UNIVERSITY
OF TRENTO

DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

38050 Povo – Trento (Italy), Via Sommarive 14
http://www.dit.unitn.it

A MULTILEVEL ASYMMETRIC SCHEME FOR DIGITAL FINGERPRINTING

G. Boato, F.G.B. De Natale, and C. Fontanari

November 2005

Technical Report DIT-05-068

A Multilevel Asymmetric Scheme for Digital Fingerprinting

G. Boato[1] *, F. G. B. De Natale[1] and C. Fontanari[2]

[1]Dept. of Information and Communication Technology, University of Trento,

Via Sommarive 14, I-38050, Trento, Italy, tel +39 0461 883917, fax +39 0461 882093

[2]Dept. of Mathematics, Fac. of Information Engineering, Politecnico di Torino,

Corso Duca degli Abruzzi 24, I-10129, Torino, Italy, tel +39 011 5647567 fax +39 011 5647599

boato@dit.unitn.it; denatale@ing.unitn.it; claudio.fontanari@polito.it

Abstract

The present paper proposes an asymmetric watermarking scheme suitable for fingerprinting and precision-critical applications. The method is based on linear algebra and is proved to be secure under projection attack. The problem of anonymous fingerprinting is also addressed, by allowing a client to get a watermarked image from a server without revealing her/his own identity. In particular, we consider the specific scenario where the client is a structured organization being trusted as a whole but involving possibly untrusted members. In such a context, where the watermarked copy can be made available to all members, but only authorized subgroups should be able to remove the watermark and recover a distortion-free image, a multilevel access to the embedding key is provided by applying Birkhoff polynomial interpolation. Extensive simulations demonstrate the robustness of the proposed method against standard image degradation operators.

I. Introduction

Digital watermarking techniques have raised a great deal of interest in the scientific community after the pioneering contribution by Cox et al. [1] (see for instance the books [2], [3], [4], and the references therein). The practice of imperceptible alteration of a document to embed a message into it plays a key role in the challenging field of copyright and copy protection and motivates the search for more efficient solutions. Here we investigate a novel asymmetric watermarking scheme based on elementary linear algebra which, besides standard robustness requirements, satisfies non trivial security and invertibility properties[1].

Indeed, watermarking security is arising a great deal of interest in both academy and industry (see for instance [6], [7], and [9]). The analogy with public key cryptography suggests to consider asymmetric structures, involving

[1]A preliminary version of this method has been presented in [5].

a private key for embedding and a public key for detection (see [8] for a detailed survey). However, this property is by no means sufficient in order to make a watermarking scheme secure: as remarked in [7], § 5, almost all available asymmetric watermarking schemes can be defeated by a standard closest point or projection attack (see Section IV below for details). On the contrary, the proposed method is definitely secure under projection attack, as we both mathematically prove and experimentally verify.

On the other hand, watermarking invertibility is crucial for several applications where the image integrity should not be irreversibly corrupted by the watermark insertion. This new paradigm has been the subject of both deeply theoretical and application oriented investigations (see for instance [10] and [11]) and is still a very active research area (see [12] and [13]). Specific applications include attribution of medical images for clinical purposes, copyright protection of biological or satellite images, personal identification via fingerprinting or iris matching. The designed scheme allows to completely remove the watermark and recover a distortion-free image by exploiting the knowledge of the embedding key. In order to ensure the access to the original image only to authorized groups, we propose to manage the embedding key in a distributed way. In [14] multilevel access is provided for precision-critical images in a hierarchical context, while the proposed scheme allows on-off access for authorized or non-authorized groups by applying a secret sharing scheme. The basic theory due to Shamir ([15]) relies on standard Lagrange interpolation, while the hierarchical secret sharing scheme by Tassa ([16]) exploits subtler properties of Birkhoff polynomial interpolation. Here we are going to adapt and simplify this last approach for the hierarchical management of the embedding key, thus extending the results presented in [17] for the joint ownership of the original image. Even though the mathematical framework is essentially the same, we point out that the application scenario is completely different.

The present contribution addresses a problem of anonymous fingerprinting. Indeed, the proposed method allows a client to get a watermarked image from a server without revealing her/his own identity. In the specific case of biometric images, where a distorsion-free copy is needed for precision-critical applications, we consider the scenario where the client is a structured organization being trusted as a whole but involving possibly untrusted members. In such a context, the watermarked copy can be made available to all members, but only authorized subgroups should be able to remove the watermark. Just to outline a realistic example where all the above ingredients are involved, let us introduce a biometric laboratory which, after a long and careful work employing very expensive machinery, has completed a high precision medical atlas and offers it to a publisher with the task of selling it to as many as possible members of the scientific community. In this scenario, our innovative scheme allows any research team to buy the access to the atlas in an anonymous way from the publisher, who provides each research group with a watermarked copy and each member of the group with a share of the embedding key proportional to her/his position in the group hierarchy. In such a way, individual use for applications where precision is not

critical (for instance, teaching purposes) is admitted under the research group responsibility (indeed, the insertion of a conventional watermark allows the authors of the atlas to discover and point out any leak to the publisher without violating the privacy of the clients). On the other hand, any trusted authorized subgroup of the buyer team by putting together the shares of its members is able to reconstruct a non-watermarked copy of the atlas for high precision reasearch purposes.

We also stress that our approach substantially improves previous asymmetric schemes applying linear algebra. Indeed, the eigenvector watermarking scheme introduced in [18] has been defeated by an effective attack (see [19], Section 4.4) and the method presented in [20] is subject to malicious disabilitation of public detection (see [20], Section III.B). On the other hand, the scheme proposed in [21] is proven to be secure under projection attack. Unfortunately, in order to achieve such a property, the watermark cannot be chosen arbitrarily, but it turns out to be heavily dependent on the host image (see in particular statement c) of the Theorem on p. 787, which shows that the watermark is forced to be a suitable multiple of a sequence deterministically extracted from the original image). As a consequence, the method of [21] is appropriate just for copyright protection, where only one key is assigned to each image, but definitely not for fingerprinting, where every recipient is identified by its own key. On the contrary, our approach is suitable also for fingerprinting, allowing the insertion into any image of an arbitrary watermarking sequence. Of course, the application of a watermarking scheme for copy control requires a reasonable robustness against standard image degradation operators. This is experimentally investigated in Section IV on two sets of biometric images of different size and characteristics with quite satisfactory results in both cases. The embedded watermark can be detected even in presence of a relevant amount of image degradation due to image processing operators, such as filtering, compression, noise addition, etc., and combination of them.

The structure of the paper is the following: in Section II we give a detailed description of the proposed watermarking method; in Section III we discuss an anonymous fingerprinting scenario involving a hierarchical access to the embedding key in a rigorous mathematical framework; in Section IV we address watermark invertibility for precision-critical images, security under projection attack and robustness against several image degradation operators; finally in Section V we draw some concluding remarks.

II. Linear algebra watermarking

We are going to describe a subspace asymmetric watermarking procedure. In this kind of asymmetric watermarking scheme the encoding and decoding algorithms as well as the detection key are public, while the embedding key is kept secret. Let us fix an integer $n \geq 1$ and a feature space $\mathcal{X}$ (for instance, the space corresponding to the entries in the top left corner of the DCT) and decompose it into two orthogonal subspaces $\mathcal{W}$ of dimension $2n$ and $\mathcal{V}$. Next, we split $\mathcal{W}$ into two orthogonal subspaces $\mathcal{G}$ and $\mathcal{H}$ of dimension n and we choose matrices G and H whose columns form an orthonormal basis of $\mathcal{G}$ and $\mathcal{H}$, respectively. Finally, we pick an arbitrary watermarking

sequence $w \in \mathbb{R}^n$.

Let $\phi_o \in \mathcal{X}$ be the feature vector associated to the original image. We write

$$\phi_o = \psi_o + \sigma_o \tag{1}$$

where $\psi_o \in \mathcal{W}$ and $\sigma_o \in \mathcal{V}$, and

$$\psi_o = Gs + Ht \tag{2}$$

The watermark embedding is defined by

$$\phi_w = \phi_o + Gw \tag{3}$$

where G is the embedding key (see Figure 1).

Next we choose a symmetric matrix A (i.e., $A^T = A$) satisfying

$$A(s + w) = s + w \tag{4}$$

and an orthogonal matrix B (i.e., $B^T = B^{-1}$) satisfying

$$Bt = \mu(s + w) \tag{5}$$

with $\mu := \|t\|/\|s + w\|$ and we define

$$D = AG^T + \mu BH^T \tag{6}$$

which is released to the public and is the crucial ingredient in the detection phase (see Figure 2). As far as B is concerned, we point out the following easy fact.

Lemma 1: If $s + w \neq 0$, then we can construct an orthogonal matrix B satisfying (5).

Proof: See Appendix.

The existence of A is ensured by the trivial choice A=I (the identity matrix), as already pointed out in [5]. However, in order to obtain higher detection performances we propose here a different choice for A. Namely, let $b_1 := \frac{s+w}{\|s+w\|}$, complete it to an orthonormal basis $(b_1, b_2, \ldots, b_n)$ of $\mathbb{R}^n$ (for instance, complete it to an arbitrary basis and then apply the standard Gram-Schmidt orthonormalization process) and let N be the matrix with b_i^T as the i-th column ($i = 1, \ldots, n$). Fix now an integer $k \geq 3$ and let

$$A = N \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 10^k & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \ldots & 0 & 10^k \end{pmatrix} N^T.$$

Hence A keeps $(s + w)$ fixed and rescales norms of vectors in all other directions in order to minimize false-positive probability.

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

$$\delta(\phi_e) = \begin{cases} 1 & \textit{if } |\mathrm{sim}(s+w, D\phi_e)| \geq \varepsilon \\ 0 & \textit{otherwise} \end{cases} \tag{7}$$

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

$$\mathrm{sim}(s+w, D\phi_e) = \begin{cases} \frac{(s+w)^T D\phi_e}{\|s+w\|\|D\phi_e\|} & \textit{if } D\phi_e \neq 0 \\ 0 & \textit{if } D\phi_e = 0 \end{cases} \tag{8}$$

Definitions (7) and (8) for the detector are motivated by the following result, which shows that the watermark is perfectly detected in the feature vector associated to the watermarked image.

Proposition 1: We have $\mathrm{sim}(s+w, D\phi_w) = 1$.

Proof: See Appendix.

Notice that the detector needs only the matrix D and the vector $s+w$. Therefore, if we take (G, H, A, B) as a secret key and $(D, s+w)$ as a public key, we obtain an asymmetric watermarking scheme.

III. Fingerprinting applications

In order to adapt the above watermarking scheme to anonymous fingerprinting, let us introduce an authority A, a client C and a server S. The role of A is to provide a safe bridge between C and S ensuring both the privacy of C and the security of S. More explicitly, A receives from C the request of an image and from S the corresponding original image. Next, A associates to C a conventional watermark w and produces the watermarked image by using the secret key (G, H, A, B). Finally, A distributes to C the watermarked image and to S the public key $(D, s+w)$. As a consequence, S is able to recognize a non-authorized use of the image without violating the privacy of C.

We stress that, in order to be sure that C and not another user is responsible of a violation it is essential that the watermarked image is kept secret and the proposed method enjoys such a property. On the other hand, in the case where C is a trusted hierarchical group, the embedding key G can be distributed to C in a hierarchical way in order to allow watermark removal only to authorized subgroups (see for instance [14] for the case of precision-critical images).

More precisely, let C be a group composed of h participants and let us consider a collection Γ of subsets of C, which is monotone in the sense that if $U \in \Gamma$ then any set containing U also belongs to Γ. A threshold secret sharing scheme with access structure Γ is a method of sharing a secret among all members of C, in such a way that only subsets in Γ can recover the secret, while all other subsets have no information about it. Assume that C is divided into levels, i.e. $C = \cup_{l=0}^{t} U_l$ with $U_i \cap U_j = \emptyset$ for every $i \neq j$. In order to reconstruct the secret, we require at least a fixed number of shares from each level. Formally, if $0 < k_0 < \ldots < k_t$ is a strictly increasing sequence of integers, then a $(k_0, \ldots, k_t; h)$-hierarchical threshold secret sharing scheme distributes to each participant a share

of a given secret s, in such a way that

$$\Gamma = \left\{V \subset U : \#\left[V \cap \left(\cup_{l=0}^{i} U_l\right)\right] \geq k_i \quad \forall i = 0, \ldots, t\right\}$$

Roughly speaking, a subset of participants can reconstruct the secret if and only if it contains at least k_0 members of level 0, at least k_1 members of level 0 or level 1, at least k_2 members from levels 0, 1, and 2, and so on.

In order to construct a suitable $(k_0, \ldots, k_t; h)$-hierarchical threshold secret sharing scheme for the embedding key G, it is natural to apply Birkhoff polynomial interpolation. The key point is that the Birkhoff scheme involves not only a polynomial, but also its (higher order) derivatives. To be formal, as in in [22], p. 124, let $E = (E_{i,j})$, $i = 1, \ldots, m$; $j = 0, \ldots, d-1$, be an $m \times d$ interpolation matrix, whose elements are zeros or ones, with exactly d ones. Let $X = x_1, \ldots, x_m$, $x_1 < x_2 < \ldots < x_m$, be a set of m distinct interpolation points. For polynomials

$$P(x) = \sum_{i=0}^{d-1} a_i x^i$$

of degree $\leq d-1$ we consider the d interpolation equations

$$P^{(j)}(x_i) = B_{i,j}$$

for $E_{i,j} = 1$, where $P^{(j)}$ denotes the j-th derivative of P and $B_{i,j}$ are given data. Here the unknowns are the d coefficients $a_0, \ldots, a_{d-1}$ of $P(x)$. However, it is easy to convince ourselves that a Birkhoff interpolation problem can admit infinitely many solutions even if the number of equations equals the number of unknowns. Indeed, think for a moment at the case in which $E_{i,0} = 0$ for every $i = 1, \ldots, h$. In such a case, the interpolation system involves only derivatives of the polynomial P, hence it keeps no track of the constant term a_0, which remains undetermined. More generally, elementary linear algebra considerations show that if a Birkhoff interpolation problem admits a unique solution then its associated interpolation matrix $E = (E_{i,j})$, $i = 1, \ldots, d$; $j = 0, \ldots, d-1$, has to satisfy the following Pólya condition

$$\#\left\{E_{i,j} = 1 : j \leq h\right\} \geq h+1 \quad 0 \leq h \leq d-1$$

(see for instance p. 126 of [22]).

The idea now is to exploit this necessary condition in order to ensure that only authorized subsets can access the secret matrix G. Intuitively speaking, an evaluation of the polynomial itself carries more information than an evaluation of any of its derivatives since it involves more coefficients; therefore it sounds reasonable to assign to a participant of higher level the evaluation of a lower order derivative. More precisely, we propose the following algorithm (see Figure 4):

1) Protect the matrix G with a secret key consisting of a sequence $s = (s_0, \ldots, \ s_z)$ with $s_i \in \mathbb{R}$ for every $0 \leq i \leq z$.

2) Let $d = k_t$ and pick a polynomial

$$P(x) = \sum_{i=0}^{d-1} a_i x^i$$

where $a_i = s_i$ for every $0 \leq i \leq z$ and a_i arbitrary elements of $\mathbb{R}$ for $z+1 \leq i \leq d-1$.

3) Identify each participant of level l with a random element $u \in \mathbb{R}$ and associate to u the share $P^{(k_{l-1})}(u)$, where $P^{(k)}$ denotes as above the k-th derivative of P and $k_{-1} := 0$.

Fix now a subset of the structured group $V := \{u_1, \ldots, \ u_m\} \subset A$ with $m \geq d$. Up to reordering we may assume that $u_i \in U_{l(i)}$ with $l(i) \leq l(j)$ for every $i \leq j$. Consider the $m \times d$ matrix M_V whose i-th row is given by

$$\frac{d}{dx^{k_{l(i)-1}}} \left(1, x, x^2, \ldots, x^{(d-1)}\right)(u_i) \tag{9}$$

In order to reconstruct the secret sequence s, the members of V have to solve the following linear system:

$$M_V \begin{pmatrix} a_0 \\ \vdots \\ a_{d-1} \end{pmatrix} = \begin{pmatrix} P^{k_{l(1)-1}}(u_1) \\ \vdots \\ P^{k_{l(m)-1}}(u_m) \end{pmatrix} \tag{10}$$

in the unknowns $a_0, \ldots, a_d$.

The key point is that (10) is a Birkhoff interpolation problem with associated interpolation matrix $E_V = (E_{i,j})$, $i = 1, \ldots, m$; $j = 0, \ldots, d-1$ defined as follows:

$$E_{i,j} = \begin{cases} 1 \ \textit{if} \ j = k_{l(i)-1} \\ 0 \ \textit{otherwise} \end{cases} \tag{11}$$

In the following, we will provide two theorems that represent the theoretical framework for reconstruction of s. Both theorems are based on the fact that $V \in \Gamma$ if and only if E_V satisfies the Pólya condition.

Theorem 1: If $V \notin \Gamma$ then V cannot reconstruct the secret sequence s.

Proof: See Appendix.

Moreover, we can apply Theorem 10.1 in [22], p.128, whose statement can be rephrased as follows:

Proposition 2: A Birkhoff interpolation problem admits a unique solution for almost all choices of interpolation points $x_1, \ldots, x_m$, i. e. outside of a subset of $\mathbb{R}^m$ with m-dimensional measure zero, if and only if it satisfies the Pólya condition.

Hence our random selection of the interpolation points allows us to deduce the following:

Theorem 2: If $V \in \Gamma$ then V recovers the secret sequence s.

Proof: See Appendix.

As a consequence, a set of participants of the hierarchical group C can reconstruct the secret sequence s, hence access the matrix G and finally remove the watermark, if and only if it belongs to the predefined access structure.

IV. Invertibility, security and robustness analysis

Standard watermarking techniques based on lossy compression such as least significant bit watermarking present a possible drawback. Indeed, the manipulation of the image introduce a small amount of distortion which irreversibly impacts its integrity. Although the changes are imperceptible, they need to be avoided in some precision-critical applications, in particular for biomedical images, due to legal or scientific reasons.

In the proposed asymmetric watermarking scheme the knowledge of the embedding key G and the watermarking sequence w allows to remove the watermark and therefore to recover the original image in a distortion-free way as follows

$$\phi_o = \phi_w - Gw \tag{12}$$

(see Figure 3). Extensive tests of watermark removal confirm that the recovered image is identical pixel per pixel to the original one.

We point out that, even though it is not part of the public key of the method, w can be published without occurring in additional security problems. Here security of the watermark refers to the inability by not authorized users to decode the embedded sequence. As discussed in [7], § 5, the crucial test for asymmetric watermarking security is represented by the projection attack. As explained in [21], III.B., p. 786, a projection attack replaces the feature vector ϕ_w associated to the watermarked image with a feature vector $\tilde{\phi}$ satisfying

$$\|\tilde{\phi} - \phi_w\| = \min \|\phi - \phi_w\|^2 \tag{13}$$

under the constraint

$$\delta(\phi) = \mathrm{sim}(s + w, D\phi) = 0 \tag{14}$$

Hence, $\tilde{\phi}$ is the non-watermarked feature vector closest to ϕ_w. By definition (8), condition (14) says that $(s + w)^T D\phi = 0$, i.e., ϕ has to lie on the hyperplane through the origin of the feature space having normal vector $a = D^T(s + w)$. As a consequence, the feature vector $\tilde{\phi}$ satisfying condition (13) is the projection of ϕ_w onto this hyperplane, which is given by

$$\tilde{\phi} = \phi_w - \frac{a^T \phi_w}{\|a\|^2} a \tag{15}$$

The main result of [5] is the following:

Theorem 3: For every choice of the watermark w, our scheme is secure under projection attack.

Proof: See Appendix.

Figures 5 (c) and 11 (c) show the effect of a projection attack on a couple of sample images (Figures 5 (b) and 11 (b)). The resulting degradation is apparent (PSNR 15.9 and 16.4, respectively).

We stress that the corresponding result in [21] implies that w is a multiple of s (see statement c) of the Theorem on p. 787). On the contrary, the security of our scheme does not depend on a specific watermark, thus making it suitable also for fingerprinting.

Robustness of our asymmetric watermarking scheme against standard image degradation operators and combination of them can be evaluated by simulations. We consider biometric images of different size and with different characteristics and we run our experiments on two skew databases.

The first one contains 20 biomedical and biometric images, including human brain samples and irides for identification purposes, of size 450×430 on average. In order to implement the embedding procedure, we choose $\mathcal{X}$ as the subspace corresponding to a 32×32 submatrix in the upper-left corner of the DCT of the original image. Next, we split $\mathcal{X}$ into $\mathcal{W}$, corresponding to the upper-left 20×20 submatrix, and its complementary subspace $\mathcal{V}$. Finally, we define $\mathcal{G}$ by randomly selecting half entries of $\mathcal{W}$ and $\mathcal{H}$ by taking the remaining ones. In order to construct matrices G and H we simply orthonormalize random basis of $\mathcal{G}$ and $\mathcal{H}$, respectively. We always set $k = 3$ and consider randomly generated watermark sequences of length $n = 200$, suitably scaled to meet imperceptibility (see Figures 5 (b)).

First, an image of a iris (Figures 5 (a)) is watermarked and detection responses for 100 different watermarks are investigated after the following attacks: additive white Gaussian noise with power 15 dB; additive uniform noise in the interval $[-20, 20]$; 3×3 moving average; Gaussian lowpass filtering of size 3×3 with standard deviation 0.5; median filtering using the 3-by-3 neighborhood; resizing of a linear factor of 0.6 using the nearest neighbor interpolation method; JPEG compression with quality factor 25%; 3×3 moving average and additive uniform noise in the interval $[-20, 20]$; additive white Gaussian noise with power 15 dB and JPEG compression with quality factor equal to 25%. Despite the different typology of the tested images and operations, detection works perfectly in all cases. Indeed, the really embedded watermark is always identified by a peak in the plot of sim values (see Figures 6 and 7).

Next, $\varepsilon = 0.06$ is set and the probability of detection is evaluated after a JPEG compression as a function of the quality factor on a database of 20 images and 10 different watermarks per image. The results summarized in Figure 8 show that detection probability equals 1 for JPEG compression quality factor down to 20. Such performances seem to outperform those reported in [8], Figure 6, where the detection probability for quality factor 20 is always less than 0.3. A similar analysis for white Gaussian noise addition as a function of its power is reported in Figure 9, where detection probability equals 1 for AWGN power up to 20 dB.

Finally, the false positive probability is measured by considering 20 unwatermarked images and 10 different watermarks per image and letting the detection threshold ε vary down to 0 (see Figure 10). False positive probability is definitely under $1/200$ for every $\varepsilon \geq 0.18$, thus improving the performances described in [21], Figure 6.

The same set of tests are also run considering much smaller biometric images representing faces (see for instance

Figure 11 (a)) of size 150×190 on average. In this case we have to reset all parameters and we choose $\mathcal{X}$ as the subspace corresponding to a 15×15 submatrix in the upper left corner of the DCT of the original image. Next, we split $\mathcal{X}$ into $\mathcal{W}$, corresponding to the upper left 10×10 submatrix, and its complementary subspace $\mathcal{V}$. Finally, we define $\mathcal{G}$ by randomly selecting half entries of $\mathcal{W}$ and $\mathcal{H}$ by taking the remaining ones. The matrices G and H are constructed as in previous experimental setting, by simply orthonormalizing random bases of $\mathcal{G}$ and $\mathcal{H}$ and the experiments are performed on a database of 40 faces. We set $k = 3$ and consider randomly generated watermark sequences of length $n = 50$, suitably scaled to meet imperceptibility (see Figure 11 (b)).

Figures 12 and 13 report detection responses considering Figure 11 (a) watermarked with 100 different watermarks and the same attacks as for Figure 5 (a). Also with such a different database, detection works perfectly in all cases. Indeed, the really embedded watermark is always identified by a peak in the plot of sim values.

Figure 14 reports detection probability after JPEG compression as a function of the quality factor on a database of 40 images and 10 different watermarks per image ($\varepsilon = 0.035$): also in this case, detection probability equals 1 for JPEG compression quality factor down to 20. A similar analysis for white Gaussian noise addition as a function of its power is reported in Figure 15 ($\varepsilon = 0.035$): exactly as for the previous database, detection probability equals 1 for AWGN power up to 20 dB.

Finally, the false positive probability is measured by considering 40 unwatermarked images and 10 different watermarks per image and letting the detection threshold ε vary down to 0 (see Figure 16). Once again, false positive probability becomes definitely negligible for every $\varepsilon \geq 0.12$. We point out that requiring false positive probability close to zero would cause a few missed detections in the tests of Figures 6 and 7, as well as of Figures 12 and 13. Nevertheless, those cases correspond to heavy attacks (e.g. combined operators) that would make anyway unusable the images for sensitive applications.

V. Conclusion

We present an asymmetric watermarking scheme which is robust against the most dangerous attack for asymmetric schemes, namely, the projection attack. Moreover, the proposed scheme is suitable for fingerprinting, allowing the insertion of an arbitrary watermarking sequence, and for precision-critical applications, guaranteeing the recovery of a distortion-free image. The problem of anonymous fingerprinting is also addressed, in particular we consider the scenario where the client is a structured organization. Accordingly, a multilevel access to the watermarking removal procedure is provided, by exploiting advanced mathematical tools from the theory of Birkhoff polynomial interpolation. Finally, our experimental results demonstrate robustness of the method against standard image degradation operations.

Future work will deal with the optimal choice of the watermark embedding domain with respect to robustness to geometric attacks and specific legal applications.

VI. APPENDIX

Here we provide detailed proofs of our mathematical results.

Proof: [Lemma 1] If $t = 0$, just take B equal to the identity matrix. For $t \neq 0$, let $a_1 := \frac{t}{\|t\|}$ and $b_1 := \frac{s+w}{\|s+w\|}$ and complete them to orthonormal bases $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ of $\mathbb{R}^n$. If M (resp., N) is the matrix with a_i^T (resp., b_i^T) as the i-th column ($i = 1, \ldots, n$), then $M(1, 0, \ldots, 0)^T = a_1^T$ and $N(1, 0, \ldots, 0)^T = b_1^T$. The matrix $B := NM^T$ is orthogonal since it is product of orthogonal matrices and $Ba_1^T = NM^T a_1^T = N(1, 0, \ldots, 0)^T = b_1^T$, so (5) holds. ■

Proof: [Proposition 1] ¿From definitions (6), (3), (1), (2) it follows that $D\phi_w = (AG^T + \mu BH^T)(Gs + Ht + \sigma_o + Gw) = A(s + w) + \mu Bt = (1 + \mu^2)(s + w)$ by conditions (4) and (5). Hence from (8) we deduce

$$\mathrm{sim}(s + w, D\phi_w) = \frac{(1 + \mu^2)(s + w)^T(s + w)}{(1 + \mu^2)\|s + w\|^2} = 1$$

■

Proof: [Theorem 1] Since $V \notin \Gamma$, E_V doesn't satisfies Pólya condition and it follows that the corresponding Birkhoff interpolation problem admits infinitely many solutions. Thus V cannot reconstruct s. ■

Proof: [Theorem 2] Since $V \in \Gamma$, E_V satisfies Pólya condition and with a random selection of interpolation points it is possible to apply Proposition 1. Thus the unique solution of the Birkhoff interpolation problem conveys the secret: $s_i = a_i$ for $i \leq z \leq d - 1$. ■

Proof: [Theorem 3] By (6) we have $a = D^T(s + w) = (GA^T + \mu HB^T)(s + w) = G(s + w) + Ht$ since $A^T(s + w) = A(s + w) = s + w$ by (4) and $\mu B^T(s + w) = t$ by (5). On the other hand, if we let $\psi_w = \phi_w - \sigma_o$, from (3), (1), (2) it follows that $\psi_w = \phi_o + Gw - \sigma_o = Gs + Ht + \sigma_o + Gw - \sigma_o = G(s + w) + Ht$. Hence we see that $a = \psi_w$ and from (15) we deduce

$$\tilde{\phi} = \phi_w - \frac{\psi_w^T \phi_w}{\|\psi_w\|^2}\psi_w = \phi_w - \psi_w = \sigma_o$$

by definition of ψ_w. Since $\sigma_o \in \mathcal{V}$ is the fragile part of the original feature vector, we conclude as in [21], III.B., p. 786, that the image reconstructed from $\tilde{\phi}$ has a high probability of being perceptually distorted. ■

VII. ACKNOWLEDGEMENT

We are grateful to Giulia Franceschini for kindly providing us with several biomedical images (use of such material from human subjects was approved by the Ethics Committee, Medical University of Graz, Austria).

REFERENCES

[1] I. J. Cox, J. Kilian, F. T. Leighton, T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Trans. Image Processing*, vol. 6, pp. 1673–1687, 1997.

[2] I. J. Cox, M. L. Miller, J. A. Bloom, "Digital Watermarking," *Academic Press*, London, 2002.

[3] J. Eggers and B. Girod, ”Informed Watermarking,” *Kluwer Academic Publishers*, Norwell, MA, USA, 2002.

[4] M. Barni and F. Bartolini, ”Watermarking Systems Engineering. Enabling Digital Assets Security and Other Applications,” *Signal Processing and Communications Series*, 2004.

[5] G. Boato, F. G. B. De Natale, C. Fontanari, ”An Improved Asymmetric Watermarking Scheme Suitable for Copy Protection,” *IEEE Trans. Signal Processing*, to appear in June 2006.

[6] T. Kalker, ”Considerations on watermarking security,” *IEEE Fourth Workshop on Multimedia Signal Processing*, pp. 201–206, 2001.

[7] M. Barni, F. Bartolini, T. Furon, ”A general framework for robust watermarking security,” *Signal Processing*, vol. 83, pp. 2069–2084, 2003.

[8] T. Furon and P. Duhamel, ”An Asymmetric Watermarking Method,” *IEEE Trans. Signal Processing*, vol. 51, pp. 981–995 , Apr. 2003.

[9] ”First Summary Report on Fundamentals,” ECRYPT IST-2002-507932 European Network of Excellence in Cryptology, March 2005. www.ecrypt.eu.org/documents.html

[10] T. Kalker and F. M. J. Willems, ”Capacity bounds and constructions for reversible data-hiding,” *14th International Conference on Digital Signal Processing*, vol. 1, 2002, pp. 71–76.

[11] J. Fridrich, M. Goljan, R. Du, ”Lossless data embedding–new paradigm in digital watermarking,” *EURASIP Journal on Applied Signal Processing archive*, Special issue on Emerging applications of multimedia data hiding, pp. 185–196, 2002.

[12] M. U. Celik, G. Sharma, A. M. Tekalp, E. Saber, ”Lossless generalized-LSB data embedding,” *IEEE Trans. Image Processing*, vol. 14, pp. 253–266, Feb. 2005.

[13] B. G. Mobasseri and R. J. Berger II, ”A foundation for watermarking in compressed domain,” *IEEE Signal Processing Letters*, vol. 12, pp. 399–402, May 2005.

[14] J. Domingo-Ferrer and F. Sebe, ”Invertible spread-spectrum watermarking for image authentication and multilevel access to precision-critical watermarked images,” *Proc. of the International Conference on Information Technology: Coding and Computing (ITCC’02)*, 2002, pp. 152–157.

[15] A. Shamir, ”How to Share a Secret,” *Communication of the ACM*, vol. 22, pp. 612–613, 1979.

[16] T. Tassa, ”Hierarchical Threshold Secret Sharing,” *Proc. of the Theory of Cryptography Conference*, 2004, LNSC 2951, Springer-Verlag, pp. 473–490.

[17] G. Boato, C. Fontanari, F. Melgani, ”Hierarchical deterministic image watermarking via polynomial interpolation,” *Proc. of ICIP 2005*, Genova, Italy, Sep. 2005.

[18] J. J. Eggers, J. K. Su, B. Girod, ”Public key watermarking by eigenvectors of linear transforms,” *European Signal Processing Conference*, 2000.

[19] J. J. Eggers, J. K. Su, B. Girod, ”Asymmetric Watermarking Schemes”, *Proc. of Sicherheit in Mediendaten*, 2000.

[20] H. Choi, K. Lee, T. Kim, ”Transformed-Key Asymmetric Watermarking System,” *IEEE Signal Processing Letters*, vol. 11, Feb. 2004.

[21] J. Tzeng, W.-L. Hwang, I-L. Chern, ”An asymmetric subspace watermarking method for copyright protection,” *IEEE Trans. Signal Processing*, vol. 53, pp. 784–792, Feb. 2005.

[22] R. A. DeVore and G. G. Lorentz, ”Constructive Approximation,” *Grundlehren der Mathematischen Wissenschaften*, vol. 303, Springer-Verlag, Berlin, 1993.

LIST OF FIGURES

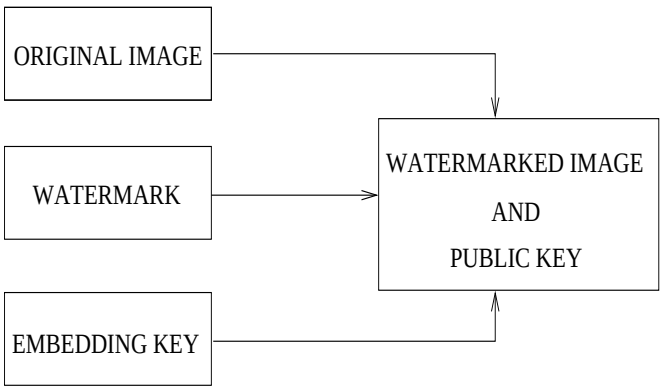

ORIGINAL IMAGE
WATERMARK
EMBEDDING KEY
WATERMARKED IMAGE
AND
PUBLIC KEY

Fig. 1.

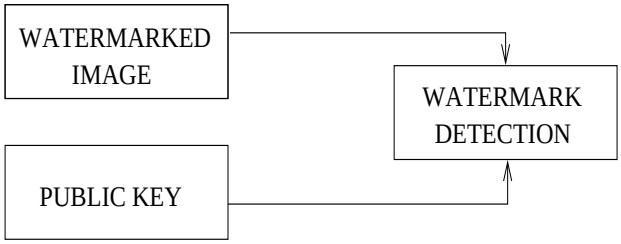


Fig. 2.

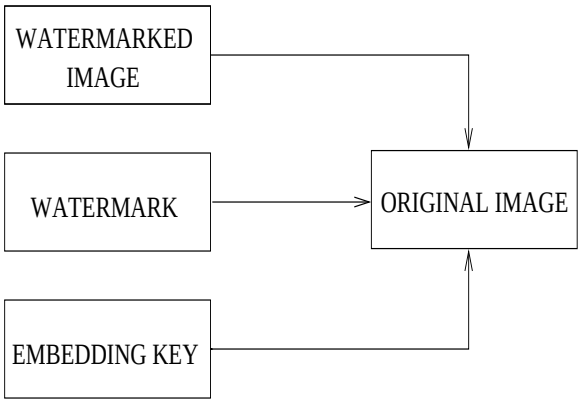

WATERMARKED IMAGE
WATERMARK
ORIGINAL IMAGE
EMBEDDING KEY

Fig. 3.

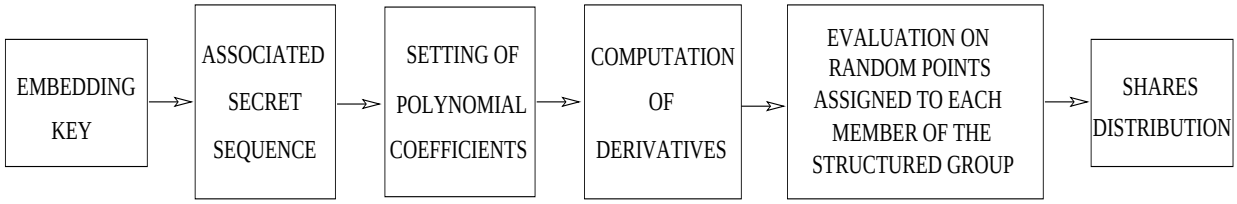
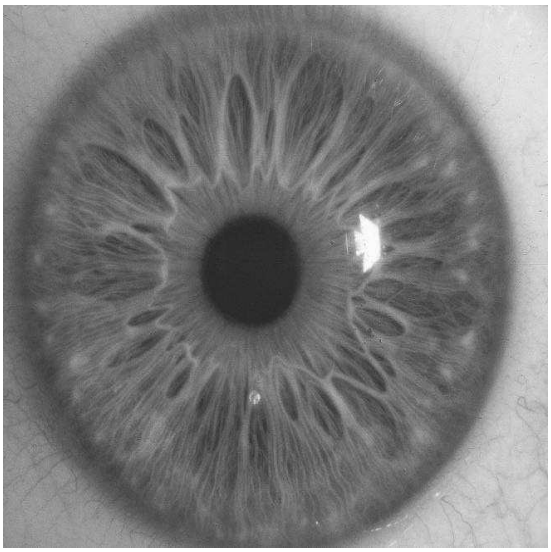
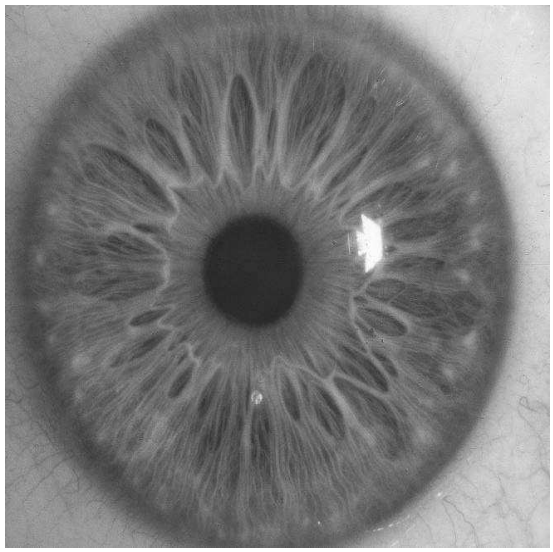

EMBEDDING KEY
ASSOCIATED SECRET SEQUENCE
SETTING OF POLYNOMIAL COEFFICIENTS
COMPUTATION OF DERIVATIVES
EVALUATION ON RANDOM POINTS ASSIGNED TO EACH MEMBER OF THE STRUCTURED GROUP
SHARES DISTRIBUTION

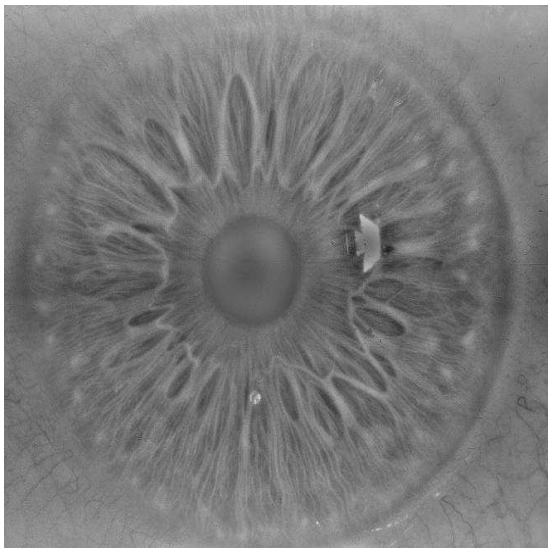
Fig. 4.



(a)



(b)



(c)

Fig. 5.

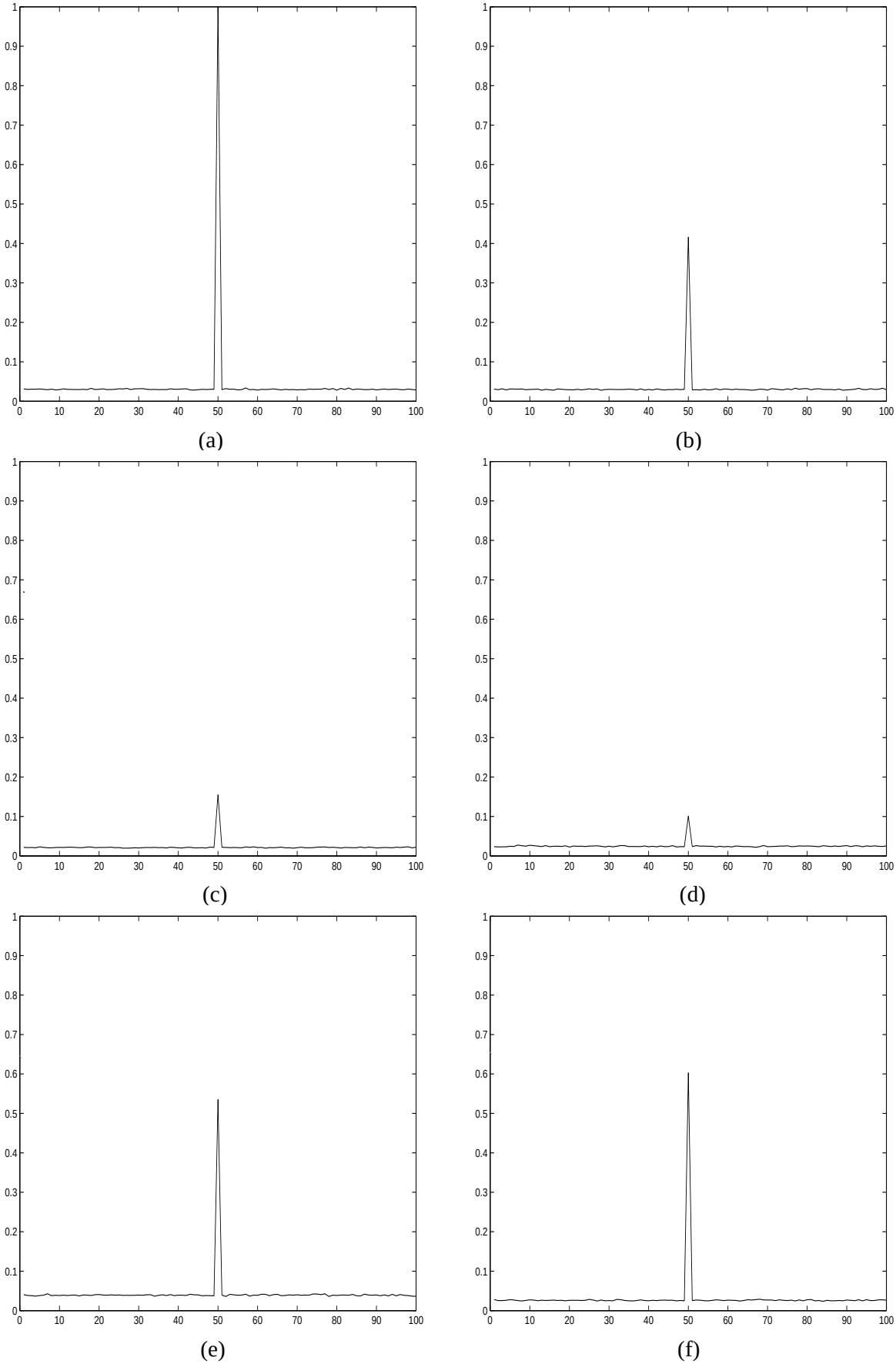


Fig. 6.

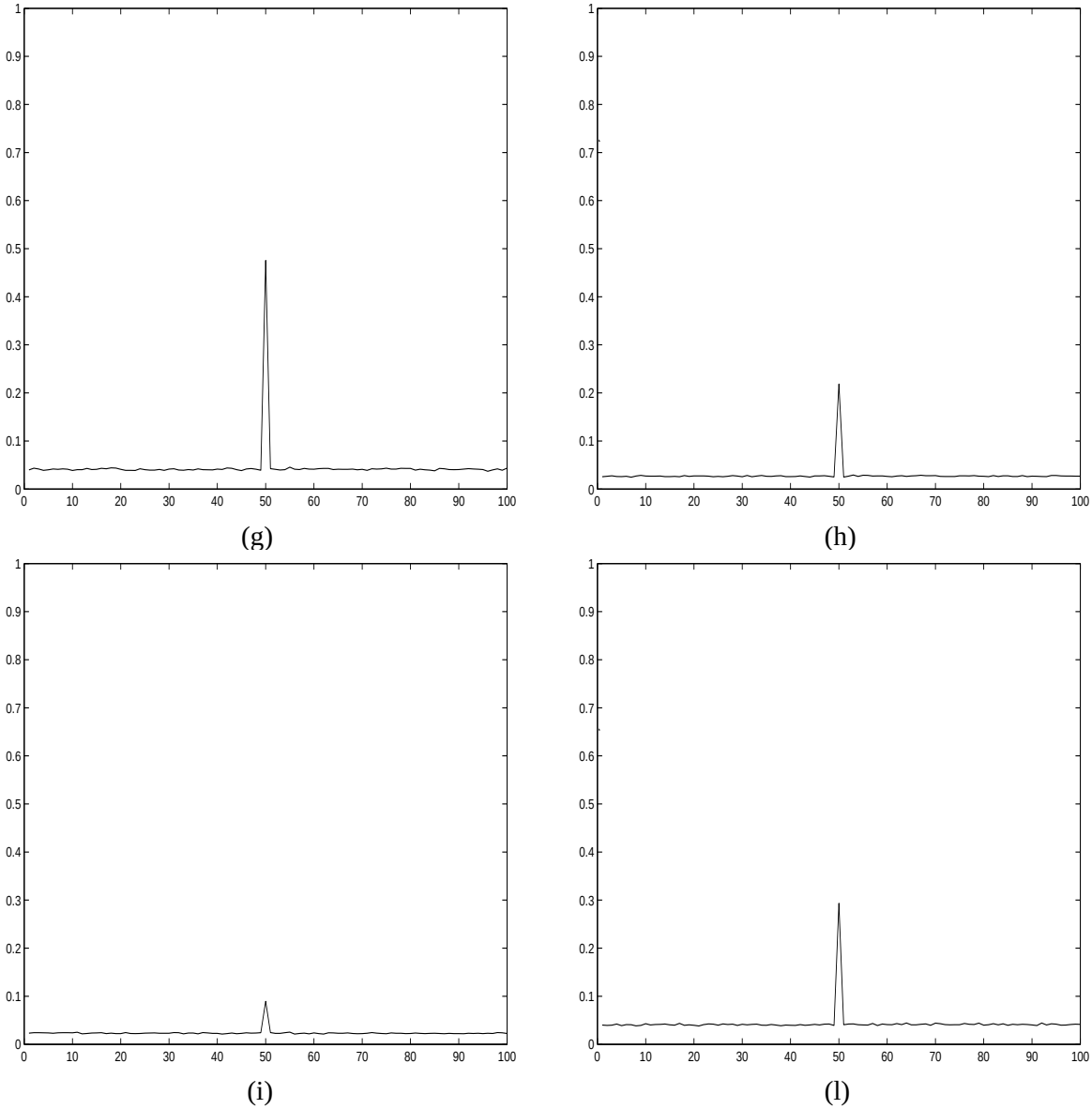


Fig. 7.

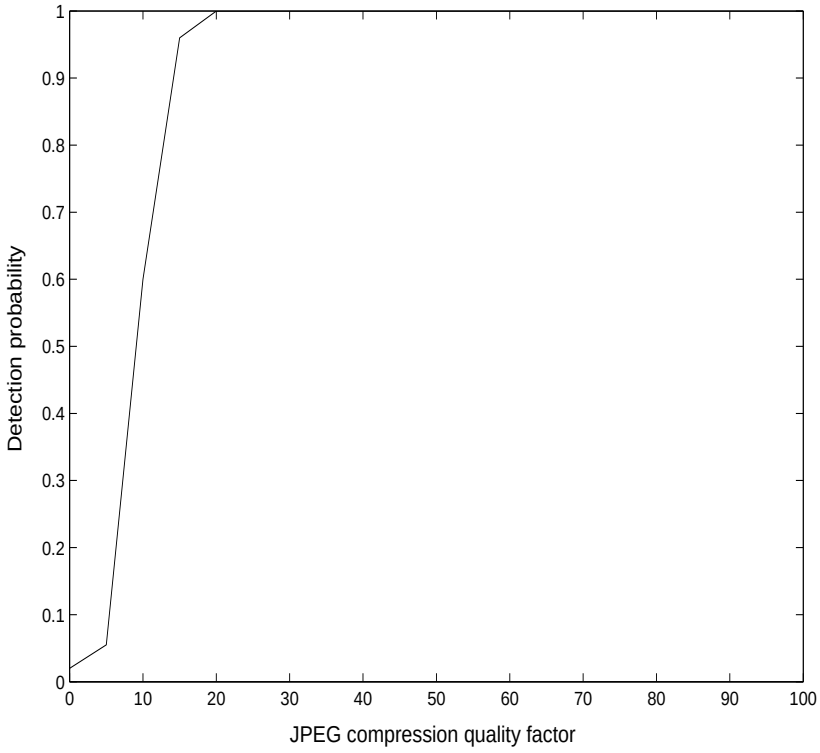

Detection probability
JPEG compression quality factor
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
10
20
30
40
50
60
70
80
90
100

Fig. 8.

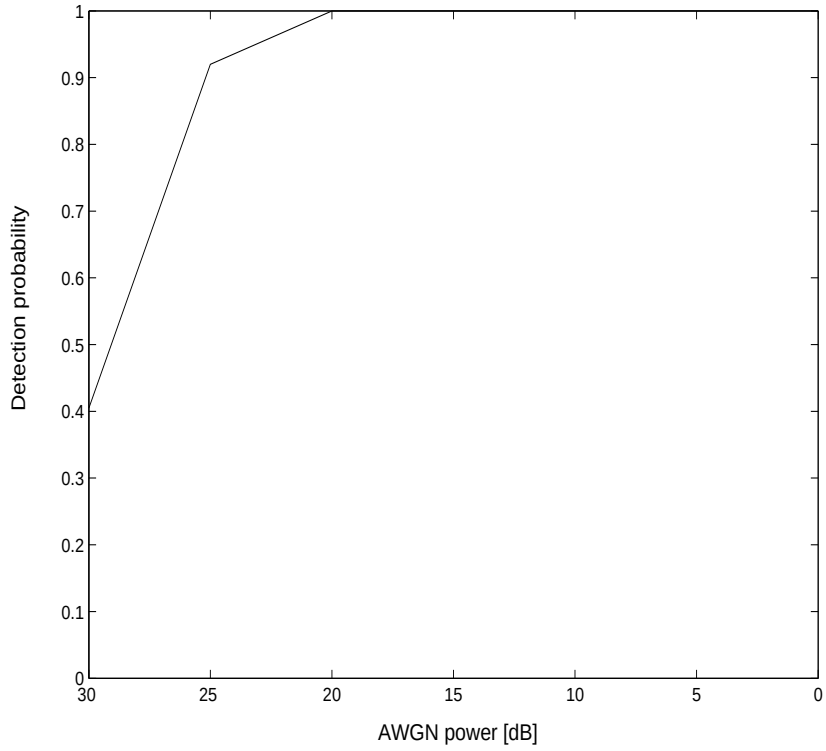

Detection probability
AWGN power [dB]
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
30
25
20
15
10
5
0

Fig. 9.

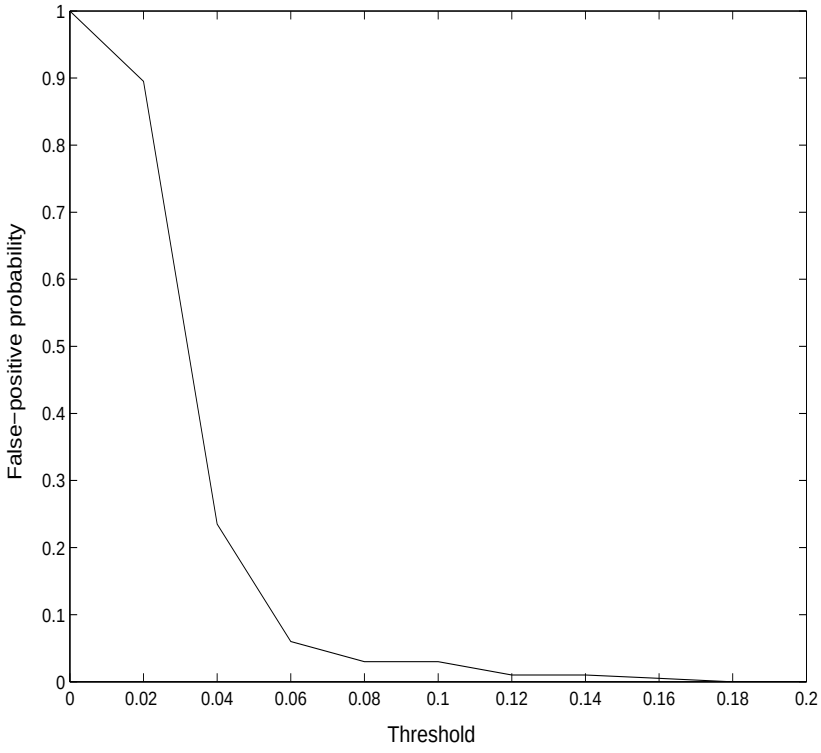
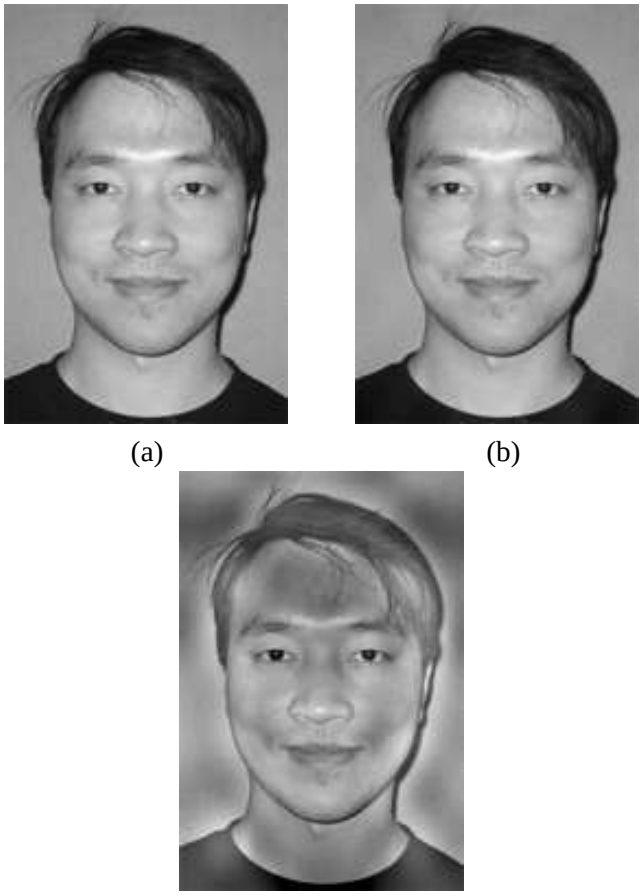

False−positive probability
Threshold
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
0.02
0.04
0.06
0.08
0.1
0.12
0.14
0.16
0.18
0.2

Fig. 10.



(a) (b)

(c)

Fig. 11.

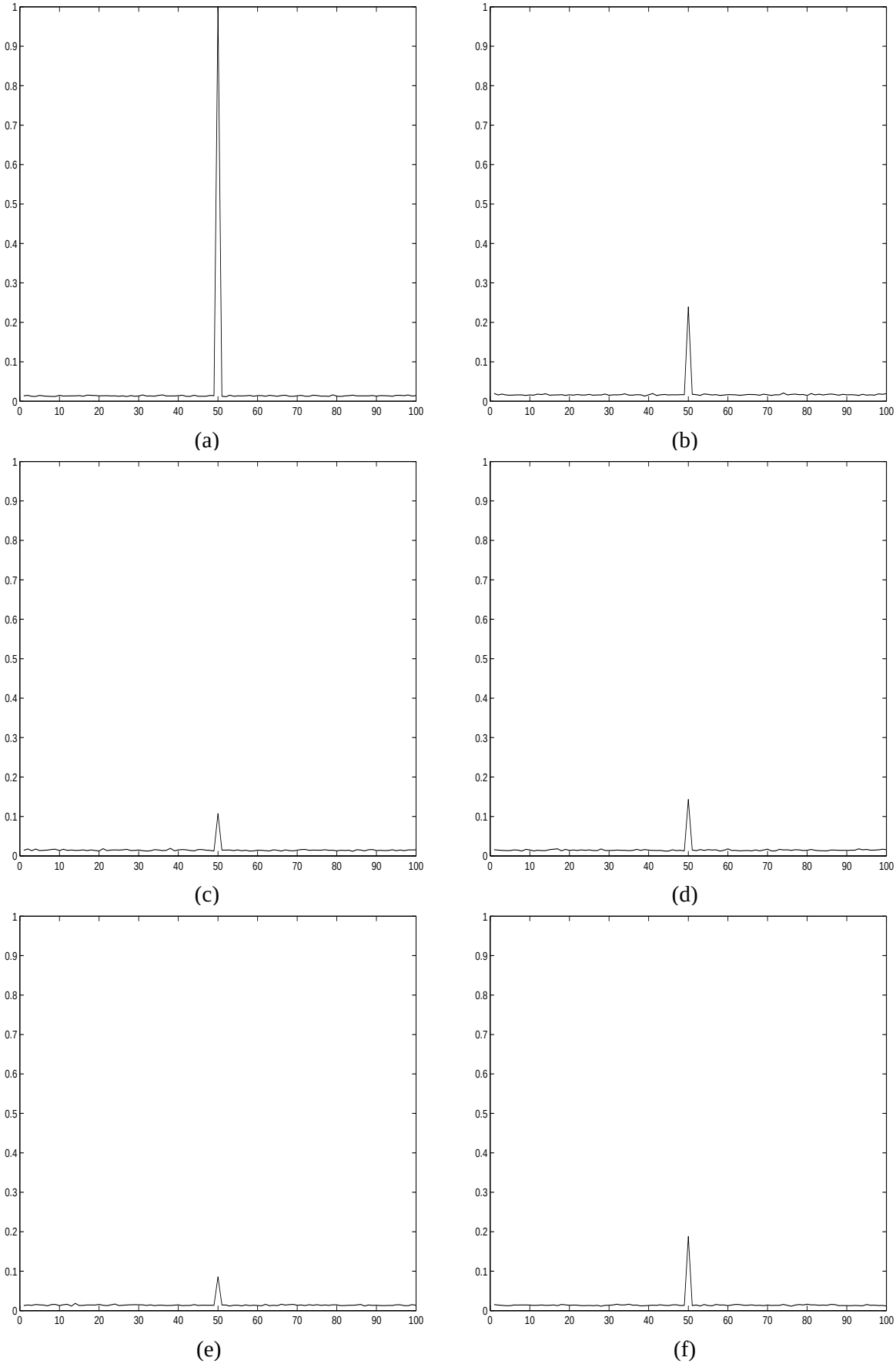


Fig. 12.

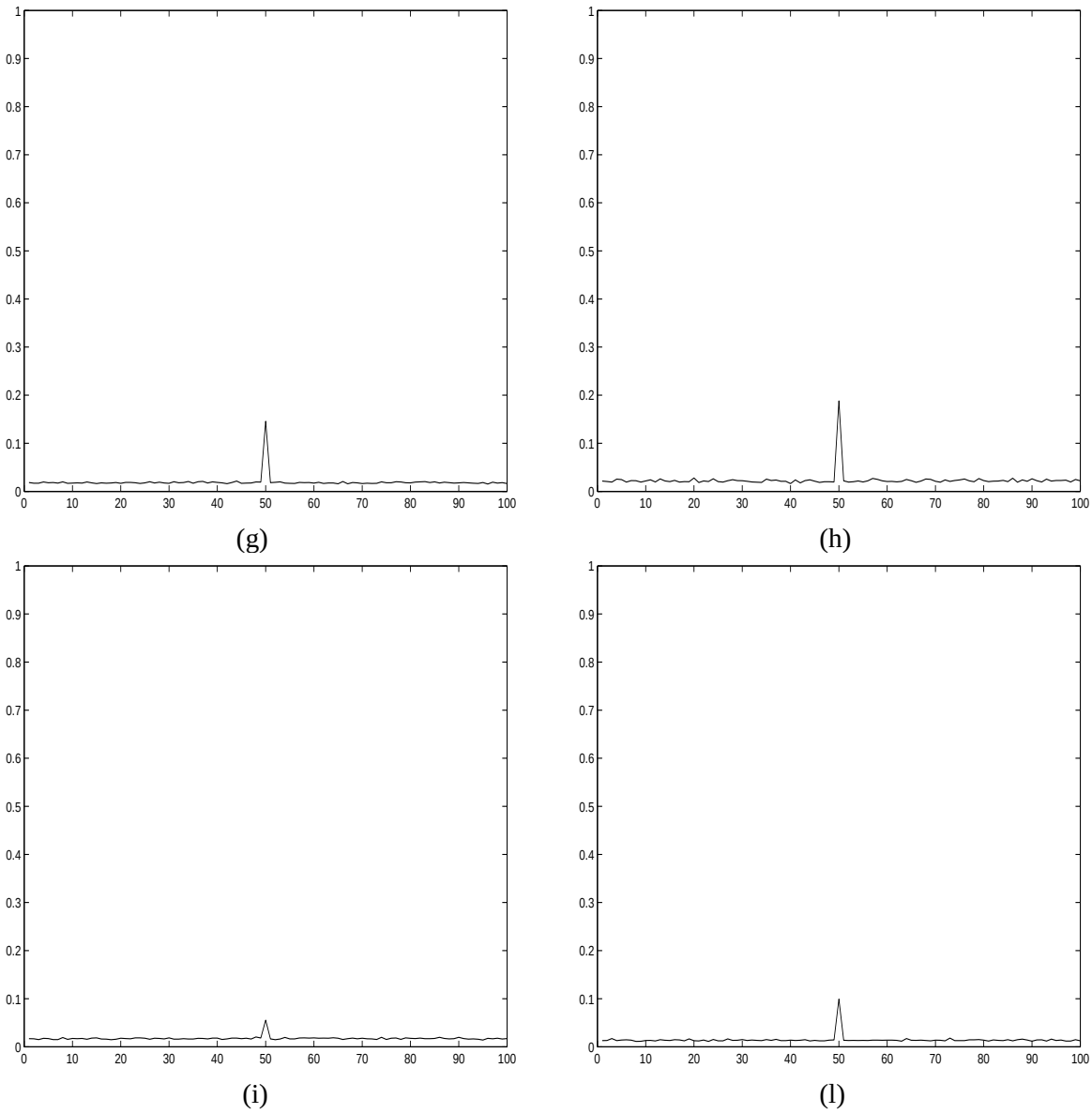


Fig. 13.

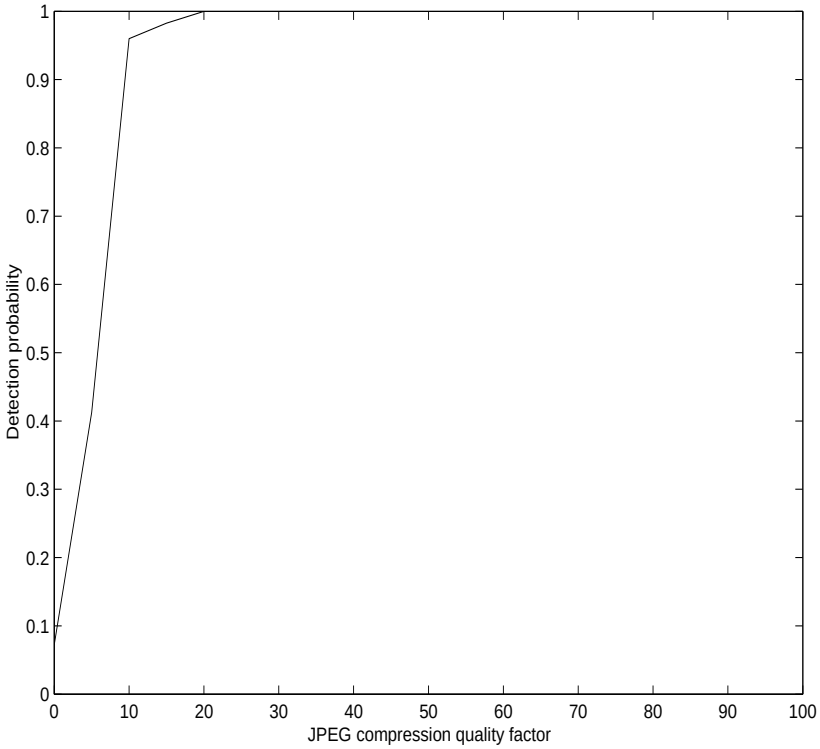

Detection probability
JPEG compression quality factor
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
10
20
30
40
50
60
70
80
90
100

Fig. 14.

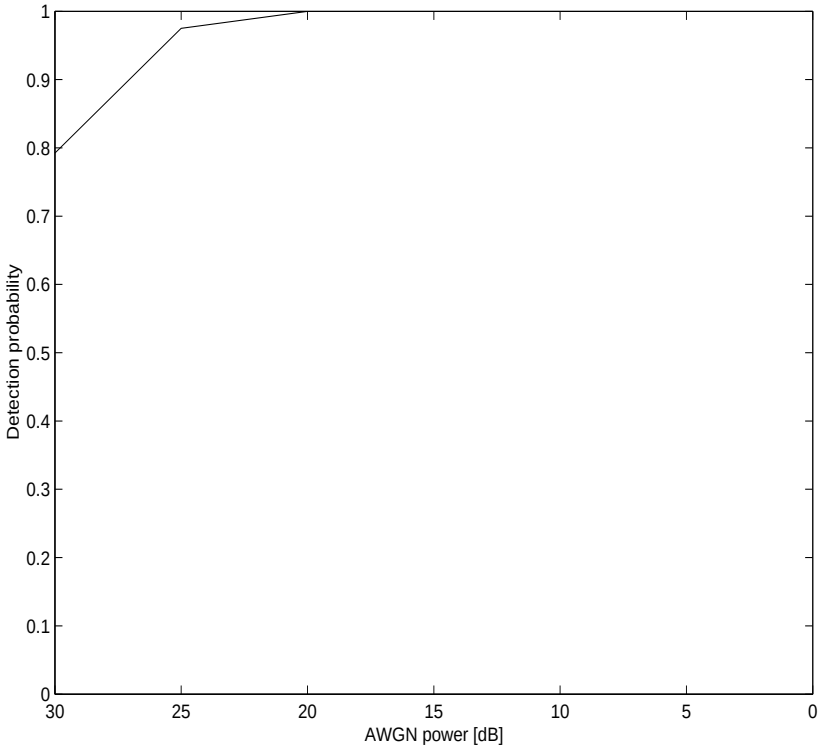

Detection probability
AWGN power [dB]
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
30
25
20
15
10
5
0

Fig. 15.

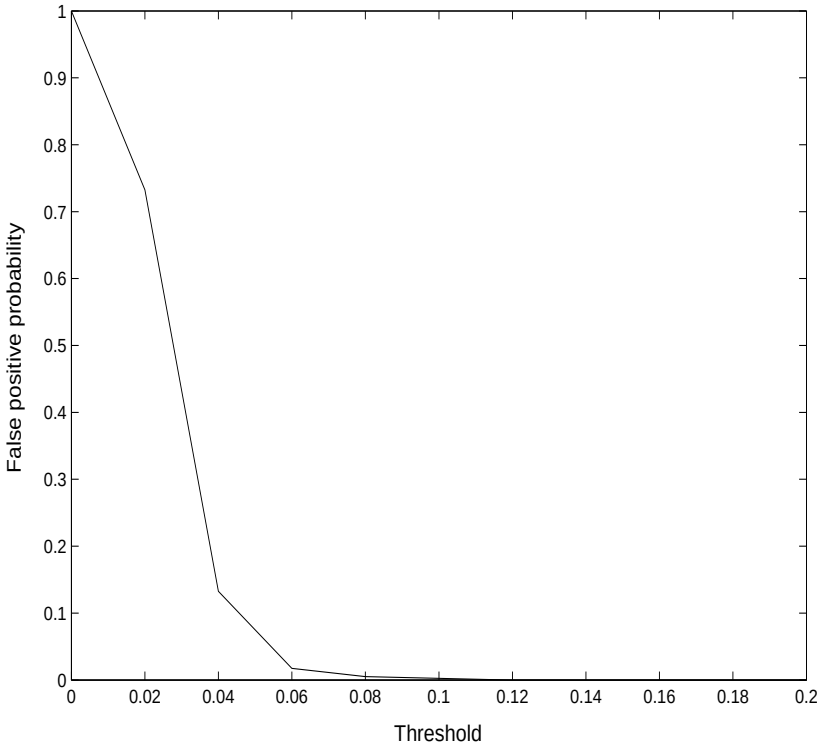

False positive probability
Threshold
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
0.02
0.04
0.06
0.08
0.1
0.12
0.14
0.16
0.18
0.2

Fig. 16.