MULTI-BIT IMAGE WATERMARKING ROBUST TO GEOMETRIC DISTORTIONS

Anastasios Tefas and Ioannis Pitas

Department of Informatics, Aristotle University of Thessaloniki
Box 451, Thessaloniki 540 06, GREECE, pitas@zeus.csd.auth.gr

ABSTRACT

A novel method for multi-bit image watermarking robust to geometric distortions is proposed. A binary watermark is embedded in a grayscale or a color host image. The ability of progressive watermark detection enables fast and robust watermark detection even after several geometric distortions of the watermarked image. The embedding of a multi-bit message and its robust decoding after the watermark detection is also discussed. Simulation results indicate the ability of the proposed method to deal with the aforementioned attacks.

1. INTRODUCTION

In the last decades massive digitization of multimedia data such as photographs, paintings, speech, music, video, documents etc., became very popular. New techniques for the representation, storage and distribution of digital multimedia information have been developed. At the same time, the amount of digital data that is distributed through international communication networks has increased rapidly . In such an environment original digital products can be easily copied, tampered and transmitted back in the network. Consequently, the design of robust techniques for copyright protection of multimedia data became necessary.

The main challenge in multimedia watermarking for copyright protection is the robustness of the watermarking techniques against several types of attacks. The attacks that are usually encountered in image watermarking methods are image filtering, lossy image compression and geometric distortions. Although for the first two types of attacks many robust methods were proposed [1, 2], the robustness of the watermarking algorithms to geometric distortions is an unsolved problem yet. Another issue that is addressed in several watermarking techniques is the embedding of multi-bit messages in the host image and the robust extraction of the message during the watermark detection [3].

In this paper a novel technique for image watermarking robust to geometric distortions is proposed. It is based on an established watermarking technique [4, 5]. A watermark signal is embedded in the spatial domain according to appropriate embedding functions. In the watermark detection the watermark signal is generated and its existence is examined according to the corresponding detection functions. The original image is not necessary during the watermark detection. The novelty of the method is based on the design of a robust watermark detector which can be implemented progressively, increasing significantly the watermark detection speed. Watermark detection after several geometric distortions of the watermarked image is performed in real time. The proposed watermarking technique is also robust against image filtering and lossy image compression. The ability of the proposed method for multi-bit watermark embedding is also discussed.

2. WATERMARK GENERATION AND EMBEDDING

The watermark generation procedure aims at generating a three-valued watermark $w(\mathbf{x}) \in \{0, 1, 2\}$, from an image $f(\mathbf{x})$, given a digital key K. The watermark is a random sequence of three-valued data, thus, it is usually produced by a pseudorandom number generator. An alternative to random number generators is to use chaotic mixing systems that provide an additional level of security [6].

After the watermark generation we proceed to the watermark embedding by altering the pixels of the original (host) image according to the following formula:

$$f_w(\mathbf{x}) = \begin{cases} f(\mathbf{x}) & \text{if } w(\mathbf{x}) = 0 \\ g_1(f(\mathbf{x}), \mathcal{N}(\mathbf{x})) & \text{if } w(\mathbf{x}) = 1 \\ g_2(f(\mathbf{x}), \mathcal{N}(\mathbf{x})) & \text{if } w(\mathbf{x}) = 2 \end{cases} \quad (1)$$

where g_1, g_2 are suitably designed functions based on $\mathbf{x}$ and $\mathcal{N}(\mathbf{x})$ denotes a function that depends on the neighborhood of $\mathbf{x}$. The functions g_1, g_2 are called *embedding functions* and they are selected so as to define an inverse detection function $G(f_w(\mathbf{x}), \mathcal{N}(\mathbf{x}))$. The detection function, when applied to the watermarked image $f_w(\mathbf{x})$, gives the watermark $w(\mathbf{x})$:

$$G(f_w(\mathbf{x}), \mathcal{N}(\mathbf{x})) = w(\mathbf{x}) \quad (2)$$

Obviously several embedding functions and the appropriate detection function can be designed giving different watermarking schemes. The function that is used in our method is based on a superposition of real quantities in the pixels which are going to be signed:

$$g_1(f(\mathbf{x}), \mathcal{N}(\mathbf{x})) = \mathcal{N}(\mathbf{x}) \oplus \alpha_1 f(\mathbf{x}) \quad (3)$$

$$g_2(f(\mathbf{x}), \mathcal{N}(\mathbf{x})) = \mathcal{N}(\mathbf{x}) \oplus \alpha_2 f(\mathbf{x}) \quad (4)$$

where α_1, α_2 are suitably chosen constants and $\mathcal{N}(\mathbf{x})$ is local neighborhood operation of the pixels around $\mathbf{x}$. The sign of α_1, α_2 is used for the detection function and its value determines the watermark power.

The size of the region around $\mathbf{x}$ used for the calculation of $\mathcal{N}(\mathbf{x})$ is important for the watermarking procedure. Moreover, the number of pixels used for the calculation of $\mathcal{N}(\mathbf{x})$ determines the upper bound of the number of watermarked pixels in an image. If a pixel to be signed is contained in the neighboring region of another signed pixel, the related watermark detection may be affected by the neighboring pixel alterations, thus resulting in a false detection. To avoid such problems we should use small watermark embedding neighborhoods (i.e., of size 3×3). The maximum number of pixels that can be signed in a host image of dimensions $N \times N$ by using blocks of $(2r + 1) \times (2r + 1)$ for calculating $\mathcal{N}(\mathbf{x})$ is given by:

$$k = \frac{N^2}{(r + 1)^2} \quad (5)$$

3. WATERMARK DETECTION

In the detection procedure we generate first the watermark $w(\mathbf{x})$ according to the watermark key K. The detection function resulting from (3,4) is defined by:

$$G(f_w(\mathbf{x}), \mathcal{N}(\mathbf{x})) = \begin{cases} 1 & \text{if } f_w(\mathbf{x}) - \mathcal{N}(\mathbf{x}) > 0 \\ 2 & \text{if } f_w(\mathbf{x}) - \mathcal{N}(\mathbf{x}) < 0 \end{cases} \quad (6)$$

The detection function is valid if $\alpha_1 > 0$ and $\alpha_2 < 0$. This fact should be accounted for the design of the embedding functions. By employing the detection function in the watermarked image a bi-valued detection image $d(\mathbf{x})$ is produced:

$$d(\mathbf{x}) = G(f_w(\mathbf{x}), \mathcal{N}(\mathbf{x})) \quad (7)$$

Based on the watermark $w(\mathbf{x})$ and the detection image $d(\mathbf{x})$, we can decide whether the watermark under investigation is embedded in the imge or not. The detection is based on the pixel to pixel comparison for the nonzero pixels in $w(\mathbf{x})$. By comparing the watermark $w(\mathbf{x})$ and the detection image $d(\mathbf{x})$ we form the false detection image:

$$e_w(\mathbf{x}) = \begin{cases} 1 & \text{if } w(\mathbf{x}) \neq 0 \text{ and } w(\mathbf{x}) \neq d(\mathbf{x}) \\ 0 & \text{otherwise} \end{cases} \quad (8)$$

The false detection image has value 1 (white pixels) if a watermarked pixel is falsely detected and 0 otherwise. The detection ratio is given by the ratio of the correctly detected pixels to the sum of the watermarked pixels in the image.

$$D_w = 1 - \frac{\text{card}\{e_w(\mathbf{x})\}}{\text{card}\{w(\mathbf{x})\}} \quad (9)$$

The embedding functions are designed in such way, so as the probability p of a pixel to be detected as signed with g_1 or g_2, for an unwatermarked image, to be 0.5. Thus, the detection ratio in an unwatermaked image forms a binomial distribution. The cumulative distribution function (*cdf*) of the watermark detection ratio is given by:

$$P_n = p^k \sum_{i=0}^{n} \frac{k!}{i!(k-i)!} \quad (10)$$

where k is the total number of the watermarked pixels and n is the number of correctly detected watermarked pixels.

The decision about the image ownership is taken by comparing the watermark detection ratio of the image to a predefined threshold T. The value of the threshold determines the minimum acceptable level of watermark detection.

4. MULTI-BIT WATERMARKING

Suppose that we want to hide a message $\mathbf{l}$ comprised of M information bits in the image $f(\mathbf{x})$ that has N pixels. Two tests are involved in the verification process. First, the watermark detector decides if the image is watermarked according to the watermark key K. If the output of the watermark detector indicates that the image is signed, the hidden message extraction can be performed afterwards. This task is accomplished by a watermark decoder whose inputs are the watermarked image $f_w(\mathbf{x})$ and the secret key K. The output of the watermark decoder is an estimate $\hat{\mathbf{l}}$ of the hidden message.

The performance of the watermark decoder is given by the probability of error P_e, defined as the probability of getting a wrong estimate of the hidden message:

$$P_e \triangleq Pr\left\{\hat{\mathbf{l}} \neq \mathbf{l}\right\} \quad (11)$$

The goal of the watermark detection test is to decide whether the image f_w is watermarked or not. In the watermark decoding test it is assumed that the image is watermarked. The goal of the watermark decoder is to obtain an estimate $\hat{\mathbf{l}}$ of the hidden message $\mathbf{l}$ such that P_e is minimized. By conditioning the decoding error probability P_e associated with the specific decoder and the minimum acceptable probability of making an error when detecting whether an image pixel is watermarked or not, also known as *bit error rate* (BER), we can estimate the maximum number of message bits that can be encrypted in the image.

Let as denote by m the number of watermark samples used in order to encrypt a message $\mathbf{l}$. In the case of image watermarking the maximum acceptable error probability of the watermark detector is conditioned by the threshold T of the watermark detection ratio. In other words, an image is considered watermarked if the watermark detection ratio is greater than the predefined threshold. Thus, the minimum number of samples needed for the encoding of the hidden message for a specific decoding error probability is constrained by the detection threshold used in the watermark detection. Let us denote by q the probability of getting a wrong estimate of a sample used for the watermark detection:

$$q \triangleq Pr\left\{e(\mathbf{x}) = 1\right\} \quad (12)$$

Error correction codes can be used for correcting the watermark detection errors, resulting at a correct decoding of the hidden message. We suppose that we use an error correction code (e.g. BCH) that can correct r errors in m bits. The objective is to find the number of information bits that can be encrypted in the codeword for a specific message decoding error probability. The probability of getting a correct estimate of the message by using an error correction code that corrects r bit errors in m bits when the BER is q is given by:

$$P_d = \sum_{i=r}^{m} \frac{m!}{i!(m-i)!} q^i (1-q)^{m-i} \quad (13)$$

In the design of the message encryption module we should consider that an acceptable value for the probability of getting a wrong estimate of the hidden message is approximately 10^{-4}. Thus, the message decoding error probability should be:

$$P_e = 1 - P_d < \epsilon \quad (14)$$

By using (14) we can calculate the minimum number of errors r that should be corrected by the error correction code for a specific codeword length m, BER q and message decoding error probability P_e. The length of the hidden message that can be encrypted in a watermarked image for several codeword lengths by setting $q = 0.9$ and $\epsilon < 10^{-4}$ is given in Table 1.

5. PROGRESSIVE WATERMARK DETECTION AND ROBUSTNESS TO GEOMETRIC DISTORTIONS

The proposed watermarking algorithm is adequate for progressive watermark detection. By the term progressive watermark detection we mean that under certain conditions the watermark detection procedure is not necessary to be performed to the entire image.

Table 1. Hidden message length for several codeword lengths.

Code Length	Errors Corrected	Message Length	Message Error Probability
127	27	15	4.96E-05
255	45	37	6.39E-05
511	78	76	7.38E-05
1023	140	123	7.13E-05

That is, the watermark detection in a small region of the image is sufficient for deciding whether the image is watermarked or not. The minimum size of the search region depends on the minimum number of watermarked pixels needed for the detection procedure. In order to estimate the minimum number of watermarked pixels needed for the detection procedure we can condition the minimum acceptable false watermark acceptance probability. Let us denote by ϵ_1 the upper bound of false watermark acceptance probability (ϵ_1 is usually set equal to 10^{-4}):

$$Pr\left\{D_{w_i} > T\right\} < \epsilon_1, \quad \forall w_i \neq w \tag{15}$$

where T is the watermark detection threshold and w is the correct watermark.

The watermark detection ratio for an image watermark other than the one embedded in the image or for an unwatermarked image follows (10). Thus, equation (15) can be rewritten as:

$$\frac{1}{2^m} \sum_{i=Tm}^{m} \frac{m!}{i!(m-i)!} < \epsilon_1 \tag{16}$$

By using DeMoivre-Laplace theorem [7] it follows that:

$$\mathbf{G}\left\{\frac{Tm - 0.5m}{0.5\sqrt{m}}\right\} > 1 - \epsilon_1 \tag{17}$$

and the minimum number m of watermarked pixels needed for the watermark detection is:

$$m > \left(\frac{\text{erfinv}(0.5 - \epsilon_1)}{2T - 1}\right)^2 \tag{18}$$

where erfinv is the inverse function of the error function:

$$\text{erf}\, x = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-y^2/2} dy \tag{19}$$

Having calculate the minimum number of watermarked pixels needed for watermark detection, the minimum search region for the watermark detection can be evaluated. The minimum number of watermarked pixels needed for watermark detection and the size of the corresponding search regions for several watermark detection thresholds T and ϵ_1 equal to 10^{-4} are plotted in Figure 1. It is obvious from the plots that a region of approximately 59×59 is sufficient for watermark detection for a watermark threshold greater than 0.65. Simulation results for 1000 watermarks at each threshold agree with the theoretical analysis as it can be observed in Figure 1b. The false watermark detection probability is always approximately $\epsilon_1 = 10^{-4}$.

According to the previous analysis we can start the watermark detection from regions smaller than the lower limit provided that the corresponding watermark detection threshold is increased such that inequality (18) is always satisfied. As the search region is increased the watermark detection threshold is decreased. The size

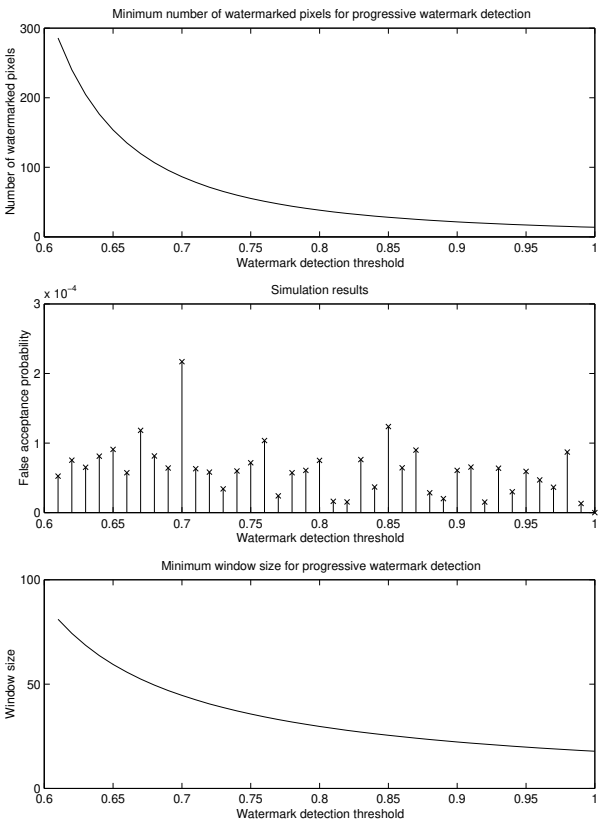

Fig. 1. Minimum number of watermarked pixels needed for progressive detection. False watermark acceptance probability achieved by simulation results for several thresholds and the corresponding theoretic number of watermarked pixels. The corresponding search region size for several thresholds.

of the smaller region that we can start from is given by the condition that the probability of rejecting the correct watermark, by performing watermark detection only in this region, should be lower than ϵ_2:

$$Pr\left\{D_{w_i} < T\right\} < \epsilon_2, \quad w_i = w \tag{20}$$

where T is the watermark detection threshold, w is the correct watermark and ϵ_2 is a very small number (approximately 10^{-4}). Progressive watermark detection is illustrated in Figure 2. Watermark detection starts from a small region and if the watermark detection ratio in this area is larger than the corresponding threshold the watermark detection proceeds to the next contour. By comparing at each step the watermark detection ratio to the corresponding threshold the algorithm stops when the search region becomes greater than the lower limit given by (18), deciding that the watermark under investigation is indeed embedded in the image or when the watermark detection ratio falls under the corresponding threshold, deciding that the image is not watermarked.

The proposed algorithm allows very fast watermark detection thus enabling correct watermark detection for several geometric distortions of the watermarked image. Specifically, the detection of a watermark shifted to every pixel of an image is performed in real time. Moreover, robustness against image cropping is achieved by exhaustive search of the watermark in the test image which is performed in real time due to progressive watermark detection.

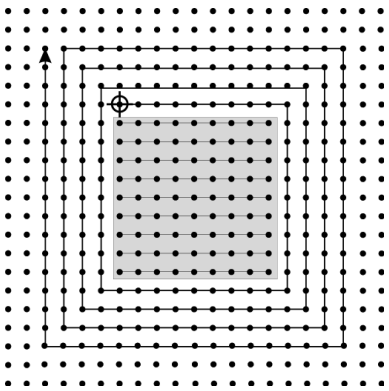

Fig. 2. Progressive watermark detection.

Accordingly, the watermark detection for several geometric distortions, like scaling and rotation, of the watermarked image is implemented in a few seconds. The speed of the proposed algorithm can be further improved by constructing watermark signals of specific structures (e.g. self similar, symmetric etc.) thus reducing the search space.

6. SIMULATION RESULTS

As it was described in the introduction, the main objective of an image watermarking algorithm is robustness against several types of attacks (e.g. image filtering, lossy image compression, geometric distortions etc.). The robustness of the proposed algorithm against image filtering and lossy image compression was presented in [4]. Moreover, the method is robust against JPEG compression up to 30:1 for images of size 512×512 or more. For mean filtering with window of size 3×3 and 5×5 the watermark is detected 100% with certainty 99.99%. Perfect watermark detection is also achieved after median image filtering with window of size 3×3 while the probability of watermark detection is reduced to 81% for median filtering of size 5×5.

The proposed improved version is also robust against geometric distortions due to progressive watermark detection and allows embedding of multi-bit watermarks. The robustness of the proposed progressive watermark detection against image cropping, rotation and scaling as well as for combined attacks has been tested in a number of experiments. For cropped images the detection ratio is always 1 and the search time for the watermark detection is less than 1 second for images of various sizes. The estimated *pdf* of the watermark detection ratio after rotation of the watermarked image at 1000 random angles is illustrated in Figure 3. It is obvious that the watermark is always detected since the watermark detection ratio is not significantly reduced. The watermark detection ratio for combined attacks is plotted in Figure 4. The watermarked image is scaled with several scaling factors and it is rotated at random angles. It is obvious that when rotation precedes scaling for scaling factors smaller than 1 (decimation) the watermark detection ratio is higher than the detection ratio obtained when these operations are applied in reverse order. For scaling factors larger than 1 (zooming) the relative performance is inverted.

7. CONCLUSIONS

A novel method for image watermarking has been presented. The major advantage of the proposed method is its robustness against geometric distortions. A progressive watermark detection technique has also been proposed that enables fast and robust watermark detection after several geometric distortions of the watermarked image. The feature of multi-bit message encryption and its robust detection even after several alterations of the watermarked image has also been treated.

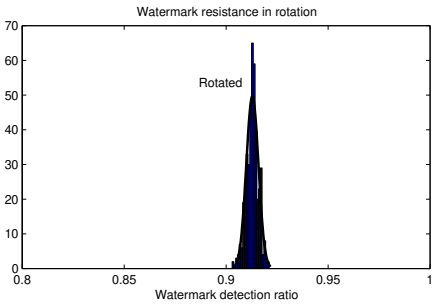

Fig. 3. Watermark robustness for rotation of the watermarked image at random angles and random watermark keys.

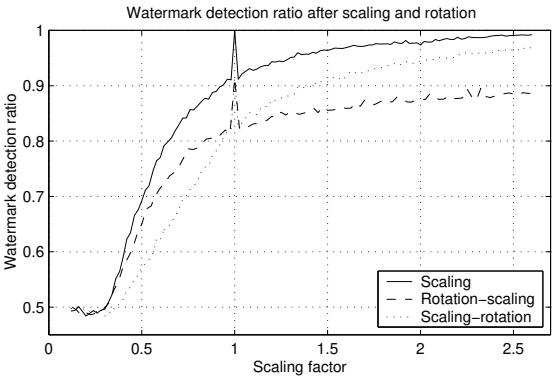

Fig. 4. Watermark robustness for scaling of the watermarked image and rotation at random angles.

8. REFERENCES

[1] M.D. Swanson, M. Kobayashi, and A.H. Tewfik, "Multimedia data embedding and watermarking technologies," *Proceedings of the IEEE*, vol. 86, no. 6, pp. 1064–1087, June 1998.

[2] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1079–1107, July 1999.

[3] F.A.P. Petitcolas, R.J Anderson, and M.G. Kuhn, "Information hiding - a survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, July 1999.

[4] G. Voyatzis and I. Pitas, "Digital image watermarking using mixing systems," *Computer & Graphics*, vol. 22, no. 3, 1998.

[5] G. Voyatzis and I. Pitas, "The use of watermarks in the protection of digital multimedia products," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1197–1207, July 1999.

[6] J. Fridrich, A.C. Baldoza, and R.J. Simard, "Symmetric ciphers based on 2d maps," in *Proc. IEEE Conf. on Systems, Man, and Cybernetics*, Octomber 1997, pp. 1105–1110.

[7] A. Papoulis, *Probability Random Variables and Stochastic Processes*, McGraw Hill, 1991.