Protection Mechanism using Cryptography and Robust Watermarking for Color Images

Rajesh Malik[1], Sonal Chugh[2]
[1]Assistant Professor in Department of Electronics and Communication Engineering, N.C.C.E Panipat, India
[2]Student Pursuing Mtech in Department of Electronics and Communication Engineering, N.C.C.E Panipat, India

ABSTRACT
Exchange of large amount of multimedia data have become feasible with the explosive growth of internet technology. People can easily copy and modify the digital product which leads to the piracy problems which is spreading over the internet and thus poses a great threat to the ownership rights. Digital Right Management (DMR) has emerged to raise the issues regarding intellectual property rights. In this paper, a two tier protection mechanism has been proposed that uses both cryptography and robust watermarking simultaneously to provide effective protection mechanism for DMR. In this the binary information is kept hidden in the color image using a secret key by firstly converting into a scrambled code that can be securely extracted and authenticated. Compare the two images to access its quality and to check if the quality needs improvement. Also to check if the proposed method can survive under various intentional or unintentional attacks.

Keywords
Digital Right Management, Robust Watermarking Cryptography, Discrete Cosine Transform.

I. INTRODUCTION

THE phenomenal growth of internet has increased the flexibility of using the digital content but this flexibility has increased the rate of piracy amongst the unauthorized users and also manipulation of the digital content using various tools. So Digital Right management has emerged as a system that prevents unauthorized users and also provides visibility to the owner continuously. The watermarking techniques generally serve the two purposes first the copyright protection from the unauthorized users and second the data authentication for the owner of the information.

A watermark is the hidden information within a digital signal (such as image, video, audio, polygonal model). It is integrated into the content of host signal itself. Digital Watermarking is referred to as simply watermarking, a pattern of bits inserted into a digital image, audio or video file that identifies the file's copyright information (author, rights, etc.) i.e. of embedding into a multimedia object a digital signature or data that is variously known as watermark, tag or label. The watermarking that survives under intentional attacks is called robust watermarking which mainly focus on high quality. The properties of such watermarking are: 1) It is invisible to human observer.2) it is difficult for an

unauthorized person to insert a false watermark in it. 3) the watermark can be quickly extracted by an authorized person. 4) the extracted watermark indicates where alterations have taken place and thus helps in improving the quality also[1]. Using cryptography along with robust watermarking provides a two-tier protection mechanism. This method securely hides binary information in color image media, and securely extracts and authenticates it using a secret key. Thus using both cryptography and robust watermarking simultaneously we can derive the parameters which can help in the enhancement of quality of image when the decoded watermarked image is compared with the original image. We also can check if this image could survive after various intentional or unintentional attacks.

A variety of robust watermarking techniques can be broadly classified in two categories: spatial-domain and transfer-domain. Unlike the spatial-domain based techniques that have relatively low bit capacity, transform-domain-based techniques can embed a large number of bits without incurring noticeable visual artifacts. Such techniques can be employed with common image transforms such as discrete cosine transform that we are using here.

This paper is organizes as follows. In Section II, we discuss the existing system. In Section III, we discuss the proposed system. In Section IV, we draw the conclusion.

II. EXISTING SYSTEM

In this system a visual cryptographic approach to generate two random shares of a watermark one is embedded into the cover-image and another is kept as a secret key for the later watermark extraction [2]. The watermark can be extracted by simply 'superimposing the key share over the image. After this a blind watermarking method for 8 bit grayscale images in 8x8 block DCT (Discrete Cosine Transformation) domain was presented. The method was based on an advanced spread-spectrum algorithm in which it extracted the difference between histogram properties of pairs of sub channels [3]. There were 63 AC and 1 DC coefficients. These watermarks resist JPEG compression up to Quality Factor 5. Then a system was developed that showed how to use watermarking technique for visual cryptography. Both halftone watermarking and visual cryptography involve a hidden secret image [4]. For watermarking, the hidden image was usually embedded in a single halftone image while preserving the quality of the watermarked halftone image. Later a blind robust watermarking technique for embedding two watermarks into a host image was proposed. The technique was based on embedding watermark information in sixteen low-frequency band coefficients of the DCT sub-blocks [5]. The Embedding process is based on changing the selected DCT-coefficients of the host image to odd or even values depending on the binary watermark's bit value. The proposed blind watermarking embedding has shown robust against several attacks.

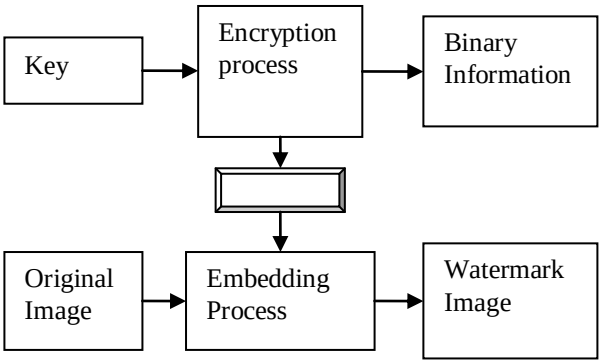
III. PROPOSED SYSTEM

Based on the existing system we found that the resilience to the various watermark attacks was about 90% because most of the existing algorithms heavily rely on low frequency AC components but this proposed embedding process uses both DC and AC DCT (discrete cosine transform) components to carry the payload. This provides more resilience to lossy compression.

Also we will try to selectively add or subtract the watermark from the DCT coefficients instead of performing adding operation in typical available algorithms so as to improve the quality of watermarked image and to see if such variations can give us the resilience above 90% corresponding to various watermark attacks.

Process Description

In our proposed system first for the insertion process we first take an original image and the watermark information that is to be embedded on the original image. Along with this we take an encryption key and AC and DC embedding parameters. Then this whole is to be decomposed in to the color image and the gray scale image. Transform the color image of the original image to Y-Cr-Cb components and consider its Y component for further processing. From the gray scale image of the original image consider its intensity. Combine both the Y component and the intensity component of the color and gray scale image of the original image and then divide it into 8×8 blocks.

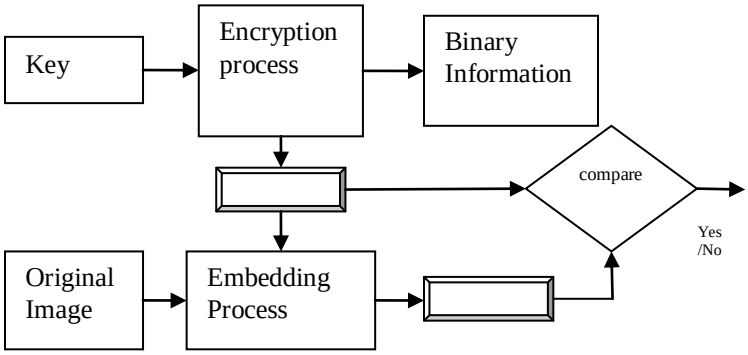


a) Embedding Process

Let us denote the "(i, j)"th DCT coefficient of the kth block by cij(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. Take the DCT of each block. M is given by [(nrow×ncol)/64] where nrow is the number of image pixels row-wise, and ncol, the number of pixels column-wise. 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 c00 and the three 3 low frequency components c01, c10, and c11. In this case, the size of the encoded watermark should be such that it can be partitioned into the same number of blocks as the original 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 wij(k). This watermark can be embedded in the cover image using the formula: ∀ i, j, and k,

C'ij (k) = {cij(k)(1 + αij) if wij (k) = 1,}
{cij(k)(1 − αij) if wij (k) = 0.}

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 [6].



b) Authentication Process

The flow of secure extraction and authentication process involves the following steps. First the watermarked test image and the original cover image are obtained. The watermark information and the original encryption key are then obtained. After initial preprocessing both watermarked and the original images are divided into 8 ×8 blocks. During this phase if the image is color then it is converted from RGB space to Y-Cb-Cr 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 coefficient in a block of watermarked image 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.

In order to improve the quality, obtained encoded watermarked image is first decoded and its quality is accessed. If it shows that some improvement is needed then we will accumulate all the parameters which could help in the Quality Improvement of the Decoded Watermarked Image such as: a) To see the effects on Quality Improvement on varying (α)a.c and (α)d.c parameters. b) To see the effects on Quality Improvement on decreasing the value of DCT.

After such quality improvement by varing the accumulated parameters we can check if the image could survive under various intentional or unintentional attacks and to achieve the above 90% resilience to such attacks.

IV. CONCLUSION

The proposed system uses cryptography and watermarking methods simultaneously to provide a two-tier protection mechanism to the digital media which can be an effective technique for DRM. Most of the existing algorithms heavily rely on low frequency AC components but this proposed embedding process uses both DC and AC DCT (discrete cosine transform) components to carry the payload. This provides more resilience to lossy compression. Also we will try to selectively add or subtract the watermark from the DCT coefficients instead of performing adding operation in typical available algorithms so as to improve the quality of watermarked image and to see if such variations can give us the resilience above 90% corresponding to various watermark attacks

V. REFERENCES

[1] Effective and Ineffective Digital Watermarks by Fred Mintzer,Gordon W.Braudaway and Minerva M. Yeung IBM T.J.Watson Research Center,P.O Box 218,Yorktown Heights, NY10598 1997 IEEE

[2] An Asymmetric Watermarking Scheme based on Visual Cryptography Young-Chang HOU+ Department of Information Management, National Central University, e-mail: ychou@im.mgt.ncu.edu.tw and Pei-Min Chen*Department of Computer and Information Science, SooChow University, e-mail: cpm@cis.scu.edu.tw. Proceedings of ICSP2000.

[3] Blind Watermarking Method Using Partitioned DCT Cchannels Zolthn Rozsnyik(l), Istv6n LovAnyi(2) Budapest University of Technology and Economics Dept. of Control Engineering and Information Technology VIPromCom-2002,4th EURASIP - IEEE Region 8 International Symposium on Video I Image Processing and Multimedia Communications, 16-19 June 2002, Zadar, Croatia.

[4] Joint Visual Cryptography and Watermarking Ming Sun Fu. Oscar C. Au* Hong Kong University of Science and Technology, Clear Water Bay, Hong Kong, China. 2004 IEEE International Conference on Multimedia and Expo (ICME.

[5] A New Blind Image Watermarking Technique for Dual Watermarks Using Low-Frequency Band DCT Coefficients Ahmed N. Al-Gindy, Ayman Tawfik Hussain Al Ahmad and Rami A. Qahwaji 1-4244-1378-8/07/$25.00 ©2007 IEEE.

[6] A New Blind Image Watermarking Technique for Dual Watermarks Using Low-Frequency Band DCT Coefficients Ahmed N. Al-Gindy, Ayman Tawfik Hussain Al Ahmad and Rami A. Qahwaji 1-4244-1378-8/07/$25.00 ©2007 IEEE

[7] CryptMark: A Novel Secure Invisible Watermarking Technique for Color Images Saraju P. Mohanty Dept. of Computer Science and Engineering R. Sheth, A. Pinto, and M. Chandy Dept. of Information Technology in IEEE 2007.