A COMPARATIVE STUDY OF DIGITAL WATERMARKING TECHNIQUE THAT ATTACK LARGE SCALE IMAGE CROPPING

P.NAGARJUNA [1] , Y.GANGADHAR [2]

[1] M.Tech, CSE, Dept of Computer Science, Kuppam Engineering College, Kuppam, A.P., India.
[2] Assoc. Professor, Dept of Computer Science, Kuppam Engineering College, Kuppam, A.P., India

ABSTRACT— *To enhance our scheme's robustness and guarantee the least impact on the embedded images, we use a reinserted encoding method in the discrete cosine transform (DCT) domain to accomplish the embedding and extraction procedure. In addition to resisting various malicious attacks, our method requires minimal information to extract the embedded watermark and restore the host image with high quality. To help describe the method, we use a simulator pre-inserted code (PIC) to perform all the procedures. Once the watermarked image is tampered with, legal users can no longer extract the watermark information to confirm the copyright. The second method involves removing embedded information from the watermarked images to construct an unmarked image of satisfactory quality. This restorability can be utilized to preserve artistic or valuable images. The robustness and quality of the restored image are important concerns in evaluating a removable watermarking scheme. Often used in pairs in this emerging field, digital watermarks have shown promise in protecting the copyright of digital products.* Keywords—component; formatting; style; styling; insert (key words)

***Index Terms*- Digital Watermark, Cover Media, Crop-Resist, Image Attacks, Lossy compression.**

I. INTRODUCTION

Traditionally, source authentication and integrity verification of digital data have been performed by digital signatures. A digital signature is a data string which associates (binds) a piece of information (in digital form) with some originating entity [2], [3]. With the availability of sophisticated image/video editing tools, authentication of multimedia data is gaining importance. Image authentication in traditional manner requires the storage and transmission of signature strings in the image header [4]. This method imposes limitations on the image/file format—sometimes preventing implementation in legacy systems. It is also susceptible to loss during format conversions—even if the underlying image data remains intact. It is therefore desirable to include the digital signatures within the image data. This goal can be achieved using watermarks [5-8], which exploit the redundancy in the image data and the insensitivity of the human visual system (HVS) to small distortions .In addition to format independence, digital watermarks have the advantage of tamper localization, which refers to the ability to identify the image regions that have been tampered (manipulated) after insertion of the watermark.

The functionality offered by digital watermarks, however, often comes at the expense of image fidelity. Most watermarking techniques modify, and hence distort, the host signal in order to insert authentication information. In many applications, loss of image fidelity is not prohibitive as long as original and modified images are perceptually equivalent. On the other hand, in medical, military, and legal imaging applications, where the need for authentication is often paramount, there are typically stringent constraints on data fidelity that prohibit any permanent signal distortion in the watermarking process. The loss of signal fidelity can be remedied by the use of lossless (also referred as reversible, invertible, or distortion- free) authentication watermarks [9-11]. These methods, like their lossy counterparts, insert authentication information by modifying the host signal, thus induce an embedding distortion. Nevertheless, they also enable the removal of such distortions and hence exact—lossless—restoration of the original host signal. The original contribution of this paper is a novel lossless authentication framework. As opposed to earlier schemes, this framework validates the authenticity and integrity of watermarked images before attempting to reconstruct the original image. If the verification step is successful, the integrity of their constructed (original) image is inferred from the uniqueness of the reconstruction procedure. This reduces computational requirements in situations when either the verification step fails or the zero-distortion reconstruction is not needed. The framework also enables public (-key) authentication without granting access to the perfect original and allows for efficient tamper localization.

Virtually all existing schemes [9–14] follow this frame work with differences in the lossless data embedding step. In [9], Fridrich et al. implemented the lossless data embedding step by compression and replacement of one or more least-significant bit planes of the image data. Later, the authors proposed a more efficient algorithm based on RS-embedding method [13].Meanwhile, Honsinger et al. [10] proposed using a spread-spectrum watermark with modulo-addition for lossless reconstruction. Similarly, De Vleeschouwer et al., Tian and vander Veen have proposed methods based on the circular interpretation of the image histogram [14], difference expansion [11], and histogram modifications [15], respectively. In [16], Dittman et al. proposed an alternative protocol based on the least significant bit (LSB) compression technique of [9], the protocol utilizes a public and a private key signature corresponding to the most and least significant bit planes, respectively. When combined with the encryption of the compressed LSB information, the method allows for public-key verification of the watermarked image while reserving the reconstruction of the perfect original to the authorized parties that hold the private-key. Despite the added functionality, the protocol is not extensible to all lossless embedding methods, for instance Honsinger's method [10]. Furthermore, it requires an increased payload, thus a higher embedding distortion, due to the second signature. Note that none of the lossless authentication methods in the literature offer tamper localization capability, which is one of the major advantages of authentication watermarks over conventional digital signatures.

In Sections II, we present a brief overview of the proposed framework, respectively. A specific implementation of the framework and related experimental results are discussed in Section III. Conclusions are drawn in Section IV.

II. PROPOSED WATERMARKING SCHEME

Embedding watermarks involves two key tasks: confirming copyright protection and maintaining the original view of the carrier image. To protect the copyright of an image, a watermarking mechanism must be robust enough to resist malicious attacks—that is, an authorized user must be allowed to retrieve are cognizable logo, even if the watermarked image has been attacked. Furthermore, the watermarked image's quality must be good so that it is difficult for an intruder to distinguish between the host image and the embedded one. In addition, the embedded information should not seriously distort the protected image, which may degrade the image's value .Thus, when evaluating a watermarking mechanism's performance, researchers concentrate on three issues: robustness, the watermarked image's quality, and the restored image's quality.

Robustness is pivotal to multiple applications of digital watermarks because it affects the watermarking system's practicability. In the embedded imaging field, robustness refers to how resistant an approach is to attacks aimed at destroying or removing hidden watermarks, including cryptographic attacks, cropping attacks, geometrical attacks, and some protocol attacks [9–14]. Among these attacks, the most damage occurs as a result of cropping, which destroys the watermark's useful information.

In previous works, cropping embedded images compromised the integrity of a digital watermark. However, images easily suffer this kind of damage during attacks[15] Thus, in our approach; we first structurally encode the watermark information and then embed it into the cover image. Consequently, the watermark's legal information can be recognized efficiently. Our experiments show that the watermark is inerasable, even if only one-quarter of the watermarked image is left. The structured encoding watermark also performs well when we take other attacks into account, including filtering, compression, and noise adding.

Still, maintaining the robustness of the embedded image is far from protecting the image. Considering the essential need to preserve valuable images, a watermarking scheme that lets authorized users remove the embedded watermark information without changing the visualization of the original image is of great significance. There are two conventional approaches for restoring unmarked images: reversible and removable methods.2–4, 7, 9 the first type let's authorized users embed information into the host image. To restore the lossless host image, a verifier can remove the embedded watermark information. These reversible methods have been applied to fragile watermarking for authentication services. However, these approaches are incapable of resisting malicious attacks, which are common in the digital world. That is, reversible methods cannot achieve the robust requirement of watermarking schemes because of the embedded watermark's sensitiveness and vulnerability. Once the watermarked image is tampered with, legal users can no longer extract the watermark information to confirm the copyright.

The second method involves removing embedded information from the watermarked images to construct an unmarked image of satisfactory quality. This restorability can be utilized to preserve artistic or valuable images. The robustness and quality of the restored image are important concerns in evaluating a removable watermarking scheme. Moreover, because it's always inconvenient to obtain the original image, extracting the watermarked picture shouldn't require information about the original—that is, it should be possible to obtain the watermark sequence referring only to the embedded image instead of other assistances besides the image itself.

To recognize the efficient information of watermark Info, which consists of 0 and 1, PIC first converts Info into the 960-bit one-dimensional (1D) sequence. Then, PIC pre-inserts the 32-bitspecial code synchronously at the beginning of Info to make up the resultant sequence asInfo'¼(special code) jj Info. At the end of Info' ,PIC adds

the same 32 bits as a reserve to form a watermark that is 32 x 32 pixels in size. Regarding the special code selection, we need a robust sequence with three characteristics. First, the code must be strong to resist malicious attacks. That is, even if some bits in the pre-inserted special code are modified, the result will be recognizable because of the exchangeable bits inside. Second, the special code must be obviously different from the normal watermark information. In our technique, the actual watermark information is recognized under the code's heading, so the pre-inserted code must be independent of the interference of the real Watermark information. Additionally, this special PIC must be 32 bits so that, when combined with the entire embedded watermark sequence, the size will be 1,024 bits.

A. Embedding Processing

In the embedding phase, we introduce procedures to embed watermark information into the host image. Here, PIC completes the embedding task based on small, or processing significant (PS), blocks.

In step 1, PIC divides the host image into several slices, each of which is sized 256 x 256.

In step 2, PIC divides each 256 x 256 slice it into non overlapping 8 x 8 blocks—that is, the PS blocks.

In step 3, for each slice, PIC transforms these 256 PS blocks into their DCT domains and selects the four lowest frequency AC coefficients in each of them to embed the watermark sequence.

As the coordinates of the selected AC coefficients are (0, 1), (1, 0), (2, 0), and (1, 1). Thus, every four bits of the watermark can be embedded into one PS block and each 32 x 32 watermark can be hidden in one slice.

B. Blind Watermark Extraction

To extract the watermark from an embedded image, PIC constructs a coordinate axis and divides the image into slices using the same method as in the embedding processing. Within one slice, PIC obtains the embedded 8 x 8 PS blocks. For these blocks, PIC performs the DCT transformation to get four intended coefficients (as Figure 2 shows). Then, PIC retrieves the third LSB of the acquired coefficient and the last bit.

C. Image Restoration

Given the copyright issue, it's popular to embed a watermark into a host image to demonstrate its authorization. On the other hand, authorized users must be able to remove embedded watermarks to restore the original digital image. Thus, the quality of the restored image is vitally important .In our method, the restored image can achieve almost lossless recovery with the secret information {k, m}, where k demonstrates the k th zigzag position in the middle-frequent band and m represents the m th bit to the inserted NP.

III. SIMULATION RESULTS

The proposed approach provides an invisible watermark to protect the copyright of digital products. We first examined the quality of the watermarked images under different test carriers.

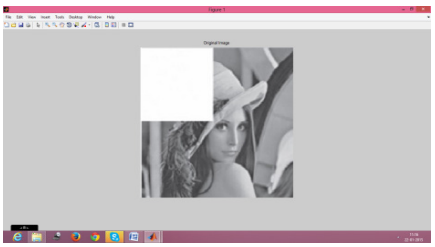

Fig.3.1. Original Image

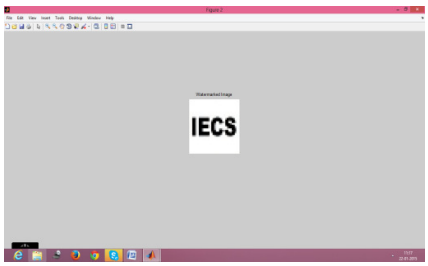

Fig.3.2. Watermarked Image

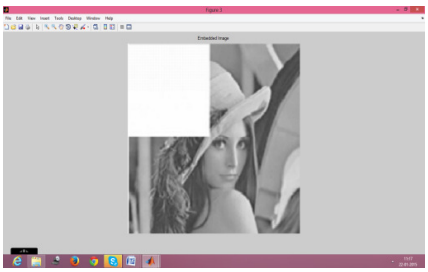

Fig.3.3. Embedded Image

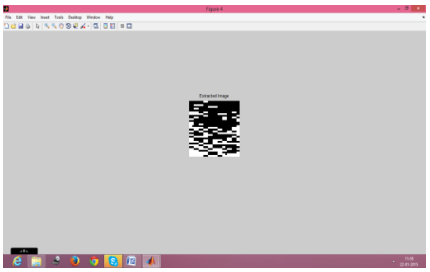

Fig.3.4. Extracted Image

Figure 3.1 to 3.4 shows the results of different test images after embedding the invisible watermark. Undoubtedly, our method can achieve high PSNR values of watermarked images and preserve satisfactory quality from the human vision perception under distinct test carriers. That is, the embedded logo does not distort the appearance of the images. Furthermore, the retrieved invisible watermarks are recognizable, so that they can correctly indicate the ownership of the protected images.

IV. CONCLUSION

Our novel, self-recognized, and crop-resistant watermarking method guarantees the visual quality of the embedded image and is robust against various attacks. Our method cannot yet handle attacks of more than 75 percent cropping, and its embedding efficiency must be improved to achieve better visualization of different types of host images. Our future research will focus on finding a more robust pre-inserted code to mark the head location of the embedded watermark's original position as well as efforts to base the embedding process on the host image feature to achieve higher visual efficiency.

REFERENCES

[1] T.H. Chen and D. S. Tsai, "Customer Right Protection Mechanism Using a Watermarking Scheme and a Watermarking Protocol," Pattern Recognition, vol. 39, no. 8, 2006, pp. 1530–1541.

[2] A.M. Altar, "Reversible Watermark Using the Difference Expansion of a Generalized Integer Transform, "IEEE Trans. Image Processing, vol. 13, no. 8,2004, pp. 1147–1156

[3] C.C. Chang et al., "Reversible Hiding in the DCT Based Compressed Images," Information Sciences, vol. 177, no. 13, 2007, pp. 2768–2786

[4] C.C. Chang, W.L. Tai, and C.C. Lin, "A Reversible Data Hiding Scheme Based on Side Match Vector Quantization," IEEE Trans. Circuits and System for Video Technology, vol. 16, no 10, 2006,pp. 1301–1308.

[5] T. Kalker et al., "A Video Watermarking System for Broadcast Monitoring," SPIE Proc. 3657: Security and Watermarking of Multimedia Contents II, SPIE, 1999, pp. 103–112.

[6] J.Fridrich, "Visual Hash for Oblivious Watermarking, "SPIE Proc. 3971: Security and Watermarking of Multimedia Contents II, SPIE, 2000, pp. 286–294.

[7] M.U. Celik, G. Sharma, and A.M. Tekalp, "Lossless Watermarking for Image Authentication: A New Framework and an Implementation," IEEE Trans. Image Processing, vol. 15, no. 4, 2006, pp.1042–1049

[8] Y.Hu and B. Jeon, "Reversible Visible Watermarking and Lossless Recovery of Original Images," IEEE Trans. Circuits and Systems for Video Technology, vol. 16, no. 11, 2006, pp. 1423–1429.

[9] C.C.Chang, P.Y. Lin, and J.S.Yeh, "Preserving Robustness and Removability for Digital Watermarks Using Sub sampling and Difference Correlation," Information Sciences, vol. 179, no. 13, 2009, pp. 2283–2293.

[10] C.Y. Lin and S.F. Chang, "A Robust Image Authentication Method Distinguishing JPEG Compression from Malicious Manipulation," IEEE Trans. Circuits and Systems for Video Technology, vol. 11, no. 2, 2001, pp. 153–168.

[11] P. Bas, J.M. Chassery, and B. Macq, "Geometrically Invariant Watermarking Using Feature Points," IEEE Trans. Image Processing, vol. 11, no. 9, 2002,pp. 1014–1028.

[12]. C.S. Lu, H.Y. Liao, and M. Kutter, "Denoising and Copy Attacks Resilient Watermarking by Exploiting Prior Knowledge at Detector," IEEE Trans. Image Processing, vol. 11, no. 3, 2002, pp. 280–292.

[13]. J. Barr, B. Bradley, and B.T. Hannigan, "Using Digital Watermarks with Image Signatures to Mitigate the Threat of the Copy Attack," Proc. Int'l Conf. Acoustics, Speech, and Signal Processing, IEEE Press,2003, pp. 69–72.

[14]. Q. Cheng and T.S. Huang, "Robust Optimum Detection of Transform Domain Multiplicative Watermarks," IEEE Trans. Signal Processing, vol. 51, no. 4, 2003, pp. 906–924.

[15]. C.S. Lu and H.-Y.M. Liao, "Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme," IEEE Trans. Multimedia, vol. 5, no. 2, 2003, pp. 161–173.

[16]. W. Lu, H. Lu, and F.L. Chung, "Robust Digital Image Watermarking Based on Sub sampling," Applied Mathematics and Computation, IEEE Press,2006, pp. 886–893.

[17]. S. Craver et al., "Resolving Rightful Ownership with Invisible Watermarking Techniques: Limitations, Attacks and Implications," IEEE J.Selected Areas in Comm., IEEE Press, 1998, pp. 573–586.

[18]. X. You et al., "A Blind Watermarking Scheme Using New Non tensor Product Wavelet Filter Banks," IEEE Trans. Image Processing, vol. 19, no. 12, 2010,pp. 3271–3284.