EMBEDDING ROBUST WATERMARKS BY CHAOTIC MIXING

G.Voyatzis and I. Pitas

Department of Informatics
University of Thessaloniki
Thessaloniki 54006, Greece
E-mail: voyatzis,pitas@zeus.csd.auth.gr

ABSTRACT

This paper presents a watermarking algorithm for copyright protection of digital images. A copyright label represented by a binary image is embedded in grayscale or color digital image. A mixing dynamical system controls embedding, detection and reconstruction of the copyright label. Detection of the watermark is succeeded either by direct reconstruction of the watermark as a binary image or by using statistical hypothesis testing.

1. INTRODUCTION

Copyright protection of multimedia products is an interesting research topic. The technology of multimedia services grows rapidly and distributed access to such services through computer networks is a matter of urgency. However, network access does not protect the copyright of digital products which can be reproduced and used illegally. An efficient way to solve this problem, is to use *watermarks* [1,2,3,4]. Watermark is a "secret" code described by a digital signal carrying information about the copyright property of the product. The watermark is embedded in the digital data such that to be perceptually unnoticed. The copyright holder is the only person who can show the existence of its own watermark and to prove the origin of the product.

This paper refers to digital grayscale or color image watermarking. For this important particular case, the following requirements should be satisfied by a watermarking algorithm :

1. Alterations introduced in the image should be perceptually invisible.
2. Watermark must be undetectable and not removable by an attacker.
3. A sufficient number of watermarks in the same image, detectable by their own key, can be produced.
4. The detection of the watermark should not require information from the original image.
5. Watermark should be robust as much as possible against attacks and image processing which preserves desired quality for the image.

The proposed watermarking algorithm satisfies the mentioned requirements (1)-(4) and uses a method to hide watermarks in the spatial domain, which shows high resistance to filtering and compression. Alterations take place directly on the intensity values of a greyscaled image or on the luminance component of a color image. The watermark is represented by a small, compared with the size of the image, binary image :

$$W = \{w_{kl} \mid 0 \leq k < M_1, 0 \leq l < M_2, w_{kl} = 0, 1\} \quad (1)$$

which is the owner's copyright signature or the authorized company's logo.

In the next section the algorithm is outlined. In section 3, the results of an extensive numerical study are represented, showing the robustness of the method under JPEG compression, median and moving average filters.

2. THE WATERMARKING ALGORITHM

Basic elements of the method are represented in [8] and a more detailed theoretical study will be presented in [9]. Next we outline the main steps of the procedures which should be followed for watermark embedding and detection.

2.1. Watermark embedding

Let I be a greyscale image or the luminance component of a color image of size $N_1 \times N_2$. An odd number of L binary watermarks W_i, identical to W, are placed side by side (horizontally and vertically) to produce a binary image W_L. The total number of pixels $\mathbf{r}$ of W_L should be smaller than the pixels of the image ($nM_1M_2 < N_1N_2$).

We select the image pixel locations $\mathbf{p}$, where the watermark will be embedded, by applying the 1-1 map :

$$\mathcal{F} : W_L \rightarrow I \ , \ \mathbf{p} = \mathcal{F}^n(\mathbf{r}; k_1, k_2, ..., k_m) \quad (2)$$

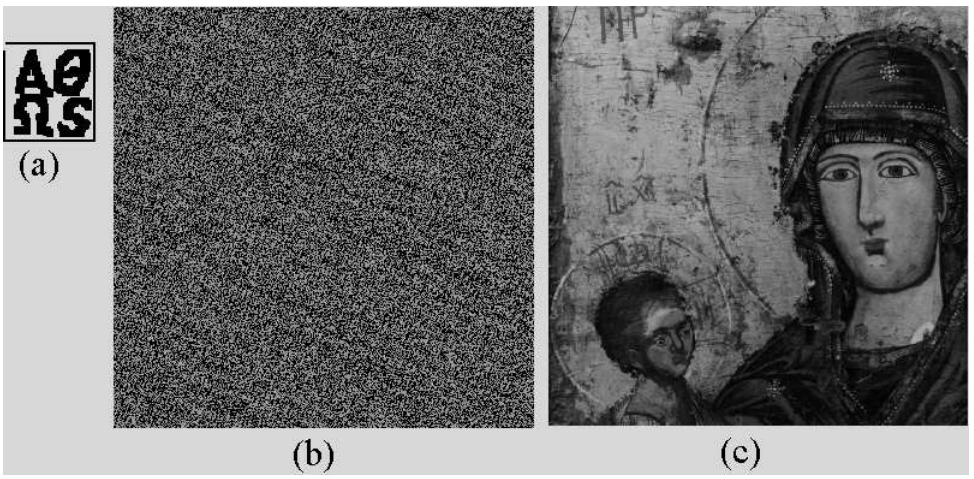

Figure 1: (a)The original watermark, (b) the global mask (scaled) (c) the original image

Figure 2: (a) the watermarked image (b)-(d) reconstructed watermarks by a JPEG compressed image (compression 5:1,10:1 and 15:1 respectively)

where k_i are integer positive parameters and n stands for iterative applications of the map. $\mathcal{F}$ is a mixing (strongly chaotic) two dimensional mapping in the real space, composed by linear operators and toral automorphisms [5]. In the space of an integer mesh (as e.g. the space of a digital image) $\mathcal{F}^T$ is periodic with periods T depend on the initial positions (pixels) [6]. However, for any finite integer mesh I and for any parameter set $\{k_i\}$ there exists a number P of iterations such that $\mathcal{F}^P(I) = I$ [7]. The inverse map $\mathcal{F}^{-1}$ exists always. The integer parameters k_i must follow some constrains (they are bounded in finite intervals). They are the owner's private *key* which is the necessary knowledge in order to proceed to the watermark detection.

We consider the following 5×5 mask for each image pixel $\mathbf{p}$:

$$\mathbf{M_p} = \begin{pmatrix} c_1 & c_2 & c_3 & c_2 & c_1 \\ c_2 & 0 & 0 & 0 & c_2 \\ c_3 & 0 & Q_{\mathbf{p}} & 0 & c_3 \\ c_2 & 0 & 0 & 0 & c_2 \\ c_1 & c_2 & c_3 & c_2 & c_1 \end{pmatrix} \qquad (3)$$

where c_1, c_2, c_3 are small constant values (≤ 4) and $Q_{\mathbf{p}}$ adapts to the image according to the formula :

$$Q_{\mathbf{p}} = f(x_{\mathbf{p}}\,,\, q\,;\, q_0\,) \qquad (4)$$

where f is a linear function, $x_{\mathbf{p}}$ denotes the intensity or the luminance value of the image pixel $\mathbf{p}$ and q depents on the average intensity or luminance of the pixels in the 3×3 block round $\mathbf{p}$. q_0 is a small constant (≤ 4) and its sign depends on the value (0 or 1) of the corresponding pixel $\mathbf{r}$ in the watermark. The sign of the parameters c_i should be $-sign(q_0)$.

A global mask of size $N_1 \times N_2$ is derived by considering all the local masks $\mathbf{M}$ and filling the complement

space by zeros :

$$\tilde{\mathbf{M}} = \bigcup_{\mathbf{p}} \mathbf{M} + \mathcal{O} \tag{5}$$

Finally $\tilde{\mathbf{M}}$ is superpositioned on the original image I to produce the watermarked image I' :

$$I' = I \oplus \tilde{\mathbf{M}} \tag{6}$$

2.2. Detection of the watermark

The detection of the watermark from the watermarked image I' can be done either by reconstructing the binary watermark W or by examining its existence by a statistical test. Next we consider a possibly modified watermarked image I'' (filtered or compressed).

The reconstruction of the watermark is based exclusively on the knowledge of the parameters k_i of the mixing map $\mathcal{F}$ (i.e. the key). For each pixel of I'' we examine the difference :

$$\Delta\mathbf{p} = x''_{\mathbf{p}} - \bar{x''}\mathbf{p} \tag{7}$$

We form a binary set Z of size $N_1 \times N_2$ by considering the value 1 if $\Delta\mathbf{p} > 0$ and 0 otherwise. Then by applying the inverse mixing map $\mathcal{F}^{-1}$ we get the binary image W''_L (which is the detected set W_L of the L identical watermarks W). If $I'' = I'$ then is also $W''_L = W_L$. The reconstructed watermark is formed pixel by pixel, by selecting the most frequent value of the L identical watermarks in W''.

A statistical detection can be applied by considering that the original watermark W and the key are known. We form the set W_L, as it is described above, which consists of two subsets W_0 and W_1 where $W_i, i = 0, 1$, contain the pixels of the binary set W_L which possess the value i. Then we calculate the means $\bar{\delta}_0$ and $\bar{\delta}_1$ of $\Delta\mathbf{p}$ for all pixels $\mathbf{p} \in I''$ which map, via $\mathcal{F}^{-1}$, into the space of W_0 and W_1 respectively

$$\bar{\delta}_i = \frac{1}{P_i} \sum_{\mathbf{p}} \Delta\mathbf{p}, \qquad \forall \mathbf{p}\ s.t.\ \mathcal{F}^{-1}(\mathbf{p}) \in W''_i \tag{8}$$

where $i = 0, 1$ and P_0, P_1 are the numbers of the pixels in the sets W_0 and W_1 respectively. When the watermarked image has not been modified somehow, then

$$\bar{\delta} = \bar{\delta}_1 - \bar{\delta}_0 \approx 2 \mid q_0 \mid \tag{9}$$

Generally, when the watermark does not exist in an image, $\bar{\delta}$ is expected to be close to zero. Thus we form the following hypothesis testing :

H_0 : There is no watermark ($\bar{\delta} = 0$)

H_1 : There is watermark ($\bar{\delta} \neq 0$)

Student's *t-test* can be applied in order to decide which hypothesis holds. The t-test statistic used is given by

$$t = \bar{\delta}/s_\delta \tag{10}$$

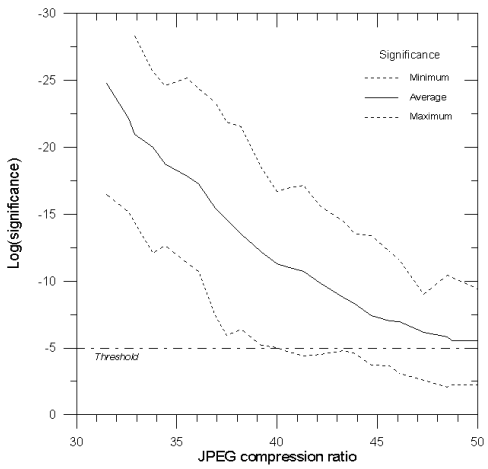

Figure 3: The statistical significance versus the JPEG compression of the image. Dotted line represents a threshold in order to accept the existence of a watermark "

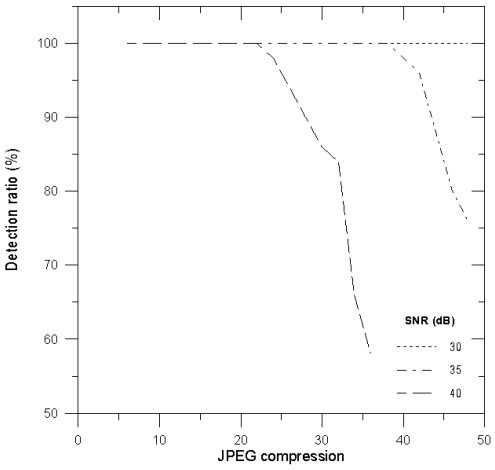

Figure 4: The performance of the algorithm under JPEG compression

where s_δ estimates the standard error of the difference of means [10]. The value of t is associated with the significance a of hypothesis H_0, i.e. the probability to accept H_1 although H_0 is correct. Thus $1 - a$ is the certainty for correct detection of the watermark. Since our decision should be quite strict, a should have quite small value or , equivalently, the certainty that the watermark indeed exist should be almost 1.

3. EXPERIMENTS

As an example the 60×60 watermark "ATHOS" shown in Fig 1a, has been used. The watermark W_L consists of $L = 31$ watermarks and by using the key

$$753 - 19 - 139 - 123 - 59 - 87$$

and parameters $\mid q_0 \mid = 4$, $\mid c_1 \mid = 2$, $\mid c_2 \mid = 2$, $\mid c_3 \mid = 3$, the mask $\tilde{\mathbf{M}}$ is formed (see Fig. 1b). $\tilde{\mathbf{M}}$ is added in the image of fig. 1c. The watermarked image is shown in Fig 2a. When the original watermarked image is

used, the watermark is perfectly reconstructed. However the watermark shows noise when the watermarked image has been modified somehow. Fig. 2(b-d) shows the watermarks reconstructed by compressed versions of the image. The watermark is well recognized even for quite high compression ratio.

We examined the performance of the method by watermarking five 24-bit RGB images of size 960×960 depicting portable Byzantine icons (Fig. 1c is included in the experiments). The watermark embedding took place on the 8-bit Y component by applying the "RGB to YUV" transformation. has been calculated from the original 24-bit RGB color images. In this case the statistical detection has been performed considering existence of the watermark when the certainty was greater than 99.999% (i.e. $a < 10^{-5}$). Ten (10) different keys (given by a random number generator under given constrains) have been used to watermark each one of the five images. The performance of the algorithm can be described by the *detection ratio* defined as follows

$$P = N_{detect}/N_{total} \tag{11}$$

where N_{detect} is the number of the correctly detected watermarks in N_{total} experiments. Each watermark was embedded such that to produce alterations providing SNR values 40dB, 35dB and 30dB approximately. The produced alterations can be manipulated by fixing properly the power of the watermark i.e. the parameters q_0, c_1, c_2, c_3 and L.

Fig. 3 shows the increase of the significance a (i.e. the decrease of the certainty for correct detection) versus the JPEG compression ratio and for the ten watermarks embedded in image of Fig 1c (SNR=35dB). We can observe that the watermarks are detected with great certainty up to high compression ratio. Figure 4 shows the performance of the algorithm of our total experiments. Up to 50:1 compression we have P=100% for SNR=30dB. However in this case the watermarked image shows slightly visible texture.

We applied the median and the moving average filters to the watermarked images. The performance P for filtering blocks of size up to 5×5 was almost 100%. We also applied the detection algorithm, without using the correct key, to find watermarks. For more than 1000 experiments the observed values of significance a were greater than 0.0005 and thus no watermarks were detected.

4. CONCLUSIONS

In this paper we outlined a watermarking algorithm which embeds robust watermarks (under filtering and compression) in greyscale or color images. The watermark is a small binary image (a logo) which represents the signature of the owner of the image. The watermark is hidden by using as a *key* a set of integer parameters which control a mixing map. The produced signal, which is added to the image, is not correlated significantly with other signals. Thus the watermark can be detected only by using the appropriate key and the mapping $\mathcal{F}$. The watermark can be reconstructed for JPEG compression up to 15:1 and also for 5×5 median and moving average filters. When large modifications take place on the watermarked image (e.g. low quality compression), the statistical hypothesis testing can detect the existence of the watermark with great certainty.

5. REFERENCES

[1] I.Pitas, "A method for signature casting on digital images", *Proc. of ICIP-96*, vol III, p.215, 1996.

[2] R.G. van Schyndel, A.Z.Tirkel and C.F.Osborne "A Digital Watermark", *Proc. ICIP94*, vol II, p.86, 1994.

[3] I.J.Cox, J.Kilian, T.Leighton and T.Shammoon "Secure Spread spectrum Watermarking for Multimedia", *Tech. Report*, NEC research Institute, no 95-10, p.1, 1995.

[4] W.Bender, D.Gruhl, N.Morimoto and A.Lu, "Techniques for data hiding", *IBM Systems Journal*, vol. 25, p.313-335, 1996.

[5] D.K. Arrowsmith and C.M.Place, "An Introduction to Dynamical systems", Cambridge Univ. Press 1990.

[6] I. Percival and F.Vivaldi, "Arithmetical properties of strongly chaotic systems", *Physica 25D*, p.105, 1987.

[7] G.Voyatzis and I.Pitas, "Chaotic mixing of digital images and applications to watermarking", *Proc. of ECMAST96*, vol.2, p.687, 1996.

[8] G.Voyatzis and I.Pitas, "Applications of Toral automorphisms in image watermarking", *Proc. of ICIP96*, vol II, p.237, 1996.

[9] G.Voyatzis and I.Pitas, in preparation.

[10] A. Papoulis, *"Probability & Statistics"*, Prentice Hall, 1991.