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 gray-scaled 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:

\[ W = \{ w_{kl} \mid 0 \leq k < M_1, 0 \leq l < M_2, w_{kl} = 0,1 \} \]  \hspace{1cm} (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 grayscale image or the luminance component of a color image of size \( N_1 \times N_2 \). An odd number of grey scale watermarks \( W_i \), identical to \( I \), are placed side by side (horizontally and vertically) to produce a binary image \( W_L \). The total number of pixels \( r \) of \( W_L \) should be smaller than the pixels of the image \( r N_1 N_2 \). We select the image pixel locations \( p \), where the watermark will be embedded, by applying the 1-1 map :

\[ F : W_L \rightarrow I, p = F' \circl r(k_1, k_2, ..., k_m) \]  \hspace{1cm} (2)
where $k_i$ are integer positive parameters and $n$ stands for iterative applications of the map. $F$ 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) $F^T$ 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 $F^P(I) = I$ [7]. The inverse map $F^{-1}$ 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 $5 \times 5$ mask for each image pixel $p$:

$$Mp = \begin{pmatrix}
c_{1} & c_{2} & c_{3} & c_{2} & c_{1} \\
c_{2} & 0 & 0 & 0 & c_{2} \\
c_{3} & 0 & Q_{p} & 0 & c_{3} \\
c_{2} & 0 & 0 & 0 & c_{2} \\
c_{1} & c_{2} & c_{3} & c_{2} & c_{1}
\end{pmatrix}$$  \hspace{1cm} (3)

where $c_1, c_2, c_3$ are small constant values ($\leq 4$) and $Q_p$ adapts to the image according to the formula:

$$Q_p = f(x_p, q; q_0)$$  \hspace{1cm} (4)

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

A global mask of size $N_1 \times N_2$ is derived by considering all the local masks $M$ and filling the complement.
space by zeros:

\[ \hat{M} = \bigcup_{p} M + O \]  

Finally \( \hat{M} \) is superimposed on the original image \( I \) to produce the watermarked image \( I' \):

\[ I' = I \oplus \hat{M} \]  

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 \( k \); of the mixing map \( F \) (i.e., the key). For each pixel of \( I'' \) we examine the difference:

\[ \Delta p = x'' - x'' \]  

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

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 \( \tilde{\delta}_0 \) and \( \tilde{\delta}_1 \) of \( \Delta p \) for all pixels \( p \) in \( I'' \) which map, via \( F^{-1} \), into the space of \( W_0 \) and \( W_1 \) respectively.

\[ \tilde{\delta}_i = \frac{1}{P_i} \sum_{p} \Delta p, \quad \forall p \text{ s.t. } F^{-1}(p) \in W_{II'} \]  

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

\[ \tilde{\delta} = \tilde{\delta}_1 - \tilde{\delta}_0 \approx 2 | q_0 | \]  

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

\[ H_0: \text{There is no watermark } (\tilde{\delta} = 0) \]
\[ H_1: \text{There is watermark } (\tilde{\delta} \neq 0) \]

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

\[ t = \tilde{\delta} / s_\delta \]  

where \( s_\delta \) 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 exists should be almost 1.

3. EXPERIMENTS

As an example the \( 60 \times 60 \) 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 \( | q_0 | = 4, | c_1 | = 2, | c_2 | = 2, | c_3 | = 3 \), the mask \( M \) is formed (see Fig. 1b). \( M \) is added in the image of Fig. 1c. The watermarked image is shown in Fig 2a. When the original watermarked image is
the correct key, to find watermarks. The performance $P$ for filtering blocks of size up to $5 \times 5$ 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 $5 \times 5$ 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