Tamper Detection in Color Image

Ali Kadhim Mousa*

Date of acceptance 17/2/2008

Abstract

In this work a fragile watermarking scheme is presented. This scheme is applied to digital color images in spatial domain. The image is divided into blocks, and each block has its authentication mark embedded in it, we would be able to insure which parts of the image are authentic and which parts have been modified. This authentication carries out without need to exist the original image. The results show the quality of the watermarked image is remaining very good and the watermark survived some type of unintended modification such as familiar compression software like WINRAR and ZIP

Introduction

Tamper becomes easier and easier with digital images in ways that are difficult to detect. For example it is hard to judge whether Fig.1 or Fig.2 is the trustworthy photograph

(Image by Ching-Yang Lin, see http:/www.ctr.columbia.edu/"cylin/auth/auth.html.).

Fig.1 is the original image, Fig.2 is the modified version; the head of Hillary has changed by the head of Monica by using one of available image processing programs. Some kinds of images are a critical piece of evidence in legal cases or police investigations, these forms of tampering might pose serious problems. A preferable solution might be to embed the signature directly into the image using watermarking [1]. We refer to such an embedded signature as an *authentication mark*. Authentication marks designed to be invalid after even slightest modification of image which are called *fragile* watermarks [2]. Watermarking systems can be classified *robust* or *fragile.* Robust watermarks are required to resist any modifications which do not decrease the commercial value of the cover image. On the contrary, fragile watermarks are *designed to fail* when the cover image is modified. A fragile watermark is one designed so that it is not robust. For example, a watermark designed for authentication purposes should be fragile. Any signal processing applications applied to the image should cause the watermark to be lost [2]. An early attempt in the field of image authentication was the method proposed in [3] where the checksums of digital images were calculated and in combination with a seal produced the watermark information that was responsible for the authentication. This work excited the idea of digital image authentication and many researchers approached the problem from different and more sophisticated ways. Another method that is both efficient and easy to compute was proposed by Yeung and Mintzer [4]. According to that method a binary logo is embedded in an image in order to detect possible alterations in the image and at the same time provide some information about the image owner. A general overview of the digital watermarking systems and methods is given in [5], while a more specific overview of a method designed with the purpose to detect the alterations in digital images (tamper proofing) is given in [6].

* Department of Computer, College of Science for Women, Baghdad University

The present work belongs to the class of methods that embed a logo in the image once to detect the possible alterations of it. Instead of the binary logo of the company or organization to proof its authenticity, a reference numbers are embedded in image to localize the altered areas.

The paper is structured as follows: in section 2 the proposed method is presented. In section 3 measurements, a set of experiments and the corresponding results are given. Finally, in section 4 conclusions are drawn.

The proposed method

The color image is divided into blocks; (4x4) or (8x8) or (16x16) or (32x32) , each block has its authentication mark embedded in it, we would be able to gain an idea of which parts of the image are authentic and which parts has been modified. Address numbering is used as authentication mark to identify the blocks of image. If the image is divided into (8x8) blocks then authentication mark will be 1, 2, 3…..64. Each number refers to location in image as shown in fig [5].

Let *B* be a block of *MxN* pixels. Each pixel value is given by the composition of the three color components *Red*, *Green* and *Blue* that are considered as *MxN* 8-bit matrices. The authentication mark, in binary form, is embedded in several pixels of one color component, in a way that 1 bit of host image is replaced by one bit of authentication mark. Let $B(i,j)$, $i=0,1,\ldots,M-1$, $j=0,1,\ldots,N-1$ be an 8-bit pixel value of the blue component. Embedding one bit of authentication mark into one of the first four LSB according to embedding function f_B. Several functions f_R, f_G, f_B can be used to embed information in one of the three color components in order to increase the secrecy. The positions of the watermarked pixels are selected to be spread along predefined block size according to a secret key that is necessary for the watermark extraction process. If the block(s) containing an authentication mark is modified, the mark is modified with it. The extraction process is similar to the watermarking process. The secret key is used in order to define the marked pixel positions that have been modified. The modified pixel values are extracted and tested using the function *f* in order to extract the embedded bit. Then the extracted authentication mark is compared with the image regions addresses that are supposed to be the same. The alterations in the authentication mark can be clearly identified, and the tampered areas are localized.

Measurements & Results

1. Quality Metrics Measurement

Techniques

For fair benchmarking and performance evaluation, the visual degradation due to the embedding is an important issue. Most distortion measures or quality metrics used in visual information processing, belong to the group of difference measures [7]. These measures are all based on the difference between the original, (undistorted) and the modified (distorted) image.

When we refer to a "perceptual model", we mean more precisely a function that gives a measure of distance between the original image, *O*, and the watermarked image, *R*. One of the simplest distance functions is the mean squared error (MSE). This is defined as :

$$MSE = \frac{\sum_{x,y}[O(x,y) - R(x,y)]^2}{W * H}$$

Where $O(x,y)$ represents a pixel, whose coordinates are (x,y), in the original (modified image), and $R(x,y)$ represents a pixel, whose coordinates (x,y), in the watermarked image. *W* & *H* represent the width and height of the image respectively [8].

Nowadays, the most popular distortion measure in the field of image and video coding and compression is the *Peak Signal to Noise Ratio (PSNR).* Its popularity is very likely due to the simplicity of the metric [8]. It is defined as:

$$PSNR = 10\log_{10}\frac{(255)^2}{MSE}$$

2. Results

In this section some results are gained. Fig 3 shows an original image of military airplane labeled with (IRAQ AIR FORCE). Fig 4 shows the process of embedding the authentication mark by dividing the image into (8x8) blocks. The watermarked image is illustrated in Fig5. In Fig 6 (**Q**) is altered to (**N**); the label (**IRAQ AIR FORCE**) changed to (**IRAN AIR FORCE**). Fig7 & Fig8 show the modified regions of image after applying watermark extraction on it. We can notice the blocks 28&29 are coarse to define the specific altered regions. If we increase the number of blocks by repartioning the image into (32x32) blocks, then finer altered regions can defined, here just the blocks contain letter (**N**) are signed, as shown in Fig 9 & Fig 10.

We have to notice that as we increase the number of partions, the payload of authentication mark is increase that will lead to degradation in the quality of marked image but finer altered regions can be specified. And as we shift the host bit from first LSB to left we increase the robustness of authentication mark but the quality of marked image decreases. Table 1 shows some ***PSNR*** measurements result from applying the suggested method on an image illustrated in Fig 3 by using various number of partions with variable host bit location. The quality of the marked image is very high because the watermark information affects at the most the 4 LSB's. Experimental results give PSNR measurements much higher than 38 dB [9]. This is considered as very acceptable, since the casual observer cannot notice any visual differences between the original and the watermarked image.

Conclusion

In this paper a watermarking method for authentication purposes was presented. The method is authenticating a specific region of a digital color image. The quality of the watermarked image is remaining very good since the method affects not more than four of the least significant bits of one color component. The authentication mark extracted successfully when watermarked image exposed to some type of famous compression software like WINRAR and ZIP. The proposed method is very fast, thus providing the advantage of using it for the authentication of large volumes of digital images.

Table 1: PSNR Values for various number of partions with variable host bit location

Bit Position	Number of Partions			
	4 x 4	**8 x 8**	**16x16**	**32x32**
1st	80.98	75.22	65.99	59.17
2nd	75.22	67.77	60.22	53.18
3rd	69.78	61.07	54.08	47.17
4th	62.32	55.20	48.04	41.10

References

1- Macq, B. M. 1995 "*Cryptography for Digital TV Broadcasting*". Proceedings of the IEEE, 83(6):944-957.

2- Cox, I. j. 2002."*Digital watermarking*". Morgan Kaufmann Publisher, USA.

3- Walton, S. 1995."*Image Authentication for a Slippery New Age*". Dr. Dobb's Journal of Software Tools for Professional programmers, Vol. 20, Apr.

4- Yeung, M. and F.Mintzer, 1997. "*An Invisible Watermarking Technique for Image Verification*".Proc. ICIP '97, Santa Barbara, California.

5- Katzenbeisser, S. and F.A.P.Petitcolas, 2000. "*Information Hiding Techniques for Steganography and Digital Watermarking*" Artech House.
6- Fridrich,J. 1999."*Methods for Tamper Detection in Digital Images*". Multimedia and Security ,Workshop at ACM Multimedia 99, Orlando, FL, USA.
7- Khalid Sayood. 1996. "*Introduction to Data Compression*". Morgan Kaufmann Puplisher, USA.
8- D.Kundur and D. Hatzinakos. 1999. "*Attack Characterization for Effective Watermarking*". Proc. Of 99 Int. Conf. on Image Processing, 2:240-244.
9- Katzenbeisser, S. and A.P. Petitcolas, 2000. "*Information Hiding Techniques for Steganography and Digital Watermarking*". Artech House, Inc.

Fig 1: Clinton and Hillary

Fig 2: Clinton and Monica

Fig 3: original military airplane image

Fig 4: dividing image into (8x8) blocks

Fig 5: watermarked image

Fig 6: modified image

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	*28*	*29*	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Fig 7: authentication marks

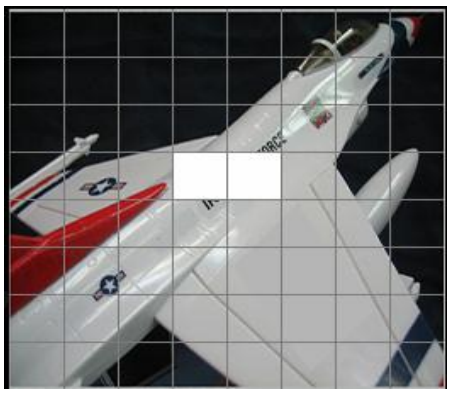

Fig 8: modified regions

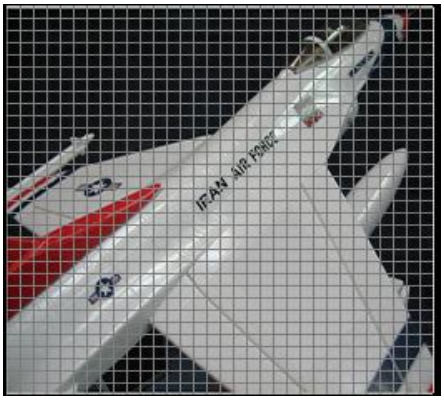

Fig 9: dividing image into (32x32) blocks

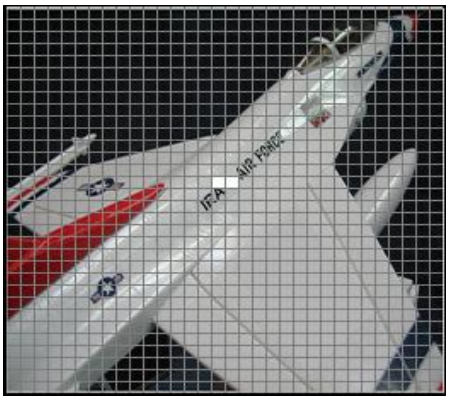

Fig 10: modified regions

أكتشاف التلاعب في الصور الملونة

علي كاظم موسى*

* مدرس/قسم الحاسبات /كلية العلوم للبنات /جامعة بغداد.

الخلاصة:

هذه الورقة البحثية نقدم طريقة لتطبيق العلامة المائية (سهلة الكسر) على الصور الرقمية الملونة . نقوم بتقسيم الصورة إلى عدد من المساحات المحددة . كل مساحة تُطمر فيها علامة مميزة (غير مرئية) تفيدنا لاحقاً في التأكد من شرعية الصورة وتحديد أي المساحات لم يتم التلاعب بها وأي المساحات جرى تبديل عليها.

عملية التأكد من شرعية الصورة وتحديد المساحات التي جرى التلاعب بها تنجز دون الحاجة الى وجود الصورة الأصلية. أظهرت النتائج جودة عالية في الصور المعلَّمة بالعلامة المائية المقترحة إضافة إلى مقاومتها للتبديلات غير المقصودة كالبرمجيات المألوفة لضغط الملفات.