UNIVERSITY
OF TRENTO

DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

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

HIERARCHICAL OWNERSHIP AND DETERMINISTIC WATERMARKING OF DIGITAL IMAGES VIA POLYNOMIAL INTERPOLATION

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

June 2006

Technical Report DIT-06-038

Hierarchical ownership and deterministic watermarking of digital images via polynomial interpolation

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

[1]Dept. of Information and Communication Technology, University of Trento,
Via Sommarive 14, I-38050, Trento, Italy.
[2]Dept. of Mathematics, Fac. of Information Engineering, Politecnico di Torino,
Corso Duca degli Abruzzi 24, I-10129, Torino, Italy.
{boato,melgani}@dit.unitn.it; denatale@ing.unitn.it; claudio.fontanari@polito.it

Keywords: image watermarking, joint ownership, polynomial interpolation.

Abstract

This paper presents a novel method for the secure management of digital images formulated within the mathematical theory of polynomial interpolation. As main innovative features, our approach is based on a hierarchical joint ownership of the image by a trusted layered authority and on a deterministic watermarking procedure, embedding a short meaningful or random signature into the image. Experimental results show that the inserted signature can almost always be fully recovered even in presence of a reasonable amount of image degradation due to image processing operators, such as filtering, geometric distortions and compression.

1. Introduction

In the last decade, digital watermarking techniques have raised a great deal of interest in the scientific community since the pioneering contribution by Cox et al. [1]. Indeed, the practice of imperceptible alteration of a document to embed a message into it plays a key role in the challenging field of ownership right protection. Much progress has been done in the last few years (see for instance [2]), but no general solution has been reached so far. This can be explained by several different factors, among which the heterogeneity of the requirements imposed by each application context and the clear definition and the operational mechanisms of the authority that would deal with the ownership verification process. In other words, currently proposed watermarking techniques strongly depend on the application scenario.

Let us consider the specific case, where a public or private organization needs to keep control on internal resources distributed to a number of users. In such a context, the organization can be regarded as an authority which has free access to the original data and assigns watermarked copies to users, who ignore the presence of the watermark. In this particular application scenario, two different problems need to be addressed: i) the management of the original data by the authority (which is trustworthy as a whole but includes possibly untrusted members); and ii) the selection of a proper watermarking technique. A well-known example is provided by the distribution of uniquely identifiable copies of a confidential British cabinet document to each minister by Margaret Thatcher in 1981. Hence, when the document was printed in the newspapers, the source of the leak could be discovered ([3], p. 4). Another realistic example for this application scenario is the case of the management of a set of confidential images involved in a legal prosecution. The control of their access is shared by the judging court (the authority) which is a hierarchical structure (president, members of the jury, etc.).

The images should be made available to a group of persons (the users) involved directly or indirectly in the prosecution process such as lawyers, officers, etc. Since the users may be not trusted, the authority wants to be able to detect possible illegal leakages. To achieve this goal, the images given to the users are watermarked with a signature that uniquely identifies them. In case of violation, an authorized subgroup of the authority can identify the source of the leakage. Accordingly, the two main ingredients of this kind of copyright management scheme are: i) a joint ownership of the original data in a group with hierarchical structure; and ii) a watermarking procedure which can exploit the original data in the reconstruction phase (i.e., it is not necessarily blind) and whose existence is hidden to users (i.e., it is steganographic according to the terminology of [3]).

As far as the authority is concerned, we stress that we consider the possibility to cope with untrusted member and therefore we need to find a way to manage the original data in a distributed way, exploiting the hierarchical structure of the organization. The hierarchical ownership handling, has been recently addressed in the context of digital image watermarking by Guo and Georganas [4], whose work exploits a secret sharing procedure generalizing the basic scheme by Shamir [5]. A (k, n)-threshold sharing scheme allows to divide a secret into n shares and requires the knowledge of at least k out of n shares to reconstruct the original content. Each share does not carry any meaningful partial plaintext of the secret and, if the number of shares available is less than k, a potential attacker can do no better than guessing, even with infinite computing time and power. Nevertheless, the solution in [4] has the annoying drawback that the procedure of shares distribution is expensive in terms of storage and complexity, since a huge number of shares is assigned to each participant. For a critical analysis of this algorithm, we refer to [6].

As an alternative, in this paper we propose a more sophisticated approach based on Birkhoff polynomial interpolation. Its main advantage is that the secret sharing is simplified by assigning just a single real number to each member of the group (no matter how complicated the corresponding access structure). An authorized subset of the authority can access the original data only if it includes a sufficient number of members for each level in the organization. Referring to the above example, this means that to access an image used in a legal prosecution one can need 1 actor of the highest level (e.g., the president) and 2 actors of the second level (e.g., two members of the jury). An interesting property of the proposed hierarchical scheme is its flexibility. Indeed, it can be applied to manage the access to different types of data (not only images) and combined with various kinds of watermarking methods depending on the application requirements and not only with that described in the following.

Concerning this last aspect, since the organization needs to keep control on copies distributed to a certain number of users, it is natural to apply a fingerprinting method by assigning to each user a unique watermark which identifies the legal recipient of the copy. Furthermore, because of the application considered, we require an exact reconstruction of the signature (watermark) assigned to each user and we assume that the users ignore the presence of the watermark (steganographic watermarking), hence no malicious attacks (e.g. collusion attack) need to be taken into account. Nevertheless, a user may need to perform some simple processing to use the data (e.g., to compress and store the data in a database or to resize it for page formatting and printing). Since the authority needs to trace the source of illegally redistributed copies, such non-malicious image processing operations should be considered in the testing of the watermarking process robustness. In order to fulfil the first requirement, instead of considering a random sequence as watermark and just a correlation measure for its detection as in [1], here a meaningful signature has to be embedded and the watermark detection should lead to a perfect recovery of the inserted signature. Such kind of watermarking schemes belongs to the category of readable watermarks according to the terminology of [7] (see for instance [8] and [9], just to quote a couple of recent contributions). In the specific context of image forensic, a version of the secret message has to be extracted from the stego message ([10]), but the problem of accepting digital image watermarking as a legal evidence of ownership is still widely open ([11], [12]). As a possible solution to this problem we propose the use of a deterministic signature to be perfectly reconstructed.

Specifically, the signature written in English alphabet is first translated into a sequence of integers by means of a look-up table. Such a sequence of integers is used to set the coefficients of a trigonometric polynomial, from which a predefined number of samples is extracted evaluated at equally spaced points. Finally, the values of the samples are embedded into the lowest frequency coefficients of the original image transformed into the DCT domain (excluding the DC component as in [1]). The watermark extraction process is based on solving a system of linear equations defined by the recovered samples. It is worth mentioning that, in [13] and [14], an analogous sinusoidal pattern has already been successfully exploited to embed a pseudo-random sequence. In these works, however, the detection of the watermark was just limited to a correlation measurement. In our watermarking scheme, characterized by a full reconstruction of the watermark, the choice of a trigonometric rather than an algebraic polynomial is motivated by the fact that standard polynomial interpolation is ill-conditioned, while the use of trigonometric functions allows to keep the condition number of the corresponding linear system close to the optimal value 1. In order to obtain a reliable deterministic polynomial reconstruction, we need to face the problem of image degradations due to the application of such standard image processing operators. Despite the preservation of the global quality of the image, the degradation may drastically corrupt some entries of the DCT image where the watermark is inserted. We overcome this issue by a suitable selection of the DCT samples conveying the watermark. In order to assess the effectiveness of the proposed watermarking approach, based on a hierarchical authority of ownership verification, we make use of a very large set of test images of different typologies. Experimental results show that our method exhibits a satisfactory effectiveness: the signature is reconstructed with 100% of accuracy for a wide range of image degradation operators. Furthermore, high performance is obtained in terms of false detection even in critical situations involving both users identified with very close signatures and strongly corrupted images.

The structure of the paper is as follows: in Section 2, we present a hierarchical secret sharing scheme for the joint ownership of the original image; in Section 3, we describe the generation, the embedding and the reconstruction phases of the watermarking scheme; in Section 4, we report experimental results; and in Section 5, we draw some concluding remarks.

2. Hierarchical joint ownership

2.1. Previous work

The main feature of a nonblind watermarking scheme is that the original image is needed in the reconstruction phase. As a consequence, an authority group A managing this process has to memorize the cover image, preferably storing it in a distributed (e.g., hierarchical) way for security reasons. As mentioned in the previous Section, in order to do that it is natural to apply a secret sharing procedure.

In this context, the basic secret sharing scheme proposed by Shamir [5] relies on standard Lagrange polynomial interpolation. Specifically, a secret $S \in \mathbb{R}$ is identified with some coefficient of a polynomial

$$p\left(x\right)=\sum_{i=0}^{k-1} a_i x^i \tag{1}$$

where for instance $a_0 = S$ and $a_1, \ldots, a_{k-1}$ are arbitrary real numbers. In order to distribute S among n participants, just fix n distinct real numbers $v_1, \ldots, v_n$ and assign to the j-th participant the share

$$p\left(v_j\right)=\sum_{i=0}^{k-1} a_i v_j^i \tag{2}$$

In order to reconstruct the secret, a subset of participants with associated real numbers $\{v_{i_1},\ldots,v_{i_s}\}$ with $1 \leq i_1 < i_2 < \ldots < i_s \leq n$, has to solve the following linear system:

$$V\begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \end{pmatrix}=\begin{pmatrix} p\left(v_{i_1}\right) \\ \vdots \\ p\left(v_{i_s}\right) \end{pmatrix} \tag{3}$$

where

$$V=\begin{pmatrix} 1 & v_{i_1} & \ldots & v_{i_1}^{k-1} \\ \vdots & & & \vdots \\ 1 & v_{i_s} & \ldots & v_{i_s}^{k-1} \end{pmatrix} \tag{4}$$

is a so-called *Vandermonde matrix* ([15], p. 155). It follows that the linear system (3) admits a unique solution if and only if $s \geq k$. In particular, at least k out of n shares are needed to reconstruct S, hence we obtain a (k,n)-secret sharing scheme.

As pointed out in [5], a hierarchical variant can be introduced by simply assigning a higher number of shares to higher level participants. In the context of digital image watermarking, a rather involved hierarchical secret sharing scheme was proposed by Guo and Georganas [4], as already pointed out in the Introduction. More recently, a refined hierarchical scheme was obtained by Tassa [16] from subtler properties of Birkhoff polynomial interpolation and improved further in [17] for application to wireless ad hoc networks. Here we are going to adapt from finite fields to real numbers this last approach, which seems to be more efficient (assigning just one share to each member) and realistic (attributing a qualitative rather than a quantitative difference between distinct levels). In the following we will detail the proposed hierarchical joint ownership approach.

2.2. Proposed methodology

Let A be the authority group composed of n participants and let us consider a collection Γ of subsets of A, which is monotone in the sense that if $V \in \Gamma$ then any set containing V also belongs to Γ. A threshold secret sharing scheme with access structure Γ is a method of sharing a secret among the members of A, in such a way that only subsets in Γ can recover the secret, while all other subsets have no information about it. Assume that A is divided into $t+1$ levels, i.e., $A = \cup_{l=0}^{t} A_l$ with $A_i \cap A_j = \emptyset$ 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 $(k_0, \ldots, k_t; n)$-hierarchical threshold secret sharing scheme distributes to each participant a share of a given secret S, in such a way that

$$\Gamma = \left\{ V \subset A : \# \left[V \cap \left(\cup_{l=0}^{i} A_l \right) \right] \geq k_i \quad \forall i = 0, \ldots, t \right\} \tag{5}$$

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 and/or level 1; at least k_2 members of level 0 and/or 1 and/or 2; and so on.

In order to construct a suitable $(k_0, \ldots, k_t; n)$-hierarchical threshold secret sharing scheme for the joint ownership of the original image, it is natural to apply Birkhoff interpolation [18] instead of Lagrange interpolation [19]. In fact, the Birkhoff scheme involves not only the polynomial, but also its (higher order) derivatives. More precisely, let $E = (E_{i,j})$, $i = 1, \ldots, m$; $j = 0, \ldots, k-1$, be an $m \times k$ *interpolation matrix*, with k entries equal to one and all remaining ones equal to zero. Let $X = x_1, \ldots, x_m$, $x_1 < x_2 < \ldots < x_m$, be a set of m distinct *interpolation points*. For every i, j with $E_{i,j} = 1$ we consider the k interpolation equations

$$p^{(j)}(x_i) = B_{i,j} \tag{6}$$

where $p^{(j)}$ denotes the j-th derivative of a polynomial p of degree $\leq k-1$ as in

(1) and $B_{i,j}$ are given data. Here the unknowns are the k coefficients $a_0, \ldots, a_{k-1}$ of p. It is clear that such a Birkhoff interpolation problem can admit infinitely many solutions even if the number of equations equals the number of unknowns, i.e. $m = k$: for instance, assume that $E_{i,0} = 0$ for every $i = 1, \ldots, n$. In this case, the interpolation system involves only derivatives of the polynomial p, hence it keeps no track of the constant term a_0, which will never be reconstructed. More generally, elementary linear algebra considerations show that if the interpolation matrix $E = (E_{i,j})$, $i = 1, \ldots, m$; $j = 0, \ldots, k-1$ does not satisfy the following *Pólya condition* ([18], p. 126)

$$\# \{E_{i,j} = 1 : j \leq h\} \geq h + 1, \quad 0 \leq h \leq k - 1 \tag{7}$$

then the corresponding Birkhoff interpolation problem admits infinitely many solutions.

The idea now is to exploit this necessary condition in order to ensure that only authorized subsets can reconstruct the secret. Intuitively speaking, an evaluation of the polynomial itself carries more informations 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:

1. Associate to the original image a secret key S identified with a sequence $(S_0, \ldots,\ S_z)$ with $S_i \in \mathbb{R}$ for every $0 \leq i \leq z$.

2. Let $k = k_t$ and pick a polynomial

$$p\,(x) = \sum_{i=0}^{k-1} a_i x^i \tag{8}$$

where $a_i = \begin{cases} S_i & 0 \leq i \leq z \\ \text{random} & z + 1 \leq i \leq k - 1. \end{cases}$

3. Identify each participant of level l with a random element $v \in \mathbb{R}$ and associate to v the share $p^{(k_{l-1})}(v)$, where $p^{(k_{l-1})}(v)$ denotes as above the k_{l-1}-th derivative of p and by definition $k_{-1} = 0$. Fix now a subset of the authority group $V = \{v_1, \ldots,\ v_m\} \subset A$ with $m \geq k$. Up to reordering we may assume that $v_i \in V_{l(i)}$ with $l(i) \leq l(j)$ for every $i \leq j$ ($l(i)$ indicates the level in the hierarchy of the i-th member of V). Consider the $m \times k$ matrix M_V whose i-th row is given by

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

In order to reconstruct the secret key S, the members of V have to solve the following linear system[1]:

$$M_V \begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} p^{k_{l(1)-1}}(v_1) \\ \vdots \\ p^{k_{l(m)-1}}(v_m) \end{pmatrix} \tag{10}$$

in the unknowns $a_0, \ldots, a_{k-1}$.

The key point is that (10) is a Birkhoff interpolation problem with associated interpolation matrix $E_V = (E_{i,j})$, $i = 1, \ldots, m$; $j = 0, \ldots, k-1$ 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 prove two theorems that provide the theoretical framework for the secret reconstruction. Both theorems are based on the following auxiliary result:

[1] We observe that one can improve the numerical stability of the linear system (10) with a careful choice of the random points $v_1, \ldots, v_m$. Indeed, it is well known that interpolation problems are usually ill conditioned and Chebyshev points represent the optimal choice as interpolation nodes ([19], § 5). In order to obtain random points, just consider a small random perturbation of Chebyshev points.

Lemma 1. *$V \in \Gamma$ if and only if E_V satisfies the Pólya condition.*

Proof. If $V \in \Gamma$, then by (5) it contains at least k_0 members of level 0, at least k_1 members in the union of level 0 and 1, and so on. From the third point of the above algorithm, participants of level 0 receive an evaluation of the polynomial as a share, participants of level 1 receive an evaluation of the k_0-th derivative of the polynomial as a share, and so on. Therefore, if we let C_j for $j = 0, \dots, k-1$ denote the j-th column of the interpolation matrix E_V, then C_j is a null column for $j \notin \{0, k_0, k_1, \dots, k_t\}$, and C_0 contains at least k_0 ones, $C_0 \cup C_{k_0}$ contains at lest k_1 ones, and so on. It follows that for every integer h with $k_{l-1} \leq h < k_l$ the union $\bigcup_{0 \leq j \leq k_{l-1}} C_j$ contains at least $k_l \geq h+1$ ones, hence (7) is satisfied. Conversely, if $V \notin \Gamma$, then E_V does not satisfy (7) for at least one value of h and therefore Pólya condition does not hold. □

Theorem 1. *If $V \notin \Gamma$ then V cannot reconstruct the secret S.*

Proof. Since $V \notin \Gamma$, by Lemma 1 E_V doesn't satisfies Pólya condition and it follows that the corresponding Birkhoff interpolation problem admits infinitely many solutions. Thus V cannot reconstruct the secret. □

More precisely, if $z = 0$ then for every $S_0 \in \mathbb{R}$ there is at least one solution $a_0, \dots, a_k$ of (10) with $a_0 = S_0$, hence all possibilities for the secret are equally likely, exactly as in the scheme proposed by Shamir.

Next, we can apply Theorem 10.1 in [18], p.128, whose statement can be rephrased as follows:

Proposition 1. *A Birkhoff interpolation problem admits a unique solution for almost all choices of interpolation points $x_1, \dots, x_m$, i. e. outside of a subset of $\mathbb{R}^m$ with m-dimensional measure equal to 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 S.*

Proof. Since $V \in \Gamma$, by Lemma 1 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 embedded secret. □

As a consequence, a set of participants can reconstruct the original image and verify the presence of the watermark if and only if it belongs to the predefined access structure.

3. The watermarking scheme

The aim of an authority A hierarchically organized into several levels is to distribute a given image I among a set of users $u^1, \ldots, u^n$, keeping some control on the use of the image by each of them. In particular, for any copy of I, that may undergo some image processing operations, any subset $V \subset A$ in the given access structure Γ should be able to identify without ambiguity the user from whom this copy comes from. As summarized in Figure 1, a secure management of I can be provided by the following procedure:

1. Fix $k \in \mathbb{N}$ not exceeding the number of pixels of I.

2. Apply the DCT to I and consider a $k \times k$ submatrix $J = (J_{i,j})$ corresponding to the lowest frequency DCT coefficients.

3. Put the entries of J, but $J_{0,0}$, into a vector $S = (a_0, \ldots, a_z)$, where $z = k^2 - 1$ (the DC component is not used in the watermarking procedure).

4. Distribute S among all members of the group according to the rules described in the Section 2, in such a way that only certain distinguished subgroups can recover S in order to use I in the watermarking reconstruction phase.

3.1. Watermark generation

In our watermarking scheme, the watermark consists in a sequence of letters assigned to each user. Such a signature can be either random or meaningful according to the authority requirements. Since we assume that the authority desires a full reconstruction of the watermark, we exploit again a polynomial framework as it will be described in the next subsections. According to a statistical analysis of the letters in the English dictionary [20], we construct a look-up table based on the principle that the more frequent a letter in the set of English words, the smaller the integer in the interval $[-13, 13]$ associated to it, so that the norm of the signature is kept as small as possible.

3.2. Watermark embedding

As illustrated in Figure 2, for all users u^q, $1 \leq q \leq n$, each one identified by a signature $s_1^q, \dots, s_l^q$ of length l an authorized subset $V \in \Gamma$ performs the following procedure:

1. Consider the trigonometric polynomial[2]

$$p^q(t) = \sum_{i=1}^{l} s_i^q \, \sin(i2\pi t) \tag{12}$$

2. Compute the sampling instants taken uniformly over the range $[0, 1]$

$$t_i = \frac{i}{k^2 - 1} \qquad i = 1, \dots, k^2 - 1 \tag{13}$$

[2] As already mentioned in the Introduction, standard polynomial interpolation is ill-conditioned, while trigonometric functions allow to solve linear systems with condition number closer to 1.

let $N = \max_{1 \le i \le k^2-1} |p^q(t_i)|$ and put the normalized evaluations of the trigonometric polynomial at the sampling instants into the $k \times k$ square matrix $W^q = (W^q_{i,j})$ defined as follows:

$$W^q_{i,j} = \begin{cases} 0 & \textit{if } i = j = 1 \\ p^q(t_{(i-1)k+j-1})/N & \textit{otherwise} \end{cases} \tag{14}$$

3. Watermark I by substituting every $J_{i,j}$ with $J_{i,j}(1 + \alpha W^q_{i,j})$, where $\alpha \in \mathbb{R}$ is a scaling factor, small enough to make the watermarked image I^q perceptually indistinguishable from I.

3.3. Watermark reconstruction

Let the image $I^{\overline{q}}$ be the watermarked copy of I given to the user $u^{\overline{q}}$, $1 \le \overline{q} \le n$, possibly decayed. In order to identify $u^{\overline{q}}$, an authorized subset $V \in \Gamma$ first reconstructs S by solving the linear system (10), puts it into a matrix and recovers J. Then, for each user u^q, $1 \le q \le n$, with signature $s^q_1, \ldots, s^q_l$, V performs the following procedure (see Figure 3):

1. Apply the DCT transform to $I^{\overline{q}}$ and consider its $k \times k$ submatrix $J^{\overline{q}} = (J^{\overline{q}}_{i,j})$ corresponding to the lowest frequency DCT coefficients.

2. Define $\Delta = (\Delta_{i,j})$ by setting

$$\Delta_{i,j} = J^{\overline{q}}_{i,j} - J_{i,j}(1 + \alpha W^q_{i,j})$$

where W^q is computed as in 3.1.2.

3. Define the set $K(t) = \{(a,b) \in \mathbb{N} \times \mathbb{N} \text{ such that } |\Delta_{a,b}| < t|J_{a,b}|\}$ corresponding to the least corrupted entries and fix the initial value $t = 1$.

4. If $\#K(t) < l$, conclude that the signature of u^q is not present in $I^{\overline{q}}$. Otherwise, compute N again as in 3.2.2 and solve the following linear system

$$\sum_{i=1}^{l} s^q_i \sin(i 2\pi t_{(a-1)k+b-1}) = \tag{15}$$

$$= \left(J^{\overline{q}}_{a,b}/J_{a,b} - 1\right)\frac{N}{\alpha} \quad \forall (a,b) \in K\left(t\right)$$

in the unknowns $s_1^q, \ldots, s_l^q$ and round the obtained solution to the closest string of integers.

5. If the signature of u^q is recovered with 100% of accuracy, then stop the procedure keeping track of the number $\#K\left(t\right)$. Otherwise, reduce the threshold t of a 2% factor and go to Step 4. Notice that only a finite number of repetitions of Step 4 is needed in order to conclude one way or another since $\#K\left(t\right)$ decreases with t.

6. Finally, $V \in \Gamma$ associates $I^{\overline{q}}$ to the user $u^{\overline{q}}$ for which the signature has been fully reconstructed. In case of conflicts, i.e., when it comes out that several different signatures are fully reconstructed from $I^{\overline{q}}$, V compares the different values of $\#K\left(t\right)$ of the corresponding users and associates $I^{\overline{q}}$ to the user $u^{\overline{q}}$ showing the highest $\#K\left(t\right)$.

4. Experimental results

In this experimental phase, we implemented our watermarking approach setting $k = 16$, $l = 8$, $\alpha = 0.1$ and tested it on a set of 70 images of different nature to deduce meaningful conclusions. In general, the watermark inserted in the image is imperceptible since on average PSNR$=$ 43 dB (see Figures 4 and 5). The attacks we considered to verify the method robustness are the following standard image degradation operations: additive white Gaussian noise with different power values; additive uniform noise with variance equal to 12; 3×3 moving average; Gaussian lowpass filtering of size 3×3 with standard deviation 0.5; rotation in a counter-clockwise direction of at most 1.5 degrees using the nearest neighbor interpolation method; resizing to various dimensions (down to one per cent of the original image area) using the nearest neighbor interpolation method; JPEG compression with quality factor down to 25%. For all these attacks, we tried to reconstruct the inserted signature with 100% of accuracy according to five different experimental scenarios.

The first scenario intends to test the possibility of applying the method independently of the image characteristics. This is done by inserting the same signature on the 70 available different images. The obtained results are summarized in Table 1 with the signature DITUNITN (Department of Information and Communication Technologies of the University of Trento). In this table, we report the detection rate (DR), the average and the minimal numbers of samples selected for watermark reconstruction (mean $\#K$ and min $\#K$, respectively). The obtained results demonstrate that the method is image independent. The embedded signature is recovered with 100% of accuracy for each image with a very high number of samples.

The second scenario aims at assessing the sensitivity of the method to the choice of the signature used to watermark the image. This is carried out by considering two images of different typologies like the Lena and Baboon images (see Figures 4 and 5, respectively) distributed among 70 users to whom random signatures were associated. For the two images, the quantitative results are reported in Table 2 and 3, respectively. The watermarked Lena and Baboon images respond very well to all attacks for every signature inserted. In addition, we report for each attack also the plots showing the number of samples found for each signature (see Figures 6 and 7). In all cases, a peak identifies the true signature corresponding to position 35 in the plots. Notice that rotation decreases the $\#K$ most among all degradation tested. Therefore, a specific variant of the method should be design to be very robust to this kind of attack, but, to the best of our knowledge, there are no proposals at present in the literature to achieve rotation-invariant watermarking in the DCT domain ([21]).

In the third scenario we evaluate the probability of false detection in a unwatermarked image in the presence of increasing noise. We look for the signature DITUNITN in a set of 100 unwatermarked Lena images corrupted by additive white Gaussian noise. The achieved results are reported in Table 4, which shows the average and the maximal number of samples selected. In all cases the number of samples selected is less than the length l and therefore it is impossible to solve the linear system (10) and reconstruct the signature. This demonstrates that the watermark detection process is capable of extracting meaningful signatures only if they have been indeed inserted into the image.

Due to the requirement of a 100% of accuracy in the decoding of the watermark in order to guarantee a legal evidence of ownership, it is important to test the capability of our method to avoid false detections from degraded watermarked images. To do so, in the fourth scenario we evaluate the false detection rate (FDR) in a watermarked image corrupted by the presence of noise with increasing power. The inserted signature (DITUNITN) is compared with a large number of randomly generated signatures in terms of the number of samples selected in the reconstruction phase. Actually, it may happen that also a random signature is perfectly reconstructed (see Table 5), but in our application this is not a problem at all. Indeed, since the authority needs to trace the source of illegally redistributed content, it will always control all signatures corresponding to all users, by performing a systematic test as in the second scenario. As already pointed out in Section 3.3 step 6, in case of conflicts (namely, if more than one signature is fully reconstructed) it is always possible to identify the really embedded signature by plotting the number of samples selected (see also Fig. 6 and 7). In this way the false detection rate of the system is zero, as shown in Table 5, although the number of fully reconstructed signatures besides the correct one is non zero. In fact, the number of samples selected for the reconstruction of the inserted signature (DITUNITN $\#K$) is highly greater than the maximum $\#K$ among all signature variations. The presented results demonstrate very well from an experimental viewpoint that the parameter $\#K$ is definitely significant to fix-up the false positive problem.

Finally, since in our scenario the authority should be free to select an arbitrary string, given an alphabet and a maximum string length, we are also interested in assessing the detection performance of the method when signatures are very close to each other. To this purpose, in the fifth experimental scenario we insert the signature DITUNITN into the Lena image corrupting it by noise of increasing power and we consider a set of four reference signatures differing from the correct one (i.e., DITUNITN) in just one or two letters. The results confirm clearly the capability of our method to deal suitably with such critical situations thanks to the comparison mechanism. Table 6 reports the number of samples selected for each of the five considered signatures.

5. Conclusions

In this paper, we have proposed a novel image watermarking technique which allows a trusted authority to recover the ownership from any reasonably distorted copy of an image distributed to several users. In order to do so, we embed into the image the signature of the corresponding user in a redundant way, exploiting a suitable trigonometric polynomial. The watermark detection is performed by the authority, which is considered as a hierarchical group managing the original image with a generalized secret sharing scheme based on Birkhoff polynomial interpolation. From the experimental results, it emerges that a perfect reconstruction of the signature can almost always be obtained for several kinds of image degradation operators independently of the image characteristics and signature used. Furthermore, the proposed method shows high performance in terms of false detection even in critical situations (strong image degradation and set of users identified with very close signatures). Finally, as mentioned previously, we stress that our hierarchical scheme is not constrained by the kind of watermarking technique adopted. Indeed, it can be combined with techniques different from that proposed in this paper in such a way to respond to other application requirements such as the robustness against malicious attacks. This aspect represents one of the envisaged future works.

References

[1] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon. *Secure Spread Spectrum Watermarking for Multimedia*. IEEE Transactions on Image Processing, Vol. 6, No. 12, 1997, 1673–1687.

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

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

[4] H. Guo and N. D. Georganas. *A Novel Approach to Digital Image Watermarking Based on a Generalized Secret Sharing Scheme*.Multimedia Systems, Vol. 9, No. 3, 2003, 249–260.

[5] A. Shamir. *How to Share a Secret*. Communication of the ACM 22 (1979), 612–613.

[6] Y. Wu. *Dynamic Ownership Verification*. 4th IEEE Pacific-Rim Conference on Multimedia, Track 2B2.7, CD-ROM, ISBN 0-7803-8186-6, Singapore, December 2003.

[7] M. Barni and F. Bartolini. *Watermarking Systems Engineering*. Signal Processing and Communications Series, 2004.

[8] A. H. Ouda and M. R. El-Jakka. *A Practical Version of Wong's Watermarking Technique*. Proc. of ICIP 2004, 2004, 2615–2618.

[9] M Fujiyoshi and H. Kiya. *An Image-Quality Guaranteed Method for Quantization-Based Watermarking using a DWT*. Proc. of ICIP 2004, 2004, 2629–2632.

[10] R. Chandramouli. *On Information Hiding with Incomplete Information about Steganalysis*. Proc. of ICIP 2004, 2004, 1161–1164.

[11] R. Akalu and D. Kundur. *Technological Protection Measures in the Courts*. IEEE Signal Processing Magazine, 2004, 109–117.

[12] M. Barni and F. Bartolini. *Data Hiding for Fighting Piracy*. IEEE Signal Processing Magazine, 2004, 28–39.

[13] H. Choi, H. Kim, and T. Kim. *Robust Sinusoidal Watermark for Images*. Electronics Letters, Vol. 35, No. 15, 1999, 1238–1239.

[14] Z. Liu and A. Inoue. *Audio Watermarking Techniques Using Sinusoidal Patterns Based on Pseudorandom Sequences*. IEEE Transactions on Circuits and Systems for Video Technology, Vol. 13, No. 8, 2003, 801–812.

[15] S. Lang. *Linear Algebra*. Third Edition, Springer, 1987.

[16] T. Tassa. *Hierarchical Threshold Secret Sharing*. Proc. of the Theory of Cryptography Conference 2004, MIT, Cambridge MA, USA, February 2004, LNSC 2951, Springer-Verlag, 2004, 473–490.

[17] E. Ballico, G. Boato, C. Fontanari, and F. Granelli. *Hierarchical Secret Sharing in Ad Hoc Networks through Birkhoff Interpolation*. Proc. if the IEEE International Conference on Telecommunications and Networking (TeNe 05), 2005.

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

[19] J.-P. Berrut and L. N. Trefethen. *Barycentric Lagrange Interpolation*. Siam Review, Vol. 46, No. 3, 2004, 501–517.

[20] http://www.askoxford.com/asktheexperts/faq/aboutwords/frequency

[21] P. Dong, G. Brankov, N. P. Galatsanos, Y. Yang, and F. Davoine. *Digital Watermarking Robust to Geometric Distortions*. IEEE Transactions on Image Processing, Vol. 14, No. 12, 2005, 2140–2150.

List of Figures

List of Tables

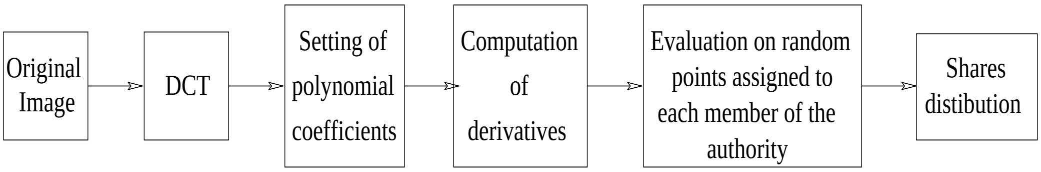

Original Image
DCT
Setting of polynomial coefficients
Computation of derivatives
Evaluation on random points assigned to each member of the authority
Shares distibution

Fig. 1.

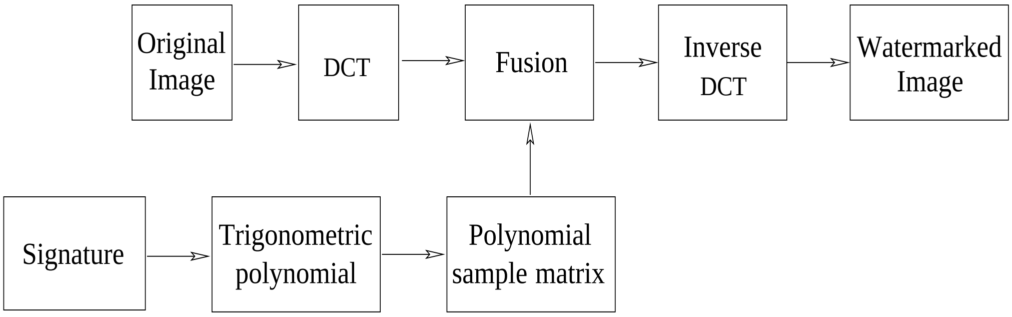

Original Image
DCT
Fusion
Inverse DCT
Watermarked Image
Signature
Trigonometric polynomial
Polynomial sample matrix

Fig. 2.

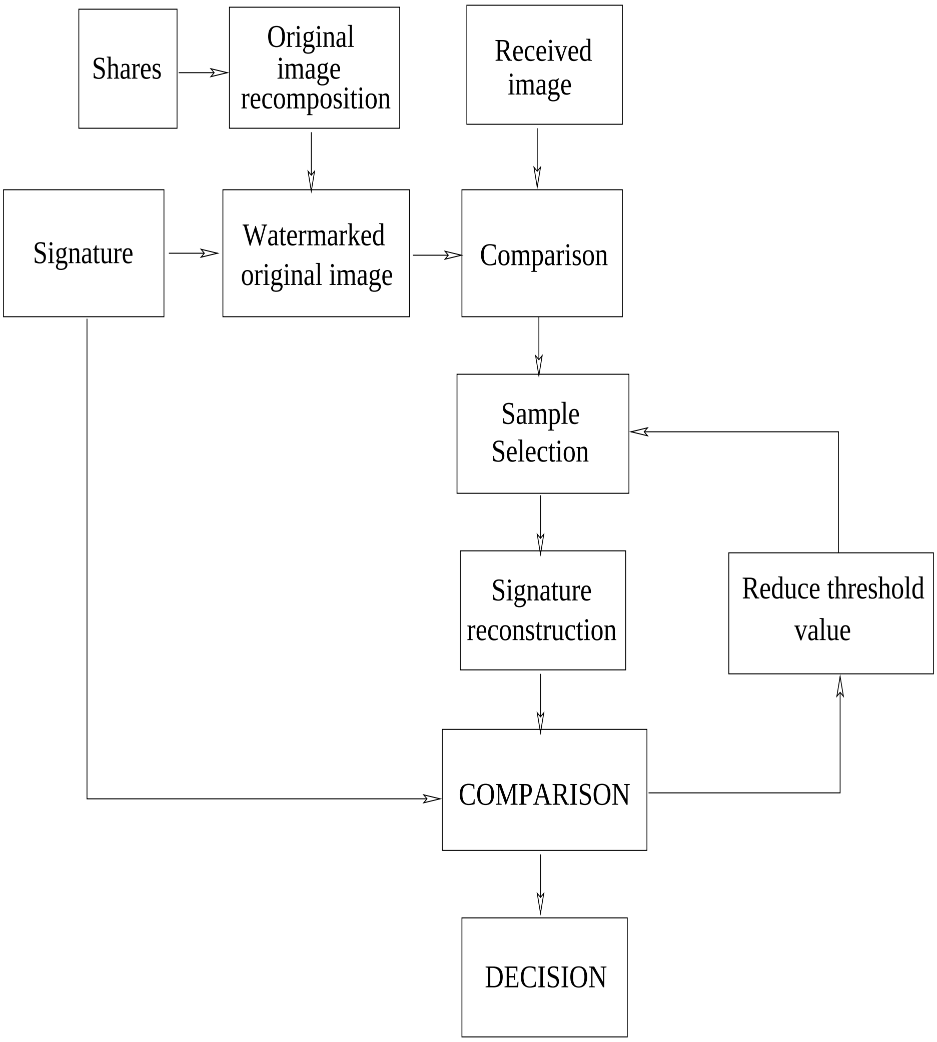
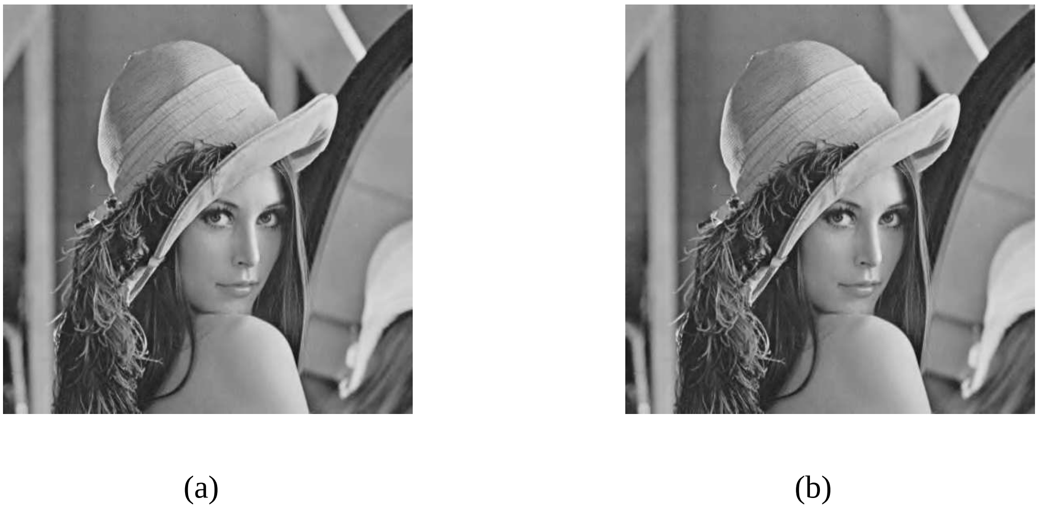

Shares
Original image recomposition
Received image
Signature
Watermarked original image
Comparison
Sample Selection
Signature reconstruction
Reduce threshold value
COMPARISON
DECISION

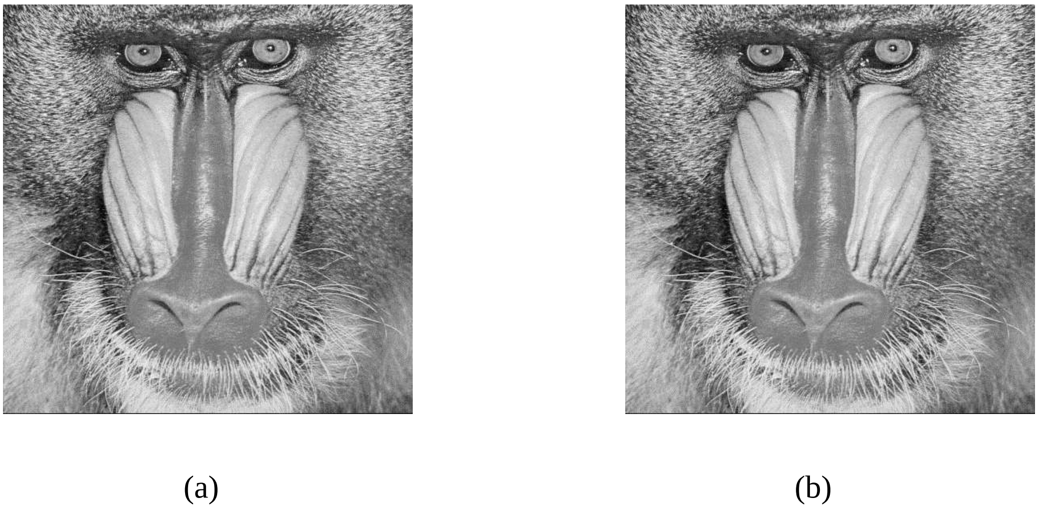
Fig. 3.



(a)

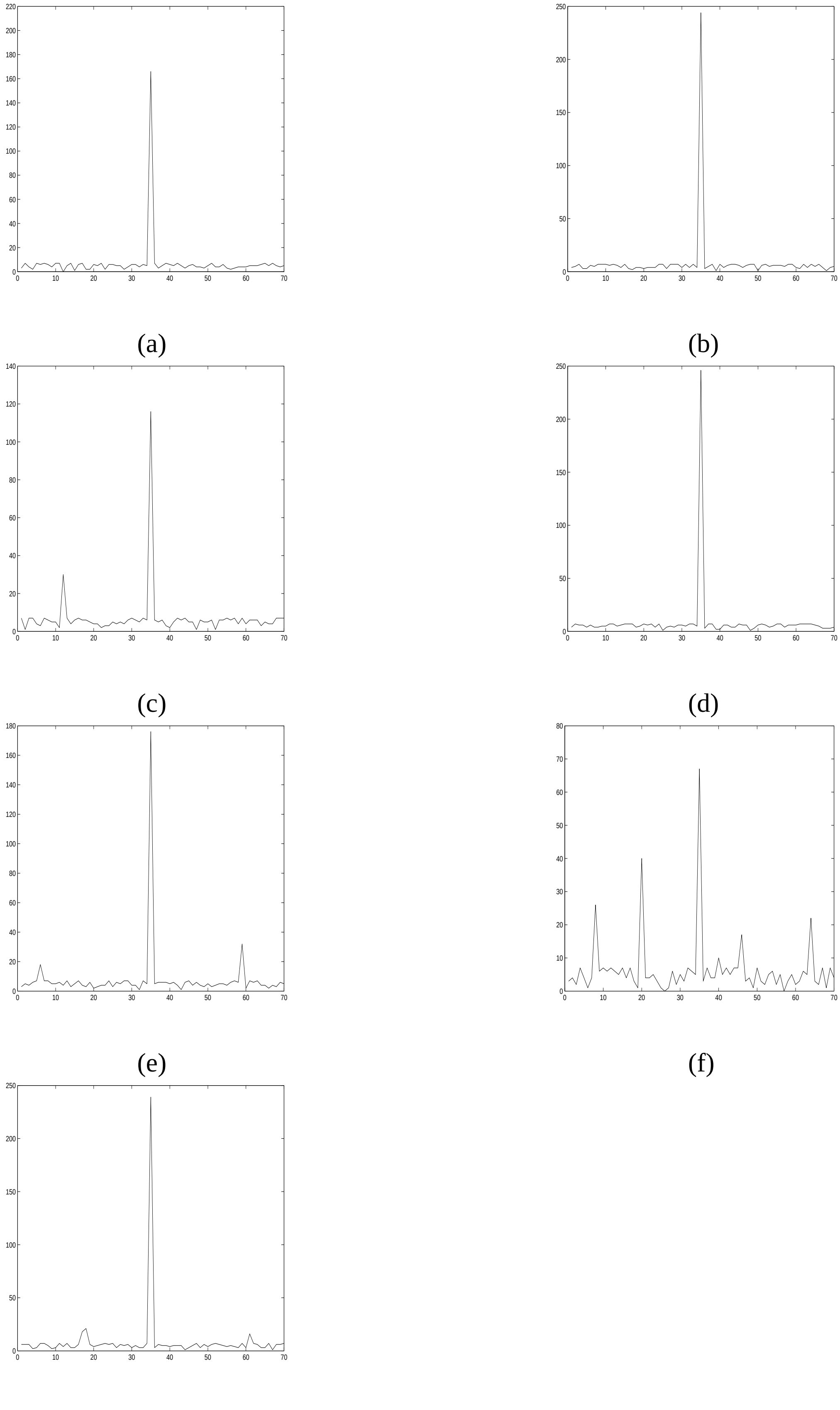
(b)

Fig. 4.



(a) (b)

Fig. 5.



(a)

(b)

(c)

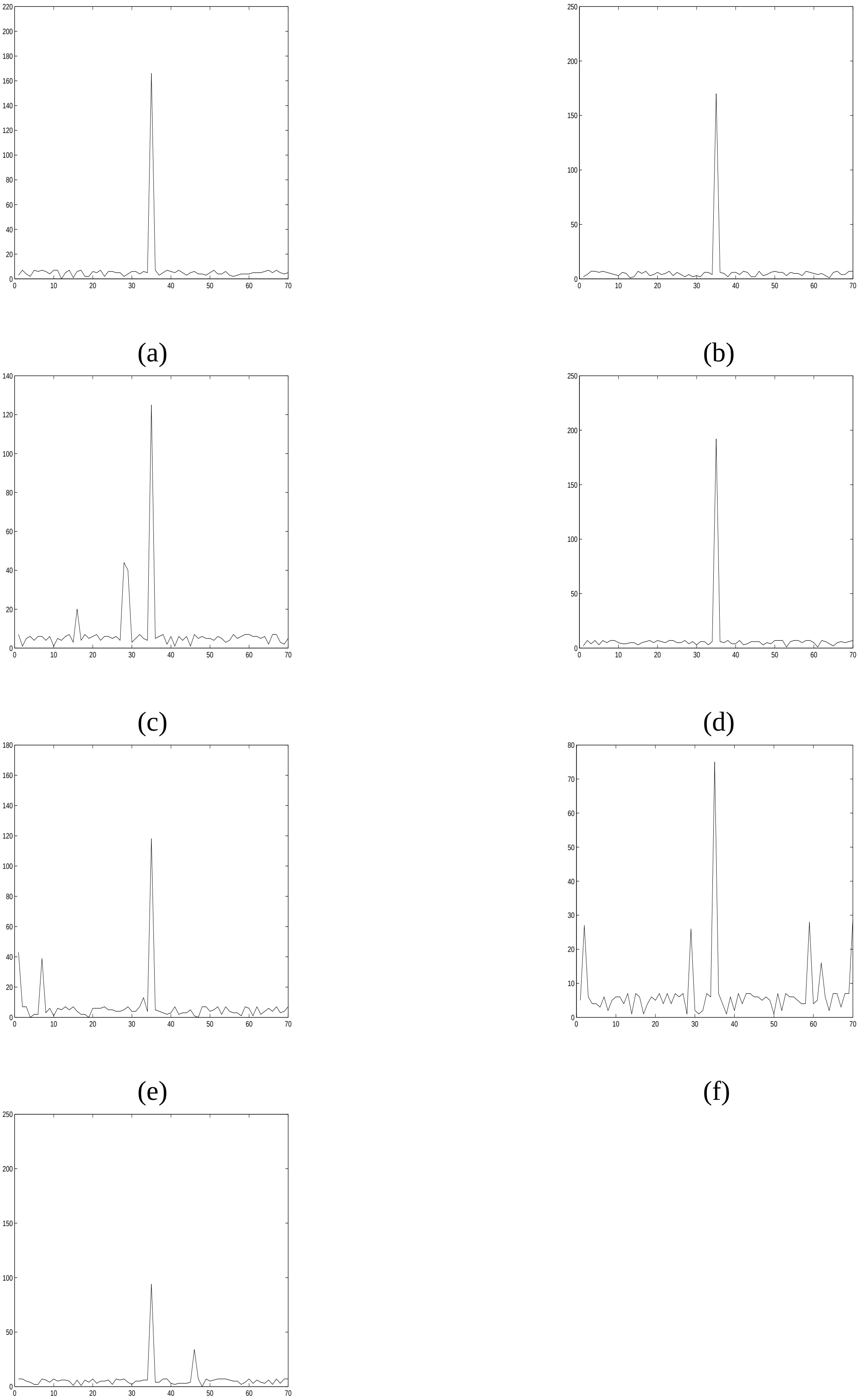
(d)

(e)

(f)

(g)

Fig. 6.



(a)

(b)

(c)

(d)

(e)

(f)

(g)

Fig. 7.

Table 1.

attack	DR [%]	mean $\#K$	min $\#K$
add. gauss. noise	100	205	96
add. unif. noise	100	194	84
moving average	100	103	51
gaussian lpf	100	206	124
resizing (0.1)	100	134	80
rotation (1.5)	100	67	46
JPEG (25%)	100	154	69

Table 2.

attack	DR [%]	mean $\#K$	min $\#K$
add. gauss. noise	100	201	46
add. unif. noise	100	201	181
moving average	99	126	61
gaussian lpf	100	200	192
resizing (0.1)	100	178	87
rotation (1.5)	99	54	8
JPEG (25%)	100	175	27

Table 3.

attack	DR [%]	mean $\#K$	min $\#K$
add. gauss. noise	100	170	41
add. unif. noise	100	163	32
moving average	100	120	16
gaussian lpf	100	193	191
resizing (0.1)	100	86	11
rotation (1.5)	99	55	11
JPEG (25%)	100	82	10

Table 4.

SNR (dB)	mean $\#K$	max $\#K$
32.5	2.47	4
31.5	2.44	4
30.5	2.36	4
29.5	2.36	4
28.5	2.39	5
27.5	2.43	5
26.5	2.41	4
25.5	2.44	5
24.5	2.66	5
23.5	2.64	5
22.5	2.59	5

Table 5.

SNR (dB)	DITUNITN $\#K$	mean $\#K$	max $\#K$	$\#$f.r.s.	FDR [%]
32.5	247	5.49	42	4	0
31.5	248	5.32	55	2	0
30.5	182	5.68	48	3	0
29.5	243	5.06	38	1	0
28.5	244	5.49	50	3	0
27.5	173	6.01	54	5	0
26.5	241	5.52	54	4	0
25.5	237	5.34	44	3	0
24.5	138	5.68	38	4	0
23.5	230	5.67	44	5	0
22.5	111	5.67	39	4	0

Table 6.

signature	$\#K$ w.o. noise	$\#K$ SNR 37.5 dB	$\#K$ SNR 32.5 dB	$\#K$ SNR 27.5 dB
DITUNITN	255	250	247	241
DITUNITV	3	6	4	7
DIEUNITN	5	6	6	54
DIMUNITN	5	32	43	28
DMAUNITN	5	5	4	35