CryptMark: A Novel Secure Invisible Watermarking Technique for Color Images

Saraju P. Mohanty
Dept. of Computer Science and Engineering
University of North Texas
Denton, TX 76203.
Email: smohanty@unt.edu

R. Sheth, A. Pinto, and M. Chandy
Dept. of Information Technology
St. Francis Institute of Technology
Mumbai - 400103, India.
Email: rajansheth@yahoo.com

Abstract

With the explosive growth of internet technology, many innovative applications requiring exchange of large amounts of multimedia data have become feasible. However, this kind of convenience with which authorized users can access information, turns out to be a mixed blessing because of information piracy. The emerging field of digital rights management (DRM) systems addresses the issues related to the intellectual property rights of digital content. In this paper, we present a novel invisible watermarking method that uses cryptography and watermarking methods simultaneously to provide a double layer protection to the digital media which can be an effective technique for DRM. Our proposed method securely hides binary information in color image media, and securely extracts and authenticates it using a secret key. Experimental results prove that our proposed invisible watermarking techniques is resilient to 90% of the well known benchmark attacks and hence a fail-safe method for providing constant protection to the ownership rights.

1 Introduction

The Internet revolution towards the end of the last millennium ushered in a new era of information technology. There has been an explosive growth in multimedia applications such as video-on-demand, distance education, *etc*. However, this kind of ultimate flexibility to avail digital content, particularly that of the images, has its negative side too. Easy access facilitates information piracy through unauthorized replication and manipulation of digital content with the help of inexpensive tools. Hence, concerns about protection and enforcement of intellectual property (IP) rights of the digital content involved in the transactions, have also been mounting. The emerging field of digital rights management (DRM) systems [3, 9] addresses these issues related to ownership rights of digital content. Two basic goals of DRM systems that can be met with digital watermarking are: i) preventing unauthorized use of the images (in general, any digital information), particularly for commercial purposes and ii) providing visibility to the authentic source or the owner of the information on a continuous basis. Research on watermarking has matured over the last decade and hence the current literature abounds with techniques in this area [8, 1, 5, 11, 7, 6, 10].

Digital watermarking, in essence, is the process of embedding into a multimedia object a digital signature or data that is variously known as watermark, tag or label. Detection or extraction of this watermark at a later time enables users to make an assertion about the authenticity and ownership of the object. Hence, watermarking is one of the key technologies that can be used for establishing ownership rights, tracking usage, ensuring authorized access, preventing illegal replication, and facilitating content authentication. When encryption techniques are used in conjunction with watermarking [4], full protection from unauthorized access of digital content can be achieved. Our novel approach aims at this two-tier protection mechanism with simultaneous use of cryptography and invisible watermarking.

Organization of the rest of the paper is as follows: We highlight the contributions of this paper in Section 2. Section 3 presents the proposed invisible watermarking algorithm. Algorithm implementation, usage and validation are detailed in Section 4 along with the introduction of watermarking system. Finally, summary and conclusions are presented in Section 5.

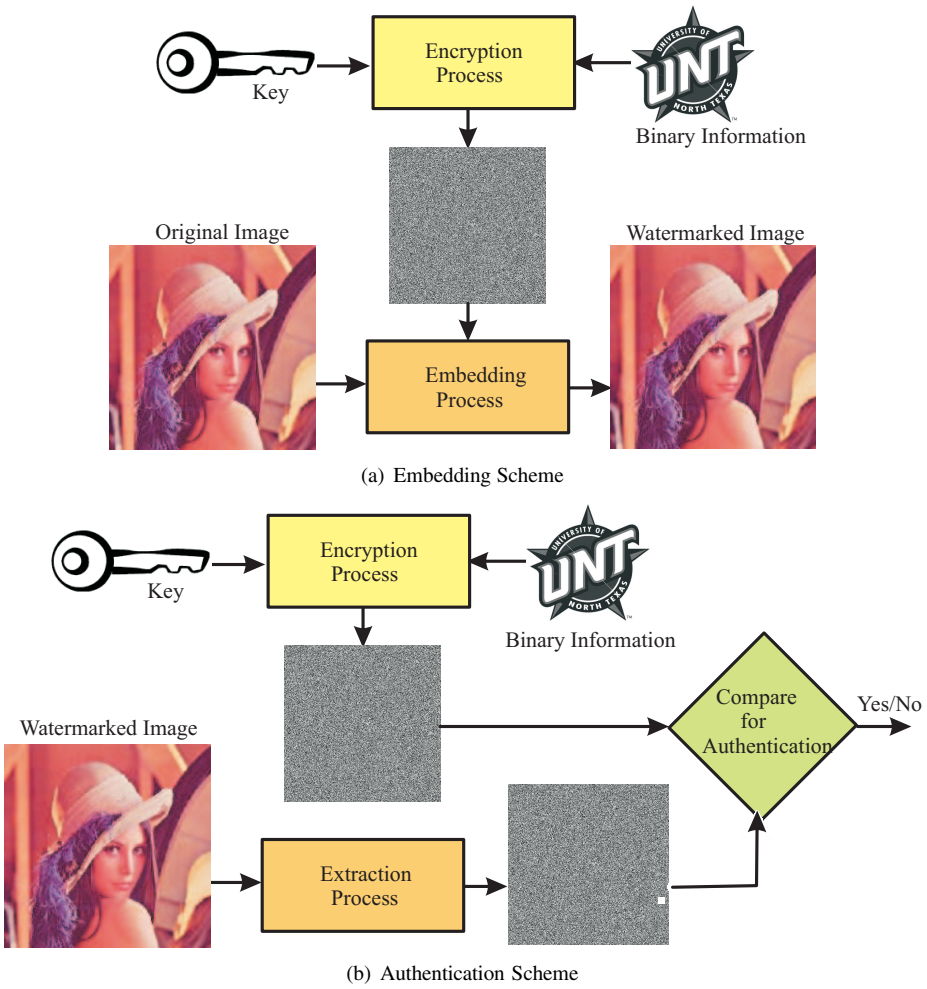
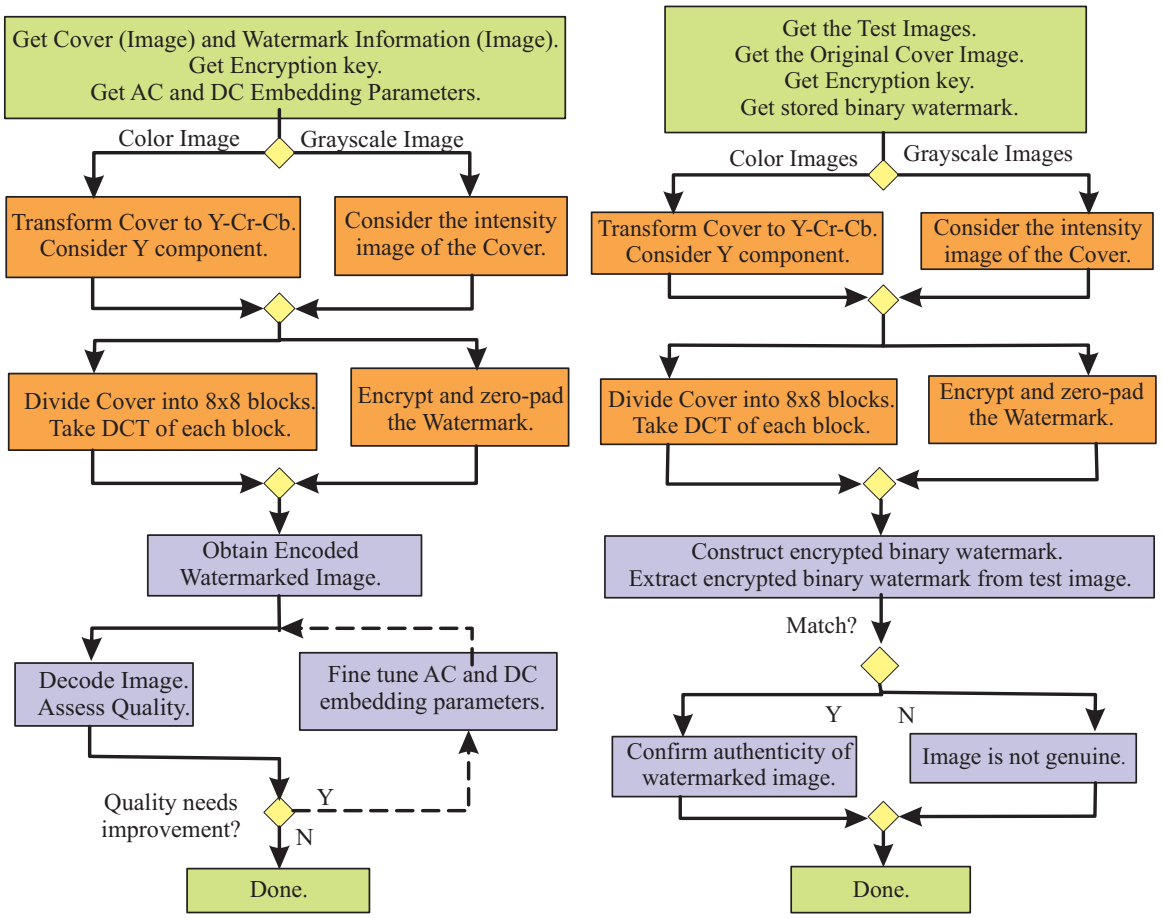


Figure 1. The Proposed Secure Watermarking Scheme: CryptMark

2 Contributions of this Paper

Various aspects of content management namely, content identification, storage, representation, and distribution and intellectual property rights management are highlighted in DRM. Unauthorized access of digital content is being prevented by implementing encryption technologies. However, it does not prevent an authorized user from illegally replicating the decrypted content. Hence, encryption alone does not address all the IP issues related to DRM. Digital watermarking can be used for establishing ownership rights, tracking usage, ensuring authorized access, preventing illegal replication and facilitating content authentication. Therefore, a two layer protection mechanism utilizing both watermarking and encryption is needed for effective DRM; the contribution of this paper is to provide such a framework. The paper presents a novel invisible watermarking method that uses cryptography and watermarking methods simultaneously to provide a double layer protection to the digital media which can be an effective technique for DRM. Our proposed method securely hides binary information in color image media, and securely extracts and authenticates it using a secret key as demonstrated in Fig. 1. The *advantage* of encrypted watermark processing is that at no point of time raw watermark information is passed in the transmission channel, thus providing *maximum security*. The proposed embedding process uses both DC and AC DCT (discrete cosine transform) components to carry the payload, unlike most of the existing algorithms who heavily rely on low frequency AC components. This provides more resilience to lossy compression, a process that is heavily dependent on smaller low frequency values of AC components. In addition, we selectively add or subtract the watermark from the DCT coefficients instead of performing adding operation in typical available algorithms. Thus, our approach allows to carry *maximum payload* with highest robustness and highest undetectability, the three contradictory objectives of data hiding mechanism.



(a) Algorithmic Flow of the Insertion Process

(b) Algorithmic Flow of the Extraction and Authentication Process

Figure 2. The Proposed Secure Invisible Watermarking Algorithm (CryptMark) Simultaneously using Encryption and Watermarking Methods.

3 The Proposed CryptMark Algorithm

The algorithmic flow of our proposed watermark secure *insertion* process is represented in Fig. 2(a). Our algorithm first encrypts the watermark and then fuses it into the intensity image of the cover image in case of a grayscale, or into the Y-component (in the Y-Cr-Cb coordinate system) of a colored. We refer to the relevant component of the cover image as I. Decomposition of the image to obtain the required component is done in the preprocessing stage of our algorithm. Encryption and hashing of the binary watermark using a user-supplied key is also performed in this preprocessing step. At this step, any image extension necessary to facilitate the division of the image into integral number of blocks is performed.

After preprocessing, the cover image I is divided into 8×8 blocks and each block is transformed into the DCT domain. Let us denote the "(i, j)"th DCT coefficient of the kth block by $c_{ij}(k)$. Supposing that the image has M blocks overall, each block can be numbered uniquely with a number in the range $[1, M]$ based on its position in the raster scanning of the image. M is given by $\left(\frac{nrow \times ncol}{64}\right)$, where $nrow$ is the number of image pixels row-wise, and $ncol$, the number of pixels column-wise. Based on our experience with perceptual analysis, we need to decide on how many frequency (DCT) components should be considered for obtaining good quality watermarked images. Let us suppose we need only the DC component c_{00} and the three 3 low frequency components c_{01}, c_{10}, and c_{11}. In this case, the size of the encoded and hashed watermark should be such that it can be partitioned into the same number of blocks as the cover image, but with a block size of 2×2. It cannot be bigger, but, if it is smaller, it can be padded with zeros. Let us now use the same notation as before and denote the watermark's binary value at position (i, j) in block k by $w_{ij}(k)$. This watermark can be embedded in the cover image using

the formula: $\forall i, j,$ and k,

$$c'_{ij}(k) = \begin{cases} c_{ij}(k)(1+\alpha_{ij}) & if \;\; w_{ij}(k) = 1, \\ c_{ij}(k)(1-\alpha_{ij}) & if \;\; w_{ij}(k) = 0. \end{cases}$$

Unlike Cox *et al.*'s method, we do not always add the watermark to the significant frequency components. Instead, we add it to some components and subtract it from the other components as suggested by Craver *et al.* [2]. This strengthen the requirement that a statistical analysis of the watermarked image should not reveal the presence of an invisible watermark. Unlike Cox *et al.* we use use two embedding factors: α_{dc} for DC components and α_{ac} for AC components. Thus, we have $\alpha_{00} = \alpha_{dc}$ and $\alpha_{01} = \alpha_{10} = \alpha_{11} = \alpha_{ac}$. Since choosing so many scaling factors (one for each frequency component) is a problem by itself, we confined ourselves to only two values that may be so chosen as not to degrade the quality of the watermarked image. Image quality can be assessed either quantitatively by measuring its SNR (Signal-to-Noise Ratio) or other similar measures.

In the case of grayscale cover images, the watermarked image I' can be obtained by performing block-wise IDCTs (Inverse Discrete Transforms) on the coefficients modified as above. However, in the case of colored images, we get only the Y-component of I' by the above process. This should be clubbed with the Cr and Cb components of the cover to get I'. At this point, we may have an optional step (dashed line) of assessing quality of the watermarked image by either visual inspection or a computational measure and fine-tuning the parameters α_{ac} and α_{dc}.

The flow of secure *extraction and authentication* process in the proposed CryptMark is demonstrated in Fig. 2(b). The extraction algorithm involves the following sequence of steps. First the watermarked (possibly suspect) test image I' and the original cover image I are obtained. The watermark information (image) and the original encryption key are then obtained. After initial preprocessing both I' and I are divided into 8×8 blocks. During this phase if the image is color then it is converted from RGB space to YCbCr representation. DCT coefficients of both the images are obtained for all the blocks. The blocks of both test image and original image are then compared. If a DCT coefficients in a block of I' is larger than the corresponding coefficient in the original image block then the watermark bit is 1, else it is 0. Finally, the extracted sequence with the binary watermark (encrypted with the key) is compared to make a decision whether the image is authentic or not.

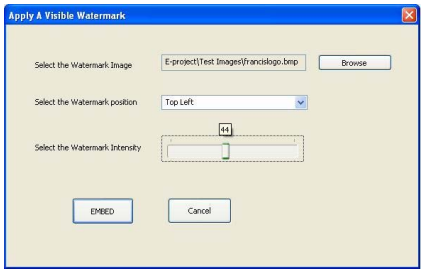
4 Algorithm Implementation and Experiments

The CryptMark algorithm is implemented in VC++.NET and integrated in our ongoing system called ISWAR (Imaging System with Watermarking and Attack Resilience) the

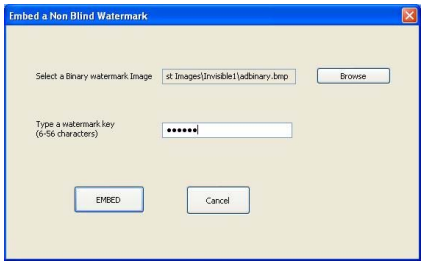
Binary Watermark
by SPM

Figure 3. The Binary Invisible Image used as Watermark in Our Experiments

(a) Open an Image



(b) Select Position, Size and Intensity (*for Visible Watermarking*)



(c) Enter Watermarking Key (*For Invisble Watermarking*)

(d) Watermarked Image

Figure 5. Graphics User Interface of ISWAR

(a) Original Lena (b) Watermarked Lena (c) Original F16 (d) Watermarked F16

(e) Original mandril (f) Watermarked mandril (g) Original pepper (h) Watermarked pepper

Figure 4. Performance Evaluation CryptMark for a Set of Test Images

executable of which is made available at the following website: `http://www.cse.unt.edu/~smohanty/ISWARwatermarker/` for public use. The system defaults for α_{ac} and α_{dc} are set to 0.1 and 0.02, respectively. These values have been found to yield optimal results and hence have been incorporated into the system as defaults. The encryption algorithm used in the algorithm is Blowfish, but it could be replaced by any other available encryption process, such as AES (Advanced Encryption Standard).

ISWAR has a user-friendly interface through which choice of the algorithms and the specification of parameters can be done. The graphical user interface (GUI) for ISWAR is shown in Fig. 5. Upon selection of the watermarking type, visible or invisible, from the watermark menu, the corresponding dialog is invoked for further information. For visible watermarking, the user needs to specify the position of the watermark on the host image as well as the relative intensity of the watermark compared to the host. For invisible watermarking a dialog is invoked for the user to select the watermark image and provide a watermark key which is used for authentication and extraction purposes.

We performed exhaustive testing of our CryptMark algorithm for several test images. The binary image used in our experiment is depicted in Fig. 3. In Fig. 4, we present the consolidated results on on the images of Lena, F16, mandrill and pepper images, respectively. The quality of the images obtained using our watermarking algorithm may be assessed by visual inspection of the watermarked images in Fig. 4. In addition, the PSNR (Peak Signal-to-noise ratio) of the watermarked images shown in the figure given in Table 1 provide a quantitative assessment of the quality. Either way, our algorithms are effective in this respect. Finally, the performance of the algorithm with respect to attack resilience has been established by the results shown in Table 1 for the well-known Stirmark attack against the algorithm. The watermarking survived all but one of the attack types included in the synthetic benchmark attack, Stirmark.

In the table, we reported only the binary outcomes of different attacks, that is, whether the watermark extracted has survived in the sense that it is recognizable as a replica of the original watermark, or not. As long as the extracted watermark is recognizable, the purpose is served. There is always a tradeoff between the perceptual quality of the watermarked image produced by an algorithm and the quality of the extracted watermark under noise and other degradations. Hence, after establishing with different images that the visual quality of our watermarked images is acceptable, we presented the results that help benchmarking our algorithm against the ideal algorithm that survives all the attack types in the Stirmark attack. The results indicate that the attack survivability of our algorithm is at 90% of that an ideal algorithm.

Table 1. Attacks Performed using Benchmarks for Testing of the Invisible-Robust Algorithm

Attacks Performed for Testing	For Various Test Image			
	Lena (SNR = 105)	F16 (SNR = 99)	mandril (SNR = 101)	pepper (SNR = 108)
JPEG Compression 0 quality	Survived	Survived	Survived	Survived
Gray scaling 16 levels	Survived	Survived	Survived	Survived
Gray scaling 256 levels, JPEG compression 0 quality	Survived	Survived	Survived	Survived
Blurring , 0 quality JPEG Compression	Survived	Survived	Survived	Survived
Partial cropping	Survived	Survived	Survived	Survived
Stirmark Self Similarities	Survived	Survived	Survived	Survived
Stirmark 0 quality JPEG compression	Survived	Survived	Survived	Survived
Stirmark median filtering	Survived	Survived	Survived	Survived
Stirmark Random Distortions	Survived	Survived	Survived	Survived

5 Summary and Conclusion

In this paper, we present a novel invisible watermarking method called CryptMark that uses cryptography and watermarking methods simultaneously to provide a double layer protection to the digital media which can be an effective technique for DRM. Exhaustive testing of the algorithm proved that the algorithm works well and can survive various forms of attacks. We are currently considering having two watermarks, a user specific binary watermark and a synthetic watermark generated by the system, and fuse them together in to the cover for additional protection and better image quality. Other possible extensions include use of wavelet transforms for embedding of strong watermarks. Blind extraction of invisible watermarks is also a planned extension particularly because of its usefulness in authentication at the receiver end as well as identification of secretive communication.

6 Acknowledgment

The authors would like to acknowledge the help of P. Guturu, Dept of Electrical Engineering, N. Pati, Dept of Computer Science and Engineering, and E. Kougianos, Dept of Engineering Technology at the University of North Texas.

References

[1] I. J. Cox and J. P. M. G. Linnartz. Some General Methods for Tampering with Watermarks. *IEEE Journal on Selected Areas in Communications*, 16(4):587–593, May 1998.

[2] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung. Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications. *IEEE Journal on Selected Areas in Communications*, 16(4):573–586, May 1998.

[3] S. Emmanuel and M. S. Kankanhalli. A Digital Rights Management Scheme for Broadcast Video. *ACM-Springer Verlag Multimedia Systems Journal*, 8(6):444–458, June 2003.

[4] A. M. Eskicioglu and E. J. Delp. An Overview of Multimedia Content Protection in Consumer Electronics Devices. *Elsevier Signal Processing : Image Communication*, 16:681–699, 2001.

[5] H. Guo and N. D. Georganas. A Novel Approach to Digital Image Watermarking Based on a Generalized Secret Sharing Scheme. *ACM-Springer Verlag Multimedia Systems Journal*, 9(3):228–238, March 2003.

[6] G. Jiang, M. Yu, S. Shi, X. Liu, and Y. D. Kim. New Blind Image Watermarking in DCT Domain. In *Proceedings of the 6th International Conference on Signal Processing*, volume 2, pages 1580 – 1583, Aug 2002.

[7] Z. M. Lu, D. G. Xu, and S. H. Sun. Multipurpose Image Watermarking Algorithm based on Multistage Vector Quantization. *IEEE Transactions on Image Processing*, 14(6):822–831, June 2005.

[8] F. Mintzer, G. Braudaway, and M. Yeung. Effective and Ineffective Digital Watermarks. In *IEEE International Conference on Image Processing (ICIP-97)*, volume 3, pages 9–12, 1997.

[9] S. P. Mohanty, R. K. C., and S. Nayak. FPGA Based Implementation of an Invisible-Robust Image Watermarking Encoder. In *Lecture Notes in Computer Science*, volume 3356, pages 344–353, 2004.

[10] Y. T. Pai, S. J. Ruan, and J. Götze. Energy-Efficient Watermark Algorithm Based on Pairing Mechanism. In *Lecture Notes in Computer Science (LNCS), KES (1)*, pages 1219–1225, 2005.

[11] N. P. Sheppard, R. S. Naini, and P. Ogunbona. On Multiple Watermarking. In *Proceedings of the ACM Multimedia workshops on multimedia and security: new challenges*, pages 3–6, 2001.