In: Proc. of 1995 IEEE Workshop on Nonlinear Signal and Image Processing (Neos Marmaras, Greece, June 20-22, 1995)

Towards Robust and Hidden Image Copyright Labeling

E. Koch & J. Zhao
Fraunhofer Institute for Computer Graphics
Wilhelminenstr. 7, 64283 Darmstadt, Germany
email: {ekoch,zhao}@igd.fhg.de

Abstract — **This paper first presents a "hidden label" approach for identifying the ownership and distribution of multimedia information (image or video data) in digital networked environment. Then it discusses criteria and difficulties in implementing the approach. Finally a method using a JPEG model based, frequency hopped, randomly sequenced pulse position modulated code (RSPPMC) is described. This method supports robustness of embedded labels against several damaging possibilities such as lossy data compression, low pass filtering and/or color space conversion.**

1 Introduction

The electronic representation and transfer of digitized multimedia information (text, video, and audio) have increased the potential for misuse and theft of such information, and significantly increases the problems associated with enforcing copyrights on multimedia information [1,2]. These problems are rooted from the intrinsic features of the digitally formated information: (1) making copies is easy and inexpensive; (2) each copy is exactly identical to the original; and (3) distribution of the copies (e.g. via network or floppy) is easy and fast. For this reason, creators or publishers of multimedia materials fear providing their works for usage in new multimedia services, and are seeking technical solutions to the problems associated with copyright protection of multimedia data.

These problems have recently raised attentions in national IT (information technology) programmes, for example, NII (National Information Infrastructure) launched in the United States in 1993 established a working group on Intellectual Property Rights which is mainly concerned with copyright law and its application and effectiveness in the context of NII [3]. Several projects are currently or have recently been concerned with copyright and related issues in the digital world, for example, the EC ESPRIT project CITED (Copyright in transmitted electronic data) [4] and COPICAT (Copyright Ownership Protection in Computer Assisted Training) [5], and the EC RACE project ACCOPI (Access Control and Copyright Protection for Images) [6].

In [2], we have summarized that the technical mechanism of copyright protection for information in digital form can be divided into three levels: access control, use right control, and labeling-based mechanism. This paper addresses the problems in developing the last level of mechanism, and presents a JPEG-based method of labeling image for copyright protection.

Although some attention has been given to steganographic labeling and similar problems [7], there exists no technology designed to secretly embed a robust and invisible (hidden) copyright label in images. In particular, no current method adequately addresses the possibilities of using data compression, low pass filtering and/or simply changing the file format to remove an embedded code. Therefore, one of the main goals of this paper is to define a reasonable set of functional requirements and design criteria for an image copyright labeling method, and to furthermore demonstrate that the main difficulties involved in designing such a system can be solved.

The discussion begins with a section which outlines the functionality of the proposed system and general design criteria for the novel embedding technique. A specific method based on the JPEG compression standard for embedding copyright labels in image data is then presented.

2 Requirements and possible attacks

In order to be effective and workable in a multimedia environment, the copyright label must be difficult to remove and survive processing which does not seriously reduce the value of the image. This encompasses a wide range of possibilities including format conversions, data compression, and low pass filtering. In addition to copyright labeling of broadcast images, application areas for steganographic labeling techniques include copyright and/or secure records labeling of electronic publishing, facsimiles, scientific imaging, and medical imaging.

Requiring the copyright label to be a reliable property identification tool imposes following basic functional requirements on the system:

(1) The image must contain a label or code, which marks it as property of the copyright holder.

(2) The image data must contain a user code, which verifies the user is in legal possession of the data.

(3) The image data is labeled in a manner which allows its distribution to be tracked.

It is assumed, the main purpose of any attack would be to make the embedded label unverifiable. There are essentially two general ways to make the embedded label unverifiable: (1) alter the image data to render the copyright label unreadable, and (2) show that the label is not a reliable identification tool.

In addition several properties of digital data and design constraints, which are related to preventing attack on the copyright label, should be considered carefully. First, forgery of a digital copyright can only be prevented, if a forger cannot produce a valid copyright code. Second, the basic nature of digital images ensures that the copyright label can be easily altered if an attacker can identify the label data. Third, most digital images found in a multimedia environment can be low pass filtered, transformed to a different format or color space, or carefully re-quantized and compressed without significantly altering the images appearance or affecting its value. Finally, the image data is the only random sequence available to mask the data, and the statistics of the images, although generally unknown, are not under the control of the copyright system.

In sum, each of these points represents a potential means of attacking the copyright label and the following functional specifications are designed to prevent these attacks:

(1) A secret key type encryption code must be created using the unique identification of a work and used as the copyright label to prevent forgery of labeling.

(2) The image data must camouflage the copyright label code both visually and statistically to prevent an attacker from finding and deleting it. The functional requirement stating that the copyright label appears to be part of a normal image sequence and visually transparent is designed to prevent this attack.

(3) The signals used to embed the copyright label must contain a noise margin to resist damage if the image is processed or compressed.

(4) The system must be designed in such a way that the copyright labels locations and the same copyright code are not used repeatedly for embedding codes in different images to prevent the label from be found by comparing different images signed by the same owner.

The noise margin created by modeling the lossy compression allows for some loss of energy in the pulse, before the pulse becomes unreadable. Therefore if the pulse energy is concentrated at low frequencies, the embedded code should be relatively robust. Unfortunately, the final consideration with regard to pulse design and visual camouflaging, is in direct conflict with using low frequency pulse shapes. Specifically, it is widely accepted that noise in the low frequencies components of images is more noticeable than noise in the high frequency components. This is the basic concept behind the very efficient transform and sub-band coding techniques [8-10]. A reasonable trade-off between protection against processing attacks and visibility of the embedded code, is to make the pulses bandpass processes. Some additional design criteria must be developed to allow both requirements to be met simultaneously.

3 System Framework

The proposed approach, called Randomly Sequenced Pulse Position Modulated Code (RSPPMC) copyright labeling, is rooted in the well-known fact that typical digital images of people, buildings and natural settings can be considered as non-stationary statistical processes, which are highly redundant and tolerant of noise [8]. Hence, changes in the image data caused by moderate levels of wideband noise or controlled loss of information are hardly visibly noticeable, even when the altered images are compared directly with the original images.

Furthermore, the statistics of image sequences are only locally stationary and apriori unknown. More importantly, the process which produces such a sequence has random properties, which prevent the sequence from being reproduced exactly by a second experiment. This type of random signal is ideally suited for the purpose of statistically masking a sparse sequence of moderately large pulses.

The RSPPMC method consists of splitting the problem into two components. The first component produces the actual copyright code and a random sequence of locations for embedding the code in the image. This component is designed with the intention of implementing it, using existing encryption and pseudo random number generation techniques [11,12]. In fact, these methods are only discussed to establish a framework for developing a novel technique for embedding data in images. The second component actually embeds the code at the specified locations, using a simple pulsing method, designed to appear to be a natural part of the image, which yet resists being damaged through simple processing techniques. This component consists of four steps:

(1) The position sequence is used to generate a sequence of pixel mapped locations where the code will be embedded.

(2) The blocks of 2-D image data, y(k,l) where k,l are the indices of discrete image points, are locally transformed and quantized at the locations selected in step 1, in a manner reflecting acceptable information loss in the image for the application to produce a 2-D image residual, n(k,l), in which the RSPPMC will actually be embedded.

(3) The code pulses, i.e. high or low, representing the binary code being embedded, are superimposed on the signal n(k,l) selected locations.

(4) The quantized data is decoded; and then, inversely transformed to produced the labeled image data.

In order to comply with functional requirements related to robustness, the transformation used in the second step includes the color space transformations and sub-banding and/or frequency transformations to allow direct access to the appropriate frequency bands in the gray scale component of an image. A quantization process is included in this step to guarantee that the label will survive a specific amount of information loss. A JPEG Compression Standard Based RSPPMC Copyright Label will be described in the next section.

4 Embedding a RSPPMC in Quantized JPEG Coefficients

Considering the functional requirement of robustness in a multimedia environment, the loss model in step 2 of the label process should be based on an industrial standard. From this perspective, image compression schemes used in GIF, TIFF, MPEG and JPEG are of interest. However, the wide spread use and growth of the JPEG [9] and MPEG formats and their efficiency in compressing images make transform coding the obvious choice for designing a copyright labeling system. Also, transform coding and/or sub-band coding techniques have the advantage of allowing direct access to specific frequency bands in the image, where the RSPPMC is to be embedded. This eliminates the problem of designing and detecting bandpass wavelets.

The basic characteristics of images, which make transform quantization a useful image data compression tool are (1) images are generally low pass processes, and (2) high frequency image components have little visual impact.

The DCT representation of images has been widely researched [10]. The typical characteristics of image DCT's are also well known. Readers unfamiliar with the DCT and image transform quantization should refer to [8-10] for details.

The second point allows the higher frequency coefficients to be more coarsely quantized than the low frequency components by the transform quantizer. Predictably, the JPEG transform quantizer utilizes this fact by increasing qs(k,l) as a function of the increasing frequency vector normal.

Using these assumptions, several signals can be derived from the image data Y(i,j), which naturally contain pulses meeting the requirements outlined in section 2. One of the simplest is the sub-block signal,

$$N(k_1,l_1,k_2,l_2) = |Y_Q(k_1,l_1)| - |Y_Q(k_2,l_2)| \qquad (1)$$

where $Y_Q(k_1,l_1)$, $Y_Q(k_2,l_2)$ are the quantized coefficient values at the selected locations. This non-stationary random process should have an expected value of approximately zero if $|k_1,l_1|$ is approximately equal to $|k_2,l_2|$. Also, the signal should have a moderate variance level in the middle frequency ranges, i.e. $1.5 < |k,l| < 4.5$, where scattered changes in the image data should not be noticeably visible. The specific frequencies being used to embed the pulses will be "hopped" in this range to increase the robustness of the signal and making it more difficult to find. The principle being employed here is identical to the concept of frequency hopped spread spectrum communications [13].

A logical choice for the detection of "highs" and "lows", based on the signal defined in (1) is decided high if:

$$N(k_1,l_1,k_2,l_2) > 0, \qquad (2a)$$

and decided low if,

$$N(k_1,l_1,k_2,l_2) < 0. \qquad (2b)$$

However, embedding the code in this signal must also take into account the JPEG quantization process and any noise margin added to the pulses in the code. Therefore, the test for a written high is set as:

$$|Y_Q(k_1,l_1)| > |Y_Q(k_2,l_2)| + p, \qquad (3a)$$

where p is a noise margin factor. The corresponding equation for a written low is:

$$|Y_Q(k_2,l_2)| > |Y_Q(k_1,l_1)|+p. \qquad (3b)$$

Standard JPEG compression uses a ”quality factor” to scale the quantization, allowing for different image qualities and compression factors. In order to guarantee that the copyright label will survive compressions up to a specific level compression, the quantization table should be scaled to the desired quality factor. Also, due to numerical problems (in calculating quantization step size according to quality factor, and in the quantization process) which can occur if the image is quantized with a JPEG quality greater than the designed factor for embedding the copyright code, some conditions must be be met. They are not discussed in this paper because of the limited space.

The method used to embed the copyright label in the sequence, $N(k_1,l_2,k_1,l_2)$, is not complicated. The high/low pulse pattern of the copyright label code is forced on the natural sequence at the selected group locations using a minimum mean square error approach, if it does not occur naturally. More complicated pulse pattern may be developed for representing the high/low bit, e.g. to use combinations (i.e. relationships) of three quantized elements $Y_Q(k_1,l_1)$, $Y_Q(k_2,l_2)$, $Y_Q(k_3,l_3)$ to replace equation (3).

In summary, the random pulse signal and conditions for detecting naturally occurring highs and lows described in equations (1) - (3) are designed to survive a JPEG compression down to a specified quality level. Clearly, decreasing the quality factor for the copyright code will make the signal more robust. However, this will also reduce the number of naturally occurring bits in the sequence. In addition, a lower quality factor will increase the likelihood that the changes necessary to superimpose the embedded code on the signal will be noticeably visible.

5 Conclusions

Using the prototypes we have developed, the experimental results indicate that the design requirements, developed in sections 2 for embedding a copyright label in image data, can be met, using the JPEG model based RSPPMC method developed in section 4. In particular, it was demonstrated that a copyright label code could be embedded in several images, using pulses with sufficient noise margins to survive common processing, such as lossy compression, color space conversion, and low pass filtering. However, these results also indicate significant room for improvement in the method. One possibility for improvement could be to use different frequency band sets for encoding the high and low pulses. Also, methods could be developed to utilize image restoration techniques and pattern recognition techniques for verifying copyright labels. For example, pattern recognition techniques could be used to read copyright labels from images which have been cropped. In addition, methods suitable for applications with special requirements, such as cartography and medical imaging, are currently being investigated.

The authors would like to acknowledge Scott Burgett and Jochen Rindfrey, for their contributions to this work.

References

[1] B. Kahin, ”The strategic environment for protecting multimedia”, IMA Intellectual Property Project Proceedings, vol. 1, no.1, 1994. pp.1-8.

[2] E. Koch, J. Rindfrey, J. Zhao. ”Copyright Protection for Multimedia Data”, *Proceedings of the International Conference on Digital Media and Electronic Publishing* (6-8 December 1994, Leeds, UK).

[3] B.A. Lehman, R.H. Brown, “Intellectual Property and the National Information Infrastructure”. Preliminary draft of the working group on intellectual property rights, July 1994.

[4] G. Van Slype. Natural language version of the generic CITED model. ESPRIT II CITED Project 5469, June 28, 1994.

[5] A.J. Kitson and D.T. Seaton (eds.). Copyright Ownership Protection in Computer Assisted Training (COPICAT), Esprit Project 8195, Workpackage 2 (Requirements Analysis), Deliverable 1, June 2, 1994.

[6] RACE M 1005: Access control and copyright protection for images (ACCOPI), Workpackage 1 Deliverable, July 1994.

[7] K. Mantusi and K. Tanaka, ”Video-Steganography: How to secretly embed a signature in a picture,” *IMA Intellectual Property Project Proceedings*, vol. 1, no. 1, 1994.

[8] A. K. Jain, *Fundamentals of Digital Image Processing*, Prentice Hall, Englewood Cliffs, NJ, 1989.

[9] G.K. Wallace, ”The JPEG still picture compression standard”, *Communications of the ACM*, vol. 34, no. 4, April 1991. pp.30-40.

[10] K.R. Rao and P. Yip *Discrete Cosine Transform: Algorithms Advantages, Applications*, Academic Press. 1990.

[11] G. J. Simmons, *Contemporary Cryptology: The Science of Information Integrity*, IEEE Press, New York, 1994.

[12] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Son, Inc., New York et al., 1994.

[13] R. C. Dixon, *Spread Sprectrum Systems*, 2nd ed., Wiley, New York, NY, 1984.