Digital Image Tracing by Sequential Multiple Watermarking

Giulia Boato, *Member, IEEE*, Francesco G. B. De Natale, *Senior Member, IEEE*, and Claudio Fontanari

***Abstract*—The possibility of adding several watermarks to the same image would enable many interesting applications such as multimedia document tracing, data usage monitoring, multiple property management. In this paper, we present a novel watermarking scheme which allows to insert and reliably detect multiple watermarks sequentially embedded into a digital image. The proposed method, based on elementary linear algebra, is asymmetric, secure under projection attack and robust against distortion due to basic operations such as storage, transmission, format conversion, etc.**

***Index Terms*—Asymmetric watermarking, image tracing, linear algebra, multiple watermarking.**

I. Introduction

SECURITY of multimedia communications is regarded by both academy and industry research as one of the most important and urgent problems of the last decades. Watermarking is the art of imperceptibly embedding a message into a work. More than 700 years ago in Fabriano (Italy), paper watermarks appeared in handmade paper, in order to identify its provenance, format, and quality. Since the early 1990s, digital watermarking has applied similar concepts to multimedia contents (images, video, music) as a technological support to digital right management. In this context, the watermark is a kind of invisible signature that allows identifying the creator or the owner of a document, and to detect possible copyright violations, and especially nonauthorized copying.

More recently, different watermarking techniques and strategies have been proposed in order to solve a number of problems, ranging from the detection of content manipulations, to information hiding (steganography), to document usage tracing. In particular, the insertion of multiple watermarks to trace a document during its lifecycle is a very interesting and challenging application. The main objective is to grant the possibility of directly detecting from the document who was the creator, who had access to the data after its creation, how the property of the document is shared among different users, allowing not only the document tracing (crucial for example in the management of images connected to a legal prosecution), but also data usage monitoring (useful in newspaper documents processing).

This kind of protection of confidential material, such as design drawings or personal data, is crucial in several industrial sectors (mechanical engineering, semiconductor industry, as well as in the automotive and chemical/pharmaceutical sectors—see [1]). Biomedical data handling provides another significant field of application with specific and severe requirements. Indeed, the importance of watermarking in medical imaging has already been pointed out in [2]. In [3] and [4], the interested reader can find a detailed list of the medical issues which can be addressed by the insertion of multiple digital watermarks. The range of application is rather wide, covering not only access control and identity verification, but also captioning and indexing issues. We stress in particular the relevance, due to the confidentiality and the diagnostic value of medical data, of tracing the history of a medical document from the patient through the various laboratories and physicians.

Notwithstanding the application potential of such methodologies, multiple-image watermarking is still an open problem. Although some researchers focused on the viability of existing watermarking approaches for the insertion of multiple signatures (see [5] for a critical assessment about the use of some of the most popular watermarking methods for tracing medical images), the development of specific techniques can provide much more effective results. The general problem of multiple digital watermarking has been the object of several investigations since the pioneering contribution [6], where the possibility of recovering different watermarks in the same image is first shown. In [7], it is suggested that the insertion of multiple watermarks can be exploited to convey multiple sets of information, while [8] and [9] discuss specific extensions of single watermarking algorithms to the case of multiple watermarks, by introducing orthogonal watermarks. More recently, a multiple watermark-embedding procedure was proposed ([10]), which allows simultaneous insertions without requiring the key sets to be orthogonal to each other. Specific applications such as the already mentioned medical image management (see, in particular, [11] and [12]) may even require the insertion of two different types of watermark, namely, a robust one for authentication purposes, and a fragile one for data integrity control. This paradigm is often referred to as multipurpose watermarking (see for instance [13] and [14]).

In this paper, we introduce a new approach that allows the tracing and property sharing of image documents thanks to the possibility of sequentially embedding multiple watermarks into the data. As in our former contribution [15], intended for the

Manuscript received March 8, 2006; revised October 20, 2006. This paper was previously presented at the International Conference on Image Processing 2006, held in Atlanta, GA, October 2006. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Wenjun (Kevin) Zeng.

G. Boato and F. G. B. De Natale are with the Department of Information and Communication Technology, University of Trento, I-38050 Trento, Italy (e-mail: boato@dit.unitn.it; denatale@ing.unitn.it).

C. Fontanari is with the Department of Mathematics, Third School of Engineering – Information Technologies, Politecnico di Torino, I-10129, Torino, Italy (e-mail: claudio.fontanari@polito.it).

Digital Object Identifier 10.1109/TMM.2007.893335

insertion of a single watermark, the present scheme is based on elementary linear algebra and it is asymmetric, in the sense that it involves a private key for embedding and a public key for detection. The main property of the proposed method is that it allows the insertion of multiple watermarks by different users, who sequentially come into play one after the other and do not need any extra information besides the public keys. This characteristic makes the present approach more attractive than previously available solutions. In particular, it solves the problem affecting other recent approaches (see for instance [16], based on [10]), where each user needs to know the secret keys used to embed all previous watermarks to successfully insert his signature. Moreover, the proposed scheme is proved to be secure against the most dangerous attack against watermarking security, namely, the closest point or projection attack, and its robustness has also been successfully assessed by simulating a distortion of the data at each stage of the process, through the addition of a noise source or format conversion. It is to be pointed out that the envisaged applications for our multiple watermarking scheme are mainly based on the hypothesis of a collaborative environment, in which malicious attacks are not a critical aspect, and it is worth mentioning that, in many cases, the only relevant manipulation is just a light JPEG compression, as described in [17].

The structure of the paper is as follows. In Section II, we describe the proposed multiple watermarking scheme. In Section III, we prove it to be effective, secure under projection attack and robust against noise addition, JPEG compression, and some other image manipulations. Finally, in Section IV, we draw some concluding remarks.

II. Watermark Embedding and Detection

We are going to describe an asymmetric watermarking procedure, where as usual the encoding and decoding algorithms as well as the detection key are known, while the embedding key is kept secret.

Let V be a feature space of dimension d (for instance, the space $\mathbb{R}^d$ corresponding to the entries in the top left corner of the DCT of a digital image) and let $\{u_1, \dots, u_n\}$ be an ordered set of users. Let us also introduce another integer $k \geq 1$ corresponding to an additional parameter of the method (useful to improve detection performances) and let us denote by $\mathcal{M}$ the set of $d \times d$ real matrices D such that $\dim(\mathrm{Ker} D) = d - k - 1$, where $\mathrm{Ker} D = \{v \in \mathbb{R}^d : Dv = 0\}$ is the kernel of D.

For each $i = 1, \dots, n$, the user u_i with associated signature $s_i \in V$ has free access to public keys $D_1, \dots, D_{i-1} \in \mathcal{M}$, receives a host signal $\phi_{i-1} \in V$ and produces a watermarked signal $\phi_i \in V$ and a public key $D_i \in \mathcal{M}$.

Since at the end of the procedure we wish to be able to detect all embedded signatures, we fix an upper bound for the number of users in terms of the parameters of the method. An effective bound turns out to be

$$n \leq \frac{d+k}{k+1} \tag{1}$$

as will become clear from the embedding algorithm.

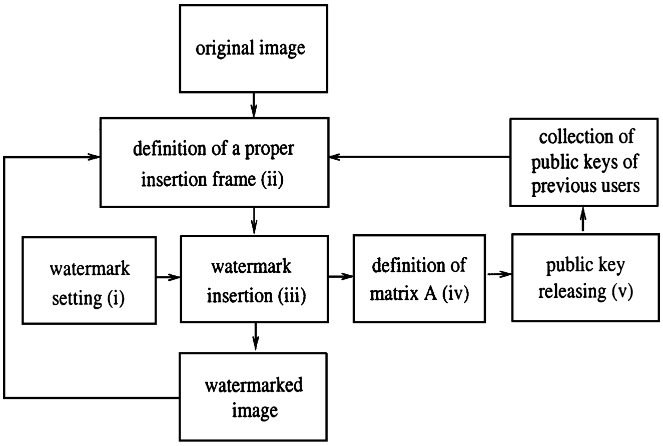

original image
definition of a proper insertion frame (ii)
collection of public keys of previous users
watermark setting (i)
watermark insertion (iii)
definition of matrix A (iv)
public key releasing (v)
watermarked image

Fig. 1. Description of the watermarks embedding procedure.

A. Watermark Embedding

Each user u_i implements the following algorithm, summarized in Fig. 1.

i) *Watermark setting*: u_i sets the watermark $w_i = \alpha s_i$ with $0 < \alpha \ll 1$ in order to meet the usual imperceptibility requirement.

ii) *Definition of a proper insertion frame*: u_i chooses a $d \times d$ orthogonal matrix M_i such that

$$D_j(M_i w_i) = 0 \tag{2}$$

for every $j \leq i-1$ (if $i = 1$ condition (2) is empty). Notice that by (1) and Corollary 1 in the Appendix, there exists at least one $v \in V \setminus \{0\}$ such that $D_j(\lambda v) = 0$ for every $j \leq i-1$ and for every $\lambda \in \mathbb{R}$. In order to construct M_i, let $g_1 = w_i/\|w_i\|$ (respectively, $h_1 = v/\|v\|$) and complete g_1 (respectively, h_1) to an orthonormal basis $(g_1, g_2, \dots, g_d)$ (respectively, $(h_1, h_2, \dots, h_d)$) of $\mathbb{R}^d$: for instance, complete them to an arbitrary basis and then apply the standard Gram-Schmidt orthonormalization process; if G (respectively, H) is the matrix with g_t^T (respectively, h_t^T) as the t-th column ($t = 1, \dots, d$), then the private key $M_i := HG^T$ is such that $M_i w_i = \|w_i\|/\|v\| v$.

iii) *Watermark insertion*: if $\phi_{i-1} = M_i v_i$ (i.e., v_i are the coordinates of ϕ_{i-1} in the basis given by the columns of M_i) then u_i watermarks ϕ_{i-1} by setting

$$\phi_i = M_i(v_i + w_i). \tag{3}$$

iv) *Definition of an auxiliary matrix*: u_i chooses an arbitrary vector subspace Z of dimension k orthogonal to $v_i + w_i$ and constructs a symmetric $d \times d$ matrix A_i (i.e., $A_i^T = A_i$) such that

$$A_i(v_i + w_i) = v_i + w_i \tag{4}$$

$$A_i(z) = Kz \quad \forall z \in Z \tag{5}$$

$$A_i(v) = 0 \quad \forall v \in \langle v_i + w_i, Z \rangle^{\perp} \tag{6}$$

where $K \gg 0$ is a nonnegative integer. More operatively, let $b_1 := (v_i + w_i/||v_i + w_i||)$ and complete it to an orthonormal basis $(b_1, b_2, \ldots, b_d)$ of $\mathbb{R}^d$: for instance, complete b_1 to an arbitrary basis and then apply the standard Gram-Schmidt orthonormalization process; if N_i is the matrix with b_t^T as the tth column $(t = 1, \ldots, d)$, then

$$A_i = N_i \begin{pmatrix} 1 & 0 & \ldots & & & \\ 0 & K & 0 & \ldots & & \\ \vdots & & \ddots & \vdots & & \\ 0 & \ldots & & K & 0 & \ldots \\ 0 & \ldots & & & 0 & \ldots \\ \vdots & & & & \vdots & \end{pmatrix} N_i^T. \tag{7}$$

v) *Public key releasing*: u_i releases to the public the detection keys

$$D_i = A_i M_i^T v_i + w_i. \tag{8}$$

Notice that, since A_i is not invertible, the private key M_i cannot be reconstructed from D_i. Since both M_i and N_i are invertible, from (7) it follows that $\dim \mathrm{Ker} D_i = d - k - 1$, hence $D \in \mathcal{M}$.

B. Watermark Detection

Let now ϕ_e be an extracted feature. The watermark detection is accomplished by the decision function

$$\delta_i(\phi_e) = \begin{cases} 1, & \text{if } |\mathrm{sim}(v_i + w_i, D_i\phi_e)| \geq \varepsilon \\ 0, & \text{otherwise} \end{cases} \tag{9}$$

where $0 \leq \varepsilon \ll 1$ is a suitable threshold and

$$\mathrm{sim}(v_i + w_i, D_i\phi_e) = \frac{(v_i + w_i)^T D_i \phi_e}{||v_i + w_i|| ||D_i\phi_e||}. \tag{10}$$

Definitions (9) and (10) for the detector are motivated by the following fact.

Proposition 1: For every $i = 1, \ldots, n$, we have $\mathrm{sim}(v_i + w_i, D_i\phi_i) = 1$. Moreover, if ϕ is any feature vector not watermarked by u_i and the integer K is big enough, then $\mathrm{sim}(v_i + w_i, D_i\phi)$ is arbitrarily close to zero. In particular, $\mathrm{sim}(v_i + w_i, D_i\phi_j)$ is almost zero if $j \leq i - 1$.

Proof: By (8), (3) and (4) we have $D_i\phi_i = v_i + w_i$, hence the first part of the claim is a direct consequence of (10). Next, if $M_i^T\phi = \sum_{t=1}^d c_t b_t$ is the expression of $M_i^T\phi$ in the basis $(b_1, b_2, \ldots, b_d)$ constructed in step 4) of the embedding algorithm, then

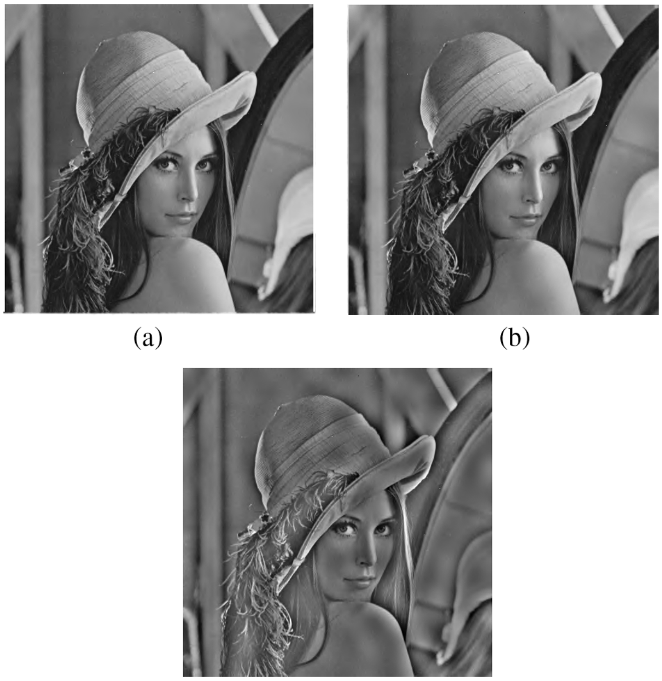
$$D_i\phi = \sum_{t=1}^{d} c_t A_i b_t = c_1 b_1 + K \sum_{t=2}^{k+1} c_t b_t$$

by (5) and (6) and we may compute

$$(v_i + w_i)^T D_i \phi = c_1 ||v_i + w_i||$$

$$||D_i\phi|| = \sqrt{c_1^2 + K^2 \sum_{t=2}^{k+1} c_t^2}.$$

Hence, we deduce $\lim_{K \to \infty} \mathrm{sim}(v_i + w_i, D_i\phi) = 0$ and also the second claim follows. ■



(a)

(b)

(c)

Fig. 2. (a) Original. (b) Watermarked $(\mathrm{PSNR} = 35.53\ \mathrm{dB})$. (c) Projected Lena $(\mathrm{PSNR} = 16.10\ \mathrm{dB})$.

The following result shows that detection still works even after several watermark embeddings.

Proposition 2: For every $i = 1, \ldots, n$, if

$$\psi_i = \phi_i + \sum_{j>i} M_j w_j$$

then $\mathrm{sim}(v_i + w_i, D_i\psi_i) = 1$.

Proof: By (3), we have

$$\psi_i = M_i(v_i + w_i) + \sum_{j>i} M_j w_j.$$

It follows from (2) that $D_i M_j w_j = 0$ for every $j > i$ and since by (8) and (4), we have

$$D_i\psi_i = v_i + w_i + \sum_{j>i} D_i M_j w_j$$

we deduce that $D_i\psi_i = v_i + w_i$ and we conclude by (10). ■

We stress that the private key is carefully defined in order to avoid conflicts between different watermarks. In particular, n arbitrary watermarks can be inserted and detected if (1) and (2) are observed.

III. Effectiveness, Security, and Robustness Analysis

A. Effectiveness

In order to experimentally verify the effectiveness of the proposed method, we test it on the standard 512 × 512 Lena and Baboon images by choosing as a feature space the upper left 15× 15 coefficients of the discrete cosine transform (DCT) (excluding as it is customary the DC component) and by sequentially embedding ten randomly generated watermarks. Hence,

TABLE I
DETECTION PERFORMANCES FOR THE LENA IMAGE

feature	PSNRw	PSNRp	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}
ϕ_0	-	-	0.10	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.02	0.02
ϕ_1	45.52	16.10	1	0.11	0.07	0.06	0.05	0.05	0.04	0.04	0.04	0.04
ϕ_2	42.55	16.10	1	1	0.11	0.08	0.06	0.05	0.05	0.05	0.04	0.04
ϕ_3	40.77	16.10	1	1	1	0.10	0.07	0.06	0.06	0.05	0.05	0.04
ϕ_4	39.51	16.10	1	1	1	1	0.10	0.08	0.06	0.05	0.05	0.05
ϕ_5	38.54	16.10	1	1	1	1	1	0.11	0.08	0.06	0.05	0.05
ϕ_6	37.75	16.10	1	1	1	1	1	1	0.11	0.08	0.06	0.06
ϕ_7	37.08	16.10	1	1	1	1	1	1	1	0.10	0.08	0.06
ϕ_8	36.50	16.10	1	1	1	1	1	1	1	1	0.11	0.08
ϕ_9	35.98	16.10	1	1	1	1	1	1	1	1	1	0.11
ϕ_{10}	35.53	16.10	1	1	1	1	1	1	1	1	1	1

TABLE II
DETECTION PERFORMANCES FOR THE BABOON IMAGE

feature	PSNRw	PSNRp	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}
ϕ_0	-	-	0.09	0.03	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02
ϕ_1	45.52	17.56	1	0.09	0.06	0.05	0.04	0.04	0.04	0.03	0.03	0.03
ϕ_2	42.60	17.56	1	1	0.09	0.06	0.05	0.05	0.04	0.04	0.04	0.03
ϕ_3	40.81	17.56	1	1	1	0.09	0.06	0.05	0.05	0.04	0.04	0.03
ϕ_4	39.55	17.56	1	1	1	1	0.09	0.06	0.05	0.05	0.04	0.04
ϕ_5	38.57	17.56	1	1	1	1	1	0.09	0.06	0.05	0.05	0.04
ϕ_6	37.78	17.56	1	1	1	1	1	1	0.09	0.06	0.05	0.04
ϕ_7	37.10	17.56	1	1	1	1	1	1	1	0.09	0.06	0.05
ϕ_8	36.52	17.56	1	1	1	1	1	1	1	1	0.09	0.06
ϕ_9	36.01	17.56	1	1	1	1	1	1	1	1	1	0.09
ϕ_{10}	35.55	17.56	1	1	1	1	1	1	1	1	1	1

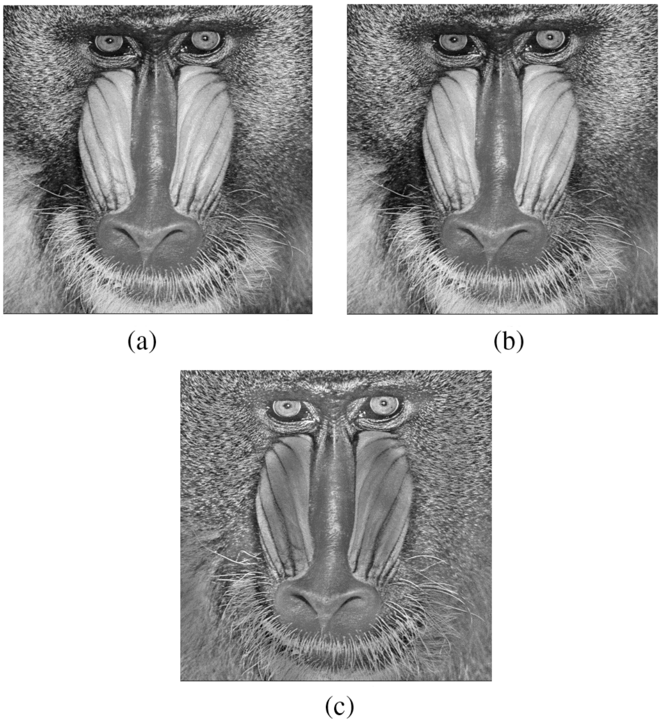
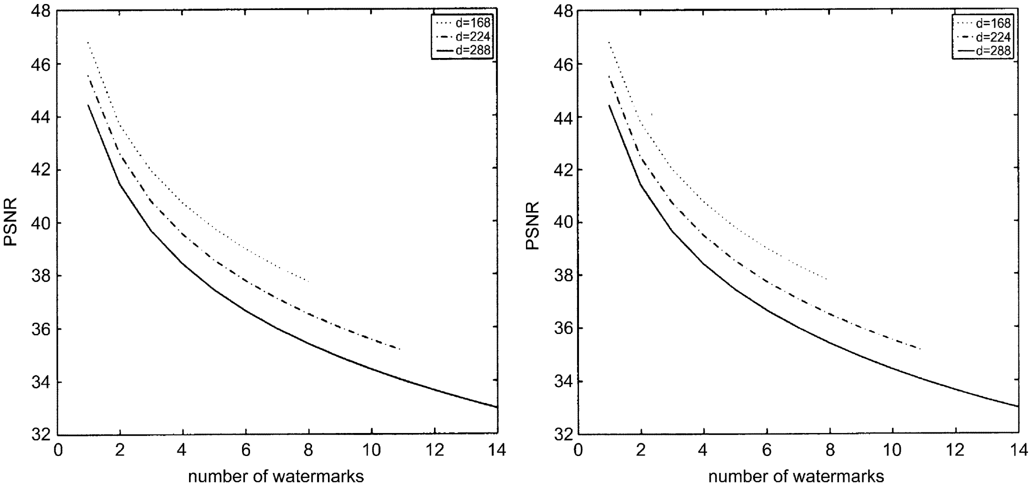

(a) (b) (c)

Fig. 3. (a) Original. (b) Watermarked ($\mathrm{PSNR} = 35.55$ dB). (c) Projected Baboon ($\mathrm{PSNR} = 17.56$ dB).

we have $d = 224$ and $n = 10$; we also set $K = 10^3$ and $k = 20$, so that condition (1) is satisfied. We report in Figs. 2(a) and 3(a) the original images corresponding to ϕ_0 and in Figs. 2(b) and 3(b) the final images corresponding to ϕ_{10} and carrying ten watermarks: it should be apparent that the watermarked image is perceptually undegraded (PSNR equal to 35.53 and 35.55 dB, respectively). Notice that the method is suitable also for demanding applications with high PSNR requirements (such as medical or legal documents processing), since all inserted watermarks can be removed by exploiting the knowledge of the corresponding private keys. The obtained detection performances are summarized in Tables I and II, where the entry corresponding to (ϕ_i, w_j) is the value of $\mathrm{sim}(v_j + w_j, D_j\phi_i)$ averaged over 100 experiments. As predicted by Proposition 1 and Proposition 2, we see that $\mathrm{sim} = 1$ whenever $j \geq i$ (hence w_j has been embedded into ϕ_i) and it is close to zero otherwise. Therefore, the watermark can be detected only by using the correct detection key. The threshold ε, which defines the decision function of the detection, can be chosen in a wide range of values, namely, $\varepsilon \in [0.12, 1]$ is valid for both the Lena and Baboon images. Moreover, we provide the PSNR value at every stage for both the watermarked image (PSNRw) and the image after projection attack (PSNRp). In particular, in Fig. 4 we report the average PSNR of the watermarked Lena and Baboon images as a function of the number of watermarks sequentially embedded, considering feature spaces of different size ($d = 168$, $d = 224$ and $d = 288$, respectively) and $n \leq 8$, $n \leq 11$ and $n \leq 14$, respectively, in such a way that condition (1) holds (k is fixed equal to 20).

B. Security

Although our method is mainly thought for data tracing in collaborative environment, we aim at demonstrating that it achieves also a good security level. In particular, we apply to the images with increasing number of watermarks embedded the most dangerous attack against asymmetric watermarking security, namely, the closest point or projection attack. Recall



(a) (b)

Fig. 4. Average PSNR of the watermarked (a) Lena and (b) Baboon images versus number of watermarks sequentially embedded for different sizes of the feature space ($d = 168$, $d = 224$ and $d = 288$) and $k = 20$.

TABLE III
Detection Performances for the Lena Image in the Case of Random WGN Addition

feature	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}
ϕ_0	0.10	0.03	0.03	0.03	0.03	0.03	0.03	0.02	0.02	0.02
ϕ_1	0.87	0.11	0.08	0.06	0.06	0.05	0.04	0.04	0.04	0.04
ϕ_2	0.77	0.87	0.10	0.08	0.06	0.05	0.05	0.04	0.04	0.04
ϕ_3	0.69	0.77	0.87	0.10	0.08	0.06	0.05	0.05	0.04	0.04
ϕ_4	0.65	0.71	0.79	0.88	0.11	0.08	0.06	0.05	0.05	0.04
ϕ_5	0.61	0.66	0.72	0.80	0.87	0.10	0.08	0.06	0.05	0.05
ϕ_6	0.57	0.62	0.66	0.73	0.77	0.87	0.10	0.08	0.06	0.05
ϕ_7	0.54	0.59	0.62	0.68	0.69	0.77	0.87	0.11	0.07	0.06
ϕ_8	0.51	0.56	0.58	0.62	0.64	0.69	0.76	0.85	0.10	0.07
ϕ_9	0.49	0.53	0.55	0.59	0.60	0.64	0.70	0.77	0.88	0.11
ϕ_{10}	0.47	0.50	0.53	0.56	0.57	0.60	0.64	0.71	0.78	0.86

TABLE IV
Detection Performances for the Baboon Image in the Case of Random WGN Addition

feature	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}
ϕ_0	0.09	0.03	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02
ϕ_1	0.84	0.09	0.06	0.05	0.05	0.04	0.04	0.04	0.03	0.03
ϕ_2	0.74	0.84	0.09	0.06	0.05	0.05	0.04	0.04	0.03	0.03
ϕ_3	0.65	0.74	0.83	0.09	0.06	0.05	0.05	0.04	0.04	0.03
ϕ_4	0.59	0.66	0.72	0.83	0.09	0.06	0.05	0.05	0.04	0.04
ϕ_5	0.53	0.59	0.64	0.73	0.83	0.09	0.06	0.05	0.05	0.04
ϕ_6	0.50	0.55	0.58	0.65	0.72	0.83	0.09	0.07	0.05	0.04
ϕ_7	0.47	0.51	0.53	0.58	0.64	0.71	0.83	0.09	0.06	0.05
ϕ_8	0.44	0.47	0.48	0.52	0.58	0.62	0.70	0.82	0.09	0.06
ϕ_9	0.42	0.45	0.46	0.49	0.54	0.57	0.62	0.71	0.83	0.09
ϕ_{10}	0.40	0.43	0.44	0.47	0.50	0.53	0.57	0.64	0.72	0.84

that a projection attack replaces the feature vector ϕ_i associated to the watermarked signal with a feature vector $\tilde{\phi}_i$ satisfying

$$\|\tilde{\phi}_i - \phi_i\| = \min \|\phi - \phi_i\|^2 \tag{11}$$

under the constraint

$$\delta(\phi) = \mathrm{sim}(v_i + w_i, D_i\phi) = 0. \tag{12}$$

Hence, $\tilde{\phi}_i$ is the non-watermarked feature vector closest to ϕ_i. By definition (10), condition (12) says that $(v_i+w_i)^T D_i \phi_i = 0$, i.e., ϕ_i has to lie on the hyperplane through the origin of the feature space having normal vector $a_i = D_i^T(v_i + w_i)$. As a consequence, the feature vector $\tilde{\phi}_i$ satisfying condition (11) is the projection of ϕ_i onto this hyperplane, which is given by

$$\tilde{\phi}_i = \phi_i - \frac{a_i^T \phi_i}{\|a_i\|^2} a_i. \tag{13}$$

The following result suggests that the signal reconstructed from $\tilde{\phi}_i$ will be dramatically distorted, hence our scheme turns out to be definitively secure under projection attack.

Proposition 3: For every $i = 1, \ldots, n$, we have $\tilde{\phi}_i = 0$.

Proof: By (8), (4), and (3), we have

$$a_i = D_i^T(v_i + w_i) = M_i A_i^T(v_i + w_i) = M_i(v_i + w_i) = \phi_i$$

TABLE V
DETECTION PERFORMANCES FOR THE LENA IMAGE WITH THE ADDITION OF WGN OF 15 dB

feature	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}
ϕ_0	0.10	0.03	0.03	0.03	0.03	0.03	0.03	0.02	0.02	0.02
ϕ_1	0.64	0.10	0.07	0.06	0.05	0.05	0.04	0.04	0.04	0.04
ϕ_2	0.53	0.65	0.11	0.08	0.06	0.05	0.05	0.05	0.04	0.04
ϕ_3	0.45	0.52	0.65	0.10	0.07	0.06	0.05	0.05	0.04	0.04
ϕ_4	0.40	0.44	0.52	0.65	0.10	0.08	0.06	0.05	0.05	0.04
ϕ_5	0.36	0.39	0.45	0.52	0.64	0.11	0.07	0.06	0.06	0.05
ϕ_6	0.33	0.36	0.39	0.45	0.53	0.66	0.10	0.08	0.06	0.05
ϕ_7	0.31	0.33	0.36	0.41	0.45	0.52	0.65	0.11	0.08	0.06
ϕ_8	0.29	0.31	0.33	0.37	0.40	0.44	0.52	0.65	0.11	0.08
ϕ_9	0.28	0.29	0.31	0.34	0.36	0.40	0.45	0.52	0.66	0.11
ϕ_{10}	0.26	0.27	0.29	0.31	0.33	0.36	0.40	0.45	0.52	0.65

TABLE VI
DETECTION PERFORMANCES FOR THE BABOON IMAGE WITH THE ADDITION OF WGN OF 15 dB

feature	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}
ϕ_0	0.09	0.03	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02
ϕ_1	0.59	0.09	0.06	0.05	0.04	0.04	0.04	0.03	0.03	0.03
ϕ_2	0.45	0.59	0.09	0.06	0.05	0.05	0.04	0.04	0.04	0.03
ϕ_3	0.38	0.46	0.58	0.09	0.06	0.05	0.05	0.04	0.04	0.04
ϕ_4	0.34	0.39	0.46	0.58	0.09	0.06	0.05	0.05	0.04	0.04
ϕ_5	0.31	0.34	0.39	0.45	0.58	0.09	0.06	0.05	0.05	0.04
ϕ_6	0.28	0.30	0.35	0.39	0.46	0.60	0.09	0.06	0.05	0.05
ϕ_7	0.26	0.28	0.31	0.34	0.39	0.46	0.59	0.09	0.06	0.05
ϕ_8	0.25	0.26	0.28	0.31	0.35	0.39	0.46	0.58	0.09	0.07
ϕ_9	0.24	0.25	0.26	0.28	0.32	0.34	0.39	0.46	0.58	0.09
ϕ_{10}	0.23	0.24	0.25	0.26	0.29	0.31	0.34	0.39	0.46	0.59

TABLE VII
DETECTION PERFORMANCES FOR THE LENA IMAGE IN CASE OF RANDOM JPEG COMPRESSION

feature	PSNR	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}
ϕ_0	-	0.10	0.03	0.03	0.03	0.03	0.03	0.02	0.02	0.02	0.02
ϕ_1	41.38	0.65	0.11	0.07	0.06	0.06	0.05	0.04	0.04	0.04	0.04
ϕ_2	40.27	0.64	0.94	0.11	0.08	0.06	0.05	0.05	0.05	0.04	0.04
ϕ_3	39.03	0.63	0.90	0.95	0.10	0.08	0.06	0.06	0.05	0.04	0.04
ϕ_4	38.17	0.62	0.87	0.92	0.96	0.11	0.08	0.06	0.06	0.05	0.05
ϕ_5	37.47	0.61	0.85	0.89	0.93	0.97	0.11	0.08	0.06	0.05	0.05
ϕ_6	36.83	0.60	0.83	0.86	0.90	0.94	0.97	0.11	0.08	0.06	0.05
ϕ_7	36.25	0.60	0.80	0.84	0.87	0.91	0.93	0.97	0.11	0.08	0.06
ϕ_8	35.79	0.59	0.78	0.82	0.85	0.88	0.91	0.94	0.97	0.11	0.08
ϕ_9	35.27	0.58	0.76	0.80	0.82	0.86	0.88	0.90	0.93	0.96	0.11
ϕ_{10}	34.93	0.57	0.75	0.78	0.81	0.84	0.86	0.88	0.91	0.94	0.97

TABLE VIII
DETECTION PERFORMANCES FOR THE BABOON IMAGE IN THE CASE OF RANDOM JPEG COMPRESSION

feature	PSNR	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}
ϕ_0	-	0.09	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02
ϕ_1	36.13	0.59	0.09	0.06	0.05	0.04	0.04	0.04	0.04	0.03	0.03
ϕ_2	35.71	0.58	0.91	0.09	0.06	0.05	0.05	0.04	0.04	0.03	0.03
ϕ_3	34.97	0.56	0.84	0.93	0.09	0.06	0.05	0.04	0.04	0.04	0.04
ϕ_4	34.15	0.54	0.77	0.85	0.93	0.09	0.06	0.05	0.05	0.04	0.04
ϕ_5	34.12	0.52	0.70	0.78	0.85	0.93	0.09	0.06	0.05	0.04	0.04
ϕ_6	33.85	0.50	0.65	0.71	0.78	0.85	0.93	0.09	0.06	0.05	0.05
ϕ_7	33.48	0.47	0.59	0.65	0.71	0.77	0.85	0.93	0.09	0.06	0.05
ϕ_8	33.33	0.44	0.54	0.59	0.64	0.69	0.76	0.84	0.93	0.09	0.06
ϕ_9	32.65	0.41	0.50	0.54	0.59	0.62	0.68	0.75	0.84	0.93	0.09
ϕ_{10}	32.88	0.39	0.46	0.49	0.53	0.56	0.61	0.67	0.75	0.84	0.94

since M_i is orthogonal and A_i is symmetric. Hence, from (13) we deduce

$$\tilde{\phi}_i = \phi_i - \frac{\phi_i^T \phi_i}{||\phi_i||^2} \phi_i = 0$$

and the proof is over. ■

As theoretically predicted by Proposition 3, the image reconstructed from a projected feature $\tilde{\phi}_i$ turns out to be heavily corrupted: this is evident from Figs. 2(c) and 3(c), which corresponds to $\tilde{\phi}_{10}$.

C. Robustness

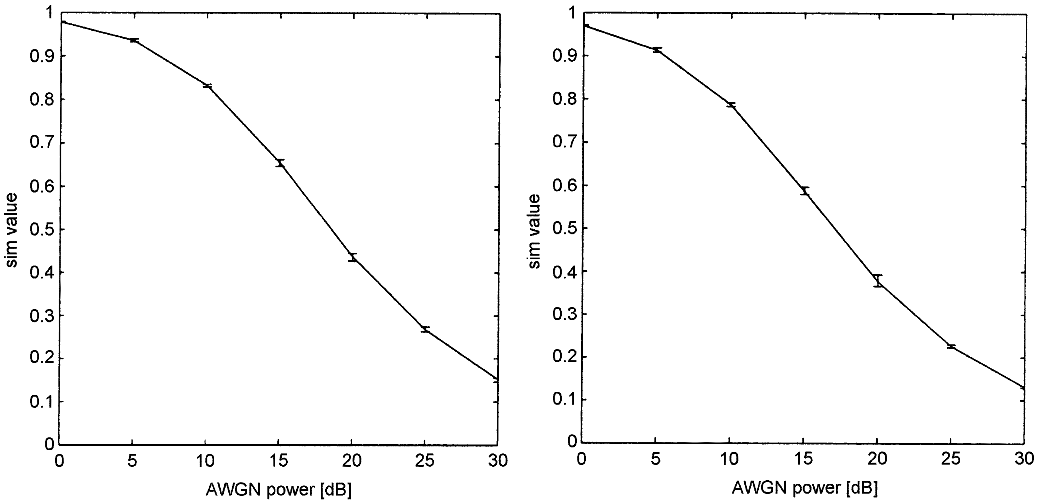
In order to prove that our method is also robust against some non malicious attacks (e.g., distortion due to basic operations such as storage, transmission, format conversion), we provide further experimental results. First, we repeat the previous watermarking procedure by adding at each stage a white Gaussian

TABLE IX
DETECTION PERFORMANCES FOR THE LENA IMAGE IN THE CASE OF JPEG80 COMPRESSION

feature	PSNR	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}
ϕ_0	-	0.11	0.03	0.03	0.03	0.03	0.03	0.02	0.02	0.02	0.02
ϕ_1	39.60	0.65	0.11	0.07	0.06	0.05	0.05	0.04	0.04	0.04	0.04
ϕ_2	38.78	0.62	0.90	0.10	0.08	0.06	0.05	0.05	0.04	0.04	0.04
ϕ_3	37.94	0.60	0.84	0.91	0.11	0.08	0.06	0.05	0.05	0.04	0.04
ϕ_4	37.25	0.58	0.80	0.87	0.93	0.10	0.07	0.06	0.05	0.05	0.04
ϕ_5	36.64	0.57	0.76	0.81	0.87	0.93	0.10	0.08	0.06	0.05	0.05
ϕ_6	36.11	0.55	0.72	0.77	0.82	0.87	0.93	0.11	0.08	0.06	0.05
ϕ_7	35.64	0.54	0.69	0.74	0.78	0.82	0.87	0.93	0.11	0.08	0.06
ϕ_8	35.21	0.53	0.67	0.71	0.75	0.78	0.83	0.87	0.93	0.11	0.07
ϕ_9	34.83	0.51	0.65	0.68	0.72	0.74	0.79	0.83	0.87	0.93	0.10
ϕ_{10}	34.45	0.50	0.62	0.66	0.68	0.72	0.75	0.78	0.82	0.88	0.93

TABLE X
DETECTION PERFORMANCES FOR THE BABOON IMAGE IN THE CASE OF JPEG80 COMPRESSION

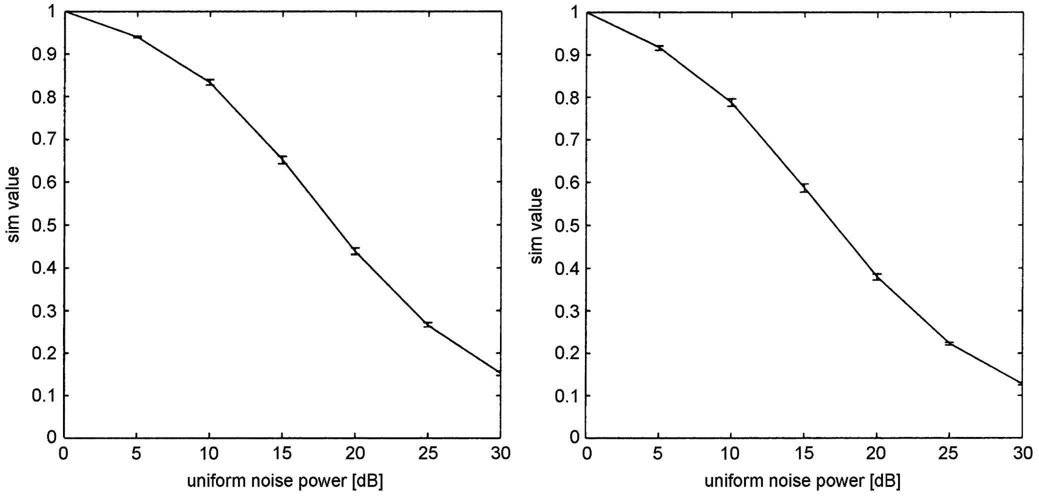
feature	PSNR	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}
ϕ_0	-	0.09	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02
ϕ_1	30.64	0.58	0.09	0.06	0.05	0.05	0.04	0.04	0.03	0.03	0.03
ϕ_2	30.53	0.55	0.86	0.09	0.06	0.05	0.05	0.04	0.04	0.03	0.03
ϕ_3	30.40	0.52	0.76	0.88	0.09	0.06	0.05	0.05	0.04	0.04	0.04
ϕ_4	30.27	0.49	0.68	0.77	0.89	0.09	0.06	0.05	0.05	0.04	0.04
ϕ_5	30.14	0.46	0.61	0.68	0.78	0.88	0.09	0.06	0.05	0.05	0.04
ϕ_6	30.02	0.43	0.55	0.61	0.69	0.78	0.89	0.09	0.06	0.05	0.05
ϕ_7	29.90	0.40	0.50	0.55	0.61	0.68	0.77	0.88	0.09	0.06	0.05
ϕ_8	29.78	0.38	0.46	0.50	0.54	0.60	0.68	0.77	0.89	0.09	0.06
ϕ_9	29.67	0.35	0.41	0.46	0.49	0.53	0.60	0.68	0.78	0.88	0.09
ϕ_{10}	29.56	0.33	0.38	0.42	0.44	0.48	0.53	0.59	0.68	0.77	0.88



(a) (b)

Fig. 5. Detection performance for (a) Lena and (b) Baboon carrying ten watermarks in the case of WGN addition with power ranging from 0 to 30 dB.

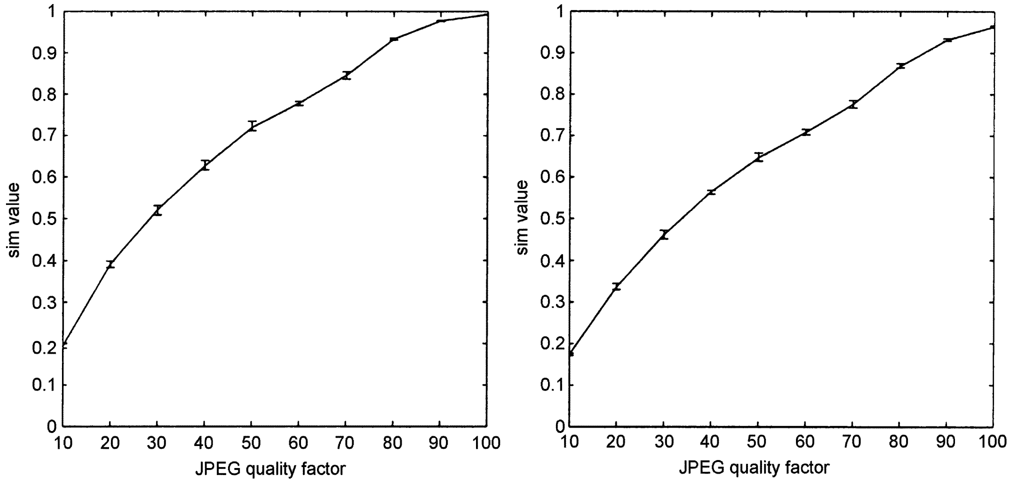
noise with a random power ranging between 0 and 15 dB, simulating a generic source of distortion that affects the image during its lifecycle. Indeed, in a scenario where a medical document passes through various laboratories and physicians, it is realistic to allow a different behavior of each user within a given tolerance. The corresponding sim values are reported in Tables III and IV for Lena and Baboon, respectively, showing that our method is able to distinguish watermarked from unwatermarked features in all cases, even in the presence of a considerable amount of noise (also after these distortions, the threshold ε can be chosen in a wide subrange of values: $[0.12,0.40] \subset [0.12,1]$). Moreover, we address the worst case, corresponding to white Gaussian noise addition with the same power 15 dB at each stage, and we report the results for Lena and Baboon in Tables V and VI, respectively. Secondly, we test the robustness of the method against JPEG compression. Tables VII and VIII show the detection performances by converting the image at each stage with a random JPEG quality factor ranging between 80 and 100, while Tables IX and X show the results if the quality factor is fixed to 80 (worst case). Notice that the JPEG compression affects in particular the first watermark insertion, due to the quantization. Thirdly, we provide some results testing the final images carrying ten watermarks. We compute the sim value (minimum, mean, and maximum among all watermarks averaged over 100 experiments) in the presence of different image degradation operators, in order to measure the robustness of the method. In Fig. 5, the relevant data are plotted for the Lena and Baboon images as a function of the WGN addition power



(a)

(b)

Fig. 6. Detection performance for (a) Lena and (b) Baboon carrying ten watermarks in the case of uniform noise addition with power ranging from 0 to 30 dB.



(a)

(b)

Fig. 7. Detection performance for (a) Lena and (b) Baboon carrying ten watermarks in the case of JPEG compression with quality factor ranging from 100 down to 10.

ranging from 0 to 30 dB. Analogously, we report in Fig. 6 the sim values in the case of uniform noise addition with power ranging from 0 to 30 dB. In both cases, it is possible to see that the detection still works in presence of powerful noise. Fig. 7 presents the experimental results corresponding to the Lena and Baboon images JPEG compressed with quality factor ranging from 100 down to 10: we stress that in all cases each watermark can be correctly detected. Some differences can be noticed in case of resizing. In Fig. 8, sim values are plotted as a function of the scaling factor where images are resized using bicubic interpolation. We observe that, due to its high frequencies spectrum, the Baboon image suffers under this manipulation and the detection does not work for scaling factors smaller than 0.6. Finally, we measure the robustness of the detection after 5 × 5 Gaussian lowpass filtering with standard deviation ranging from 0.1 to 1.1: results for the Lena and Baboon images are reported in Fig. 9.

IV. Conclusions

We have presented here a novel watermarking scheme, which allows to insert and reliably detect multiple watermarks sequentially embedded into a digital image, as it is required by challenging Digital Right Management applications such as confidential data tracing and shared property handling.

The proposed method, based on elementary linear algebra, is asymmetric, involving a private key for embedding and a public key for detection. Its robustness against standard image degradation operations (e.g., AWGN addition, JPEG compression, resizing, etc.) has been extensively tested and its security under projection attack has also been proven even though the envisaged applications refers to a collaborative environment, in which malicious attacks are not a critical aspect.

Future work will be devoted to the design of a non-collaborative version of the proposed method, addressing non trivial

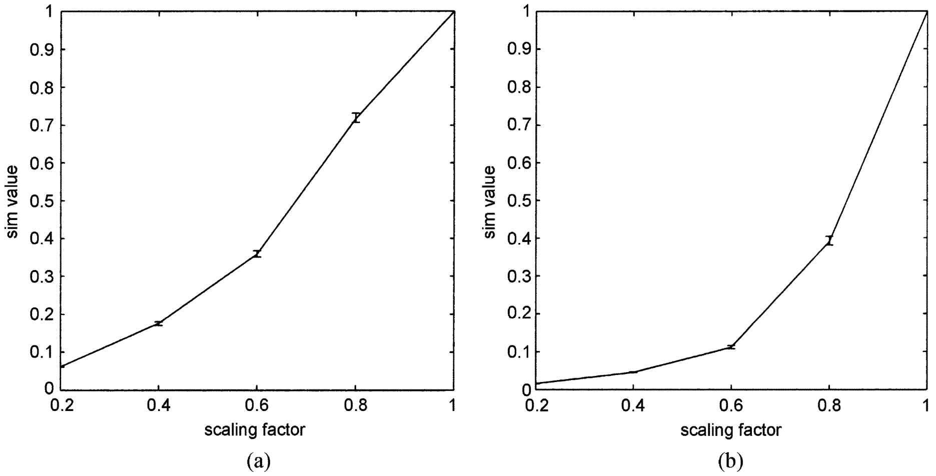


Fig. 8. Detection performance for (a) Lena and (b) Baboon carrying ten watermarks in the case of scaling with a factor ranging from 1 down to 0.2.

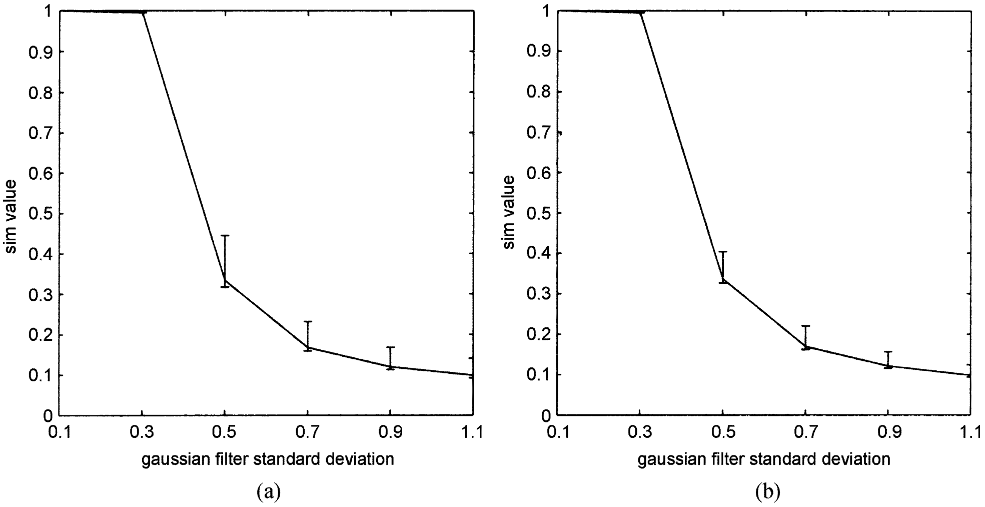


Fig. 9. Detection performance for (a) Lena and (b) Baboon carrying ten watermarks in the case of 5 × 5 Gaussian low-pass filtering with standard deviation ranging from 0.1 to 1.1.

related problems such as the collusion attack and a security evaluation from an information-theoretic point of view.

Appendix

Theorem 1: Let V be a vector space of dimension r and for $i = 1, \dots, m$ let V_i be a vector subspace of V. We have

$$\dim\left(\bigcap_{i=1}^{m} V_i\right) \geq \sum_{i=1}^{m} \dim V_i - (m-1)r.$$

Proof: By induction on m. For $m = 2$, we have to check that

$$\dim(V_1 \cap V_2) \geq \dim(V_1) + \dim(V_2) - r \tag{14}$$

which is a direct consequence of the well-known Grassmann formula. Assume now that the claim holds for $m - 1$ and we need to prove that it holds also for m. By applying (14), we obtain

$$\begin{aligned}\dim\left(\bigcap_{i=1}^{m} V_i\right) &= \dim\left(\bigcap_{i=1}^{m-1} V_i \cap V_m\right)\\ &\geq \dim\left(\bigcap_{i=1}^{m-1} V_i\right) + \dim(V_m) - r\\ &\geq \sum_{i=1}^{m-1} \dim V_i - (m-2)r + \dim(V_m) - r\\ &= \sum_{i=1}^{m} \dim V_i - (m-1)r\end{aligned}$$

so the proof is over. ■

Corollary 1: If $\dim V = d$ and $\dim V_i = d - k - 1$ for every $1 \leq i \leq n-1$ then

$$\dim\left(\bigcap_{i=1}^{n-1} V_i\right) \geq d - (k+1)(n-1)$$

In particular, if (1) holds then

$$\dim\left(\bigcap_{i=1}^{j} V_i\right) \geq \dim\left(\bigcap_{i=1}^{n-1} V_i\right) \geq 1$$

for every $j \leq n-1$.

References

[1] C. Busch and S. D. Wolthusen, "Tracing data diffusion in industrial research with robust watermarking," in *Proc. IEEE 4th Workshop on Multimedia Signal Processing 2001*, 2001, pp. 207–212.

[2] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, and R. Collorec, "Relevance of watermarking in medical imaging," in *Proc. IEEE EMBS Int. Conf. Information Technology Applications in Biomedicine 2000*, 2000, pp. 250–255.

[3] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "A multiple watermarking scheme applied to medical image management," in *Proc. IEEE Int. Conf. Engineering in Medicine and Biology Society 2004*, 2004, vol. 2, pp. 3241–3244.

[4] ——, "Multiple image watermaking applied to health information management," *IEEE Trans. Inf. Technol. Biomed.*, vol. 10, no. 4, pp. 722–732, Oct. 2006.

[5] M. Li, S. Narayanan, and R. Poovendran, "Tracing medical images using multi-band watermarks," in *Proc. 26th Ann. Int. Conf. Engineering in Medicine and Biology Society 2004*, 2004, vol. 2, pp. 3233–3236.

[6] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[7] F. Mintzer and G. W. Braudaway, "If one watermark is good, are more better?," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing 1999*, Mar. 1999, vol. 4, pp. 2067–2069.

[8] S. Stankovic, I. Djurovic, and I. Pitas, "Watermarking in the space/spatial-frequency domain using two-dimensional radon-wigner distribution," *IEEE Trans. Image Process.*, vol. 10, no. 4, pp. 650–658, Apr. 2001.

[9] C.-T. Hsu and J.-L. Wu, "Hidden digital watermarks in images," *IEEE Trans. Image Process.*, vol. 8, no. 1, pp. 58–68, Jan. 1999.

[10] P. H. W. Wong, O. C. Au, and Y. M. Yeung, "A novel blind multiple watermarking technique for images," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 813–830, Aug. 2003.

[11] C.-S. Woo, J. Du, and B. Pham, "Multiple watermark method for privacy control and tamper detection in medical images," in *Proc. Workshop on Digital Image Computing 2005*, 2005.

[12] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "A medical image watermarking scheme based on wavelet transform," in *Proc. 25th Ann. Int. Conf. IEEE-EMBS 2003*, 2003, pp. 856–859.

[13] C.-S. Lu and H.-Y. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Trans. Image Process.*, vol. 10, pp. 1579–1592, Oct. 2001.

[14] Z.-M. Lu, D.-G. Xu, and S.-H. Sun, "Multipurpose image watermarking algorithm based on multistage vector quantization," *IEEE Trans. Image Process.*, vol. 14, no. 6, pp. 822–831, Jun. 2005.

[15] G. Boato, F. G. B. De Natale, and C. Fontanari, "An improved asymmetric watermarking scheme suitable for copy protection," *IEEE Trans. Signal Process.*, vol. 54, pp. 2833–2834, Jul. 2006.

[16] P. H. W. Wong, A. Chang, and O. C. Au, "A sequential multiple watermarks embedding technique," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing 2004*, May 2004, vol. 3, pp. 393–396.

[17] A. Piva, M. Barni, F. Bartolini, and A. De Rosa, "Data hiding technologies for digital radiography," *IEE Proc. Vision, Image, and Signal Processing*, vol. 152, pp. 604–610, Oct. 2005.

Giulia Boato (S'03–M'06) received the Laurea degree in mathematics in 2002 and the Ph.D. in information and communication technologies in 2005, both from the University of Trento, Italy.

In 2006, she was a Visiting Researcher at the University of Vigo, Spain. Currently, she is Assistant Professor of telecommunications at the University of Trento, working in the Multimedia Communications Laboratory. Her research interests are focused on image and signal processing, with particular attention to multimedia data protection and data hiding.

Francesco G. B. De Natale (M'96–SM'03) received the Laurea degree in electronic engineering in 1990 and the Ph.D. in telecommunications in 1994, both from the University of Genoa, Italy.

In 1995–1996, he was Visiting Professor at the University of Trento, Italy, and from 1996 to 1999, Assistant Professor at the University of Cagliari, Italy. He is currently Full Professor of telecommunications at the University of Trento, where he coordinates the didactic activities of the Bachelor and Master Courses in telecommunications engineering. He is Deputy Head of the Department of Information and Communication Technologies, where he leads the research activities of the Multimedia Communications Lab. His research interests are focused on image and signal processing, with particular attention to multimedia data compression, processing and transmission.

Prof. De Natale was General Co-Chair of the Packet Video Workshop in 2000, and Technical Program Co-Chair of the IEEE International Conference on Image Processing (ICIP) in 2005. In 1998, he was co-recipient of the IEEE Chester-Sall Best Paper Award.

Claudio Fontanari received the Laurea degree in mathematics from Trento University, Italy, and the Ph.D. in mathematics from Scuola Normale Superiore, Pisa, Italy.

He is currently Assistant Professor, Department of Mathematics, Third School of Engineering – Information Technologies, Politecnico di Torino, Italy. His research interests lay in the field of algebraic geometry and its applications.