COPYRIGHT PROTECTION OF IMAGES USING ROBUST DIGITAL SIGNATURES

Nikos Nikolaidis[1] *Ioannis Pitas*[2]

[1]Dept. of Electrical & Computer Engineering, University of Thessaloniki, Thessaloniki 540 06, GREECE
[2]Dept. of Informatics, University of Thessaloniki, Thessaloniki 540 06, GREECE, pitas@zeus.csd.auth.gr

ABSTRACT

A method for copyright protection of digital images is presented in this paper. Copyright protection is achieved by embedding an "invisible" signal, known as *digital signature*, in the digital image. Signature casting is performed in the spatial domain by slightly modifying the intensity level of randomly selected image pixels. Signature detection is done by comparing the mean intensity value of the marked pixels against that of the not marked pixels. Statistical hypothesis testing is used for this purpose. The signature can be designed in such a way that it is resistant to JPEG compression and lowpass filtering. This is done by minimizing the energy content of the signature signal in higher frequencies. Experiments on real image data verify the effectiveness of the method.

1. INTRODUCTION

Digital storage, transmission and manipulation of video signals and still images exhibited a tremendous growth in the last few years, mainly due to the expansion of computer networks and the introduction of multimedia technologies to the information market. With digital television being not so far away, one can expect that digital video will be a hot research topic for the years to come. Following this trend, copyright protection of the stored/transmitted digital images will become a very important issue. One way to protect images against illegal recordings and retransmissions is to embed a signal, called *digital signature* or *copyright label* or *watermark*, that completely characterizes the person who applied it and, therefore, marks it as being his intellectual property. Digital signatures [1] should be :

- undeletable by an "attacker"
- easily and securely detectable by their owner
- perceptually and statistically invisible
- resistant to lossy compression, filtering and other types of processing.

Devising an algorithm capable of producing signatures that fulfil all these contradicting requirements is not an easy task. A number of attempts to introduce copyright labelling techniques that comply with some or all of the above specifications have been reported lately in the literature [2]-[5]. However research on copyright protection of images is still in its early stages and none of the existing methods is totally effective against attacks. In this paper we extend the algorithm proposed in [4] towards signatures that are robust to JPEG compression and to other possible "attacks" such as median and lowpass filtering. The outline of this paper is the following. The basic algorithm is described in Section 2. Design of signatures that are robust to filtering and compression is discussed in Section 3. Experiments on real image data are presented in Section 4.

2. ALGORITHM DESCRIPTION

Consider an image of dimensions $N \times M$ represented as follows :

$$I = \{x_{nm}, n \in \{0, ..., N-1\}, m \in \{0, ..., M-1\}\} \quad (1)$$

where $x_{nm} \in \{0, 1, \ldots, L-1\}$ is the intensity level of pixel (n, m). A signature pattern S is a binary pattern of the same size where the number of "ones" equals the number of "zeros":

$$S = \{s_{nm}, n \in \{0, ..., N-1\}, m \in \{0, ..., M-1\}\}, \quad s_{nm} \in \{0, 1\}. \quad (2)$$

It is obvious that, in order to be used for copyright protection, the signature pattern should be known only to the signature owner. Using S we can split I in two subsets of equal size :

$$\begin{aligned} A &= \{x_{nm} \in I,\ s_{nm} = 1\} && (3)\\ B &= \{x_{nm} \in I,\ s_{nm} = 0\} && (4)\\ |A| &= |B| = \frac{|I|}{2} = \frac{N \times M}{2} = P && (5)\\ I &= A \cup B && (6) \end{aligned}$$

The digital signature is superimposed on the image as follows :

$$C = \{x_{nm} \otimes k,\ x_{nm} \in A\} \quad (7)$$

where $\otimes$ is a superposition law. The signed image is then given by:

$$I_s = C \cup B. \quad (8)$$

The signature can be considered as a two-dimensional signal f_{nm} :

$$f_{nm} = \begin{cases} k & , s_{nm} = 1 \\ 0 & , s_{nm} = 0 \end{cases} \quad (9)$$

Let us denote by $\bar{a}$, $\bar{b}$, $\bar{c}$ and s_a, s_b, s_c the sample mean values and the sample standard deviations of the pixels belonging to the subsets A, B, C, respectively. Signature detection is based on the examination of the difference $\bar{w}$ of the mean values $\bar{c}$, $\bar{b}$:

$$\bar{w} = \bar{c} - \bar{b}. \quad (10)$$

If the image has been signed then $\bar{w}$ is close to k whereas in the case of an unsigned image or an image bearing a signature different from the one that we are looking for, $\bar{w}$ is approximately zero. In other words, $\bar{w}$ is a random variable whose mean is zero for an unsigned image and k for an image that has been signed. The decision on whether the image is signed or not is taken using hypothesis testing. The test statistic q that has been used is given by [6] :

$$q = \frac{\bar{w}}{\hat{\sigma}_{\bar{w}}} \quad (11)$$

where :

$$\hat{\sigma}_{\bar{w}}^2 = \frac{s_c^2 + s_b^2}{P}. \tag{12}$$

The Null and the Alternative Hypotheses in this case are :

H_0**:** There is **no** signature in the image.

H_1**:** There **is** a signature in the image.

Under the null hypothesis the test statistic q follows a zero mean Student distribution with $(2P-2)$ degrees of freedom. In order to decide whether the image is signed or not, the value of q is tested against a threshold t. If $q > t$ we assume that the image is signed, otherwise we conclude that the image bears no signature. The threshold $t_{1-\alpha}$ that minimizes both the type I error (accept the existence of a signature although there is none) and the type II error (reject the existence of a signature although there is one) is given by :

$$t_{1-\alpha} = \frac{k}{2\hat{\sigma}_{\bar{w}}}. \tag{13}$$

This value of $t_{1-\alpha}$ corresponds to a specific certainty level $(1-\alpha)$ i.e. a probability of correct signature detection. Solving for k we obtain the relationship:

$$k = \lceil 2\hat{\sigma}_{\bar{w}} t_{1-\alpha} \rceil. \tag{14}$$

Therefore, during the signature superposition we can specify the degree of certainty $(1-\alpha)$ which we want to have during the signature detection phase and, using (14), obtain the value of k that will lead to this desired value. In conclusion, the proposed algorithm can be summarized as follows :

Signature casting : Generate S. Decide for the desired certainty level, calculate k using (14) and cast the signature using (7), (8).

Signature detection : Generate S. Evaluate q using (10)-(12) and compare it with $t_{1-\alpha}$ to decide for the signature existence.

The above method leads to signatures that ensure safe detection with minimum visual distortion. For example, by using a value of $k = 3$, i.e., a value that is practically invisible when superimposed to half of the (randomly selected) image pixels (MSE between the signed and the original image: 4.5), we can obtain a probability of correct detection 99.98% (test image: Lenna).

3. ROBUST SIGNATURE DESIGN

Unfortunately the method outlined in the previous section is not robust to compression using the well-established JPEG standard which achieves efficient image compression by combining the Discrete Cosine Transform (DCT) with appropriate DCT coefficient quantization schemes. This is due to the fact that the signature signal f_{nm} described in the previous section is essentially a low-power, high-frequency noise. As a consequence, it is heavily distorted by JPEG, which allocates less bits to higher DCT frequencies. Furthermore, the signatures can be easily deleted by other lowpass operations such as mean or median filtering. In the following we propose two methods to design signatures that can withstand big compression ratios and lowpass operations without being deleted. Both techniques reduce the energy content of the signature signal in high frequencies, thus providing immunity from lossy compression and filtering.

The first way to achieve compression robustness is by using signatures where the signed pixels, i.e. the pixels in A, form blocks of a certain size, e.g. 2×2 or 3×3. For instance, instead of randomly selecting P of the image pixels for marking, one can alternatively choose $P/4$ randomly positioned blocks of size 2×2. It is obvious that since the number of signed pixels equals P this variation behaves exactly like the algorithm described in Section 2 with respect to the detection phase. However the new signature signal is more "lowpass" and thus it can endure much higher JPEG compression. The bigger the block size, the more robust to compression the signature becomes. Unfortunately, by using big blocks visually distinguishable signatures can result.

The second method to design signatures robust to compression exploits the fact that the detection algorithm described in Section 2 is based on the difference $\bar{w}$ of the mean values $\bar{c}, \bar{b}$ in order to decide for the existence of a signature. Therefore, the detection algorithm will give the same results if, instead of superimposing the same constant k to all the pixels in A, we use a different value k_{nm} for each signed pixel, provided that the sum $\sum\sum f_{nm}$ is kept the same :

$$\sum_{n=0}^{N-1}\sum_{m=0}^{M-1} f_{nm} = Pk. \tag{15}$$

This versatility in the choice of k_{nm} enables us to design signatures that are of low energy content in the higher DCT frequencies. The approach used to design such a signal is the following. First, the signature pattern S is produced and a value for k that will lead to the desired certainty level is chosen according to (14). The signature signal f_{nm} is then divided into blocks of size 8×8 in the same way as in the DCT algorithm and the optimum values k_{nm} are separately calculated for each block. Suppose that the number of the signed pixels within a certain block D is r and that f_{nm}^D $(n, m = 0 \ldots 7)$, F_{uv}^D $(u, v = 0 \ldots 7)$ denote the signature signal in the spatial and the DCT frequency domain respectively. F_{uv}^D is given by [7] :

$$F_{uv}^D = \tag{16}$$
$$\tfrac{1}{4}C(u)C(v)[\textstyle\sum_{n=0}^{7}\sum_{m=0}^{7} f_{nm}^D cos\frac{(2n+1)u\pi}{16} cos\frac{(2m+1)v\pi}{16}]$$

where $C(u)$ are appropriate scale coefficients. The design of a low frequency signature signal can be achieved by minimizing the following energy function with respect to $k_{nm},\ n, m \in D$:

$$\Phi = \sum_{u,}\sum_{v \in H} (F_{uv}^D)^2 \tag{17}$$

where H is some user-selected set of higher frequencies, e.g :

$$H = \{u, v:\ 4 < u \leq 7 \quad or \quad 4 < v \leq 7\}. \tag{18}$$

Minimization of Φ should take into consideration the following constraints :

1. k_{nm} should be chosen so that (15) holds for the whole image. This can be achieved by enforcing the following constraint to the signature values inside the block D :

$$\sum_{n=0}^{7}\sum_{m=0}^{7} f_{nm}^D = rk \tag{19}$$

2. k_{nm} should lie within a certain range so that the signature remains perceptually unnoticeable :

$$k_{min} \leq k_{nm} \leq k_{max} \tag{20}$$

For example if $k = 3$ then a suitable choice for k_{min}, k_{max} could be $0, 6$ respectively.

As can be seen from (16), (17), Φ is quadratic in k_{nm}. Therefore finding the values of k_{mn} that minimize (17) under the previous constraints is a quadratic minimization problem which has been solved using quadratic programming techniques [8]. The signatures produced this way comprise of smooth geometrical shapes instead of impulses. It should be noted that the optimization procedure is image independent and needs to be performed only once for a specific signature and image size. Furthermore, the two methods proposed in this section can be easily combined to achieve robustness to even bigger compression ratios.

The effect of the optimization algorithm on the signature signal is illustrated in Figures 1, 2. Fig. 1 shows the signature signal within a 8×8 block when a constant value of $k = 3$ is used and the signature pixels are chosen so as to form 2×2 blocks. The number of signed pixels in the 8×8 block for this particular case is $r = 28$. The optimized signature using the proposed algorithm with $k_{min} = 0$, $k_{max} = 6$ and H given by (18) can be seen in Fig. 2. The new signature "fades" smoothly to zero and, therefore, its energy content in the higher DCT frequencies is limited. Note that although some of the signature pixels have been set to zero the sum of the signature signal values is the same with that of the signal in Fig. 1.

4. EXPERIMENTAL RESULTS

The resistance of the proposed signature casting algorithms to lossy JPEG compression was tested by applying them on many images, e.g. the test image "Lenna" (Fig. 3) and finding the maximum compression that allows signature detection. It must be noted here that, for a given image, the maximum compression that the signatures can withstand is not the same for all the signature patterns. The maximum compression depends on the value of $\bar{w}$ for the signature under examination. Signatures with big value of $\bar{w}$ are less vulnerable to compression. The compression ratios presented in the sequel refer to a signature where $\bar{w}$ is very close to k.

The test image signed with the signature described in Section 2 and $k = 3$ can withstand compression only up to $1 : 4.5$ before the signature becomes undetectable. However, using the signature optimization algorithm with $k = 3$, $k_{min} = 0, k_{max} = 6$ and H given by (18) the signature remained intact even after the image has been compressed down to $1 : 8.2$. Using the first technique in Section 3 with block size 2×2 and a constant value of k equal to 3, we were able to obtain signatures that were not deleted even if a compression ratio of $1 : 15.5$ was used. The best results were obtained using a combination of these techniques, i.e. signing the image using 2×2 blocks and then optimizing the signature using $k = 3$, $k_{min} = 0, k_{max} = 6$ and H given by (18). Using this technique we obtained signatures able to withstand compression up to $1 : 24$. Furthermore, the signatures designed this way survived 3×3 mean and median filtering. The signed image using the last technique can be seen in Fig. 4. The alternations to the image are barely visible. The JPEG compressed image using the maximum compression i.e $1 : 24$ can be seen in Fig. 5. Note that although the image is rather severely distorted, the signature is still detectable.

An implementation of this algorithm in executable form can be downloaded from the ftp site *poseidon.csd.auth.gr* (directory /pub/digital.signatures) by anonymous ftp and can be used as shareware for signing digital pictures.

5. CONCLUSIONS

A new method for the copyright protection of digital images using digital signatures has been proposed in this paper. The proposed method produces signatures that are not detectable by visual inspection but in the same time are robust to JPEG compression and lowpass filtering. Variations that produce signatures that are immune to geometric transformations and also image-dependent are currently under investigation.

REFERENCES

[1] B. M. Macq, J. J. Quisquater, "Cryptology for Digital TV Broadcasting", Proceedings of the IEEE, pp. 944-957, June 1995.

[2] E. Koch, J. Zhao, "Towards robust and hidden image copyright labelling", *Proc. IEEE Workshop on Nonlinear Signal and Image Processing*, I. Pitas editor, pp. 452-455, 1995.

[3] O. Bruyndonckx, J.J. Quisquater, B. Macq, "Spatial method for copyright labelling of digital images", *Proc. IEEE Workshop on Nonlinear Signal and Image Processing*, I. Pitas editor, pp. 456-459, 1995.

[4] I. Pitas, T. Kaskalis, "Applying signatures on digital images", *Proc. IEEE Workshop on Nonlinear Signal and Image Processing*, I. Pitas editor, pp. 460-463, 1995.

[5] R.G. van Schyndel, A.Z. Tirkel, C.F. Osborne, "A digital watermark", *Proc. IEEE International conference on Image Processing*, vol. 2, pp. 86-89, 1994.

[6] A. Papoulis, *Probability & Statistics*, Prentice Hall, 1990.

[7] G. K. Wallace, "The JPEG still picture compression standard", IEEE Transactions on Consumer Electronics, vol 38, pp. 18-34, February 1992.

[8] G. R. Walsh, *Methods of Optimization*, Willey, 1975.

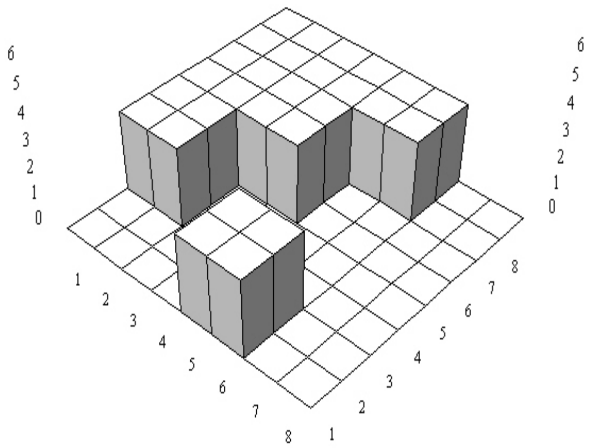

Figure 1. The signature signal within an 8×8 block when a constant value $k = 3$ is used.

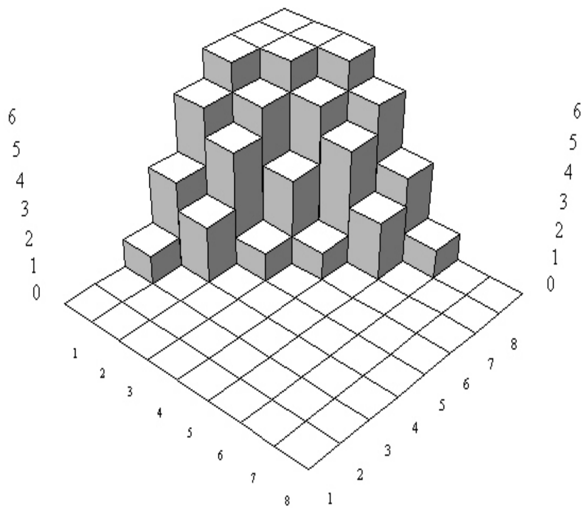

Figure 2. The same signal when the signal is optimized for low energy content in the higher frequencies.

Figure 3. Original image "Lenna".

Figure 4. Signed image "Lenna".

Figure 5. Signed image "Lenna" compressed using JPEG. Compression ratio 1:24. The signature is still detectable.