th Information Hiding Workshop, pp. 27-41, Apr. 2001.

[9] C. W. Honsinger, P. W. jones, M. Rabbani, and J. C.Stoffel, "Lossless recovery of an original image containing embedded data," United States patent,6,278,791, 2001.

[10] J. Tian, "Revocable watermarking by difference expansion," in Proceedings of Multimedia and Security Workshop at ACM Multimedia, Dec. 2002.

[11] H. Lu, R. Shen, F.L. Chung, "Fragile Watermarking Scheme for Image Authentication," *IEE Electronics Letters*, pp. 898-900, June 2003

[12] The Daubechies wavelet transform
Kristian Sandberg,Dept. of Applied Mathematics
University of Colorado at Boulder

[13] Self-Similar watermarks for counterfeiting geometrical attacksV. Solachidis[1], S. Tsekeridou[2], S. Nikolopoulos[1] and I. Pitas[11]Department of Informatics, Aristotle University of Thessaloniki,Box 451,Thessaloniki 54124, Greece,e-mail: {vasilis, nikolopo, pitas}@aiia.csd.auth.gr [2]Electrical & Computer Engineering Dept. Democritus Univ. of Thrace ,Xanthi 67100, Greece ,e- mail:tsekerid@ee.duth.gr

[14] attacks on digital wavelet agewate rmarks, Andreja Sam˘covi´c,J´an Tur´an