



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

July 2005

Technical Report DIT-05-012

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

¹Dept. of Information and Communication Technology, University of Trento,
Via Sommarive 14, I-38050, Trento, Italy.

²Dept. 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. A realistic example of such an application scenario 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). More generally, 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]).

The first issue, i.e., 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). We also propose a novel deterministic approach to steganographic image watermarking, requiring exact reconstruction of the signature (watermark) assigned to each user. Instead of considering a long random sequence as watermark and just a correlation measure for its detection as in [1], here a short meaningful or random signature is embedded and the watermark detection consists in a perfect recovery of the inserted signature.

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 [7] and [8], 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. As customary in watermarking applications, we require our scheme to be robust against standard image processing operators, such as various filters, geometric distortions and compression. In order to obtain a reliable deterministic polynomial reconstruction, we need to face the problem of image degradations due to the application of such 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. The obtained 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.

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. In greater detail, his idea consists simply to identify a secret $S \in \mathbb{R}$ with some coefficients of a polynomial

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

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

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

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

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

where

$$V = \begin{pmatrix} 1 & v_{i_1} & \dots & v_{i_1}^{k-1} \\ \vdots & & & \vdots \\ 1 & v_{i_s} & \dots & v_{i_s}^{k-1} \end{pmatrix} \quad (4)$$

is a so-called *Vandermonde matrix* ([9], p. 155). It follows that the linear system (3) is determined, i.e., it 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 [10] from subtler properties of Birkhoff polynomial interpolation and improved further in [11] 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., $A = \cup_{i=0}^t A_i$ 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 $0 < k_0 < \dots < k_t$ is a strictly increasing sequence of integers, then a $(k_0, \dots, k_t; n)$ -hierarchical threshold secret sharing scheme distributes to each participant a share

of a given secret S , in such a way that

$$\Gamma = \{V \subset A : \# [V \cap (\cup_{i=0}^t A_i)] \geq k_i \quad \forall i = 0, \dots, t\} \quad (5)$$

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 $(k_0, \dots, k_t; n)$ -hierarchical threshold secret sharing scheme for the joint ownership of the original image, it is natural to apply Birkhoff interpolation [12] instead of Lagrange interpolation [13]. In fact, the Birkhoff scheme involves not only the polynomial, but also its (higher order) derivatives. More precisely, let $E = (E_{i,j})$, $i = 1, \dots, m$; $j = 0, \dots, k - 1$, be an $m \times k$ interpolation matrix, including k elements equal to one and all remaining elements set to zero. Let $X = x_1, \dots, x_m$, $x_1 < x_2 < \dots < x_m$, be a set of m distinct interpolation points. For polynomials of degree $\leq k - 1$ such as (1), for $E_{i,j} = 1$ we consider the k interpolation equations

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

where $p^{(j)}$ denotes the j -th derivative of p and $B_{i,j}$ are given data. Here the unknowns are the k coefficients a_0, \dots, a_{k-1} of $p(x)$. For this problem, it is straightforward to deduce that a Birkhoff interpolation problem can admit infinitely many solutions even if the number of equations equals the number of unknowns, i.e. $m = k$. Indeed, for instance, let us consider the case in which $E_{i,0} = 0$ for every $i = 1, \dots, n$. 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 the interpolation matrix $E = (E_{i,j})$, $i = 1, \dots, k$; $j = 0, \dots, k - 1$ does not satisfy the following *Pólya condition* ([12], p. 126)

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

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, \dots, S_z) with $S_i \in \mathbb{R}$ for every $0 \leq i \leq z$.
2. Let $k = k_t$ and pick a polynomial

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

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

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 $p^{(h)}$ denotes as above the h -th derivative of p and $k_{-1} \triangleq 0$. Fix now a subset of the authority group $V = \{v_1, \dots, v_m\} \subset A$ 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

$$\frac{d}{dx^{k_{l(i)-1}}} (1, x, x^2, \dots, x^{(k-1)}) (v_i) \quad (9)$$

In order to reconstruct the secret key S , the members of V have to solve the

following linear system¹:

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

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

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

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

In the following, we will provide two theorems that represent the theoretical framework for the secret reconstruction. 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 S .*

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

Moreover, we can apply Theorem 10.1 in [12], 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 zero, if and only if it satisfies the Pólya condition.*

¹We observe that one can improve the numerical stability of the linear system (10) with a careful choice of the random points v_1, \dots, v_m . Indeed, it is well known that interpolation problems are usually ill conditioned and Chebyshev points represent the optimal choice as interpolation nodes ([13], § 5). In order to obtain random points, just consider a small random perturbation of Chebyshev points.

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 $V \in \Gamma$, 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 $i \leq z \leq k - 1$. \square

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, \dots, 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 this copy comes from. As summarized in Figure 1, a secure management of I can be provided by the following procedure:

1. Fix $d \in \mathbb{N}$ 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 $S = (a_0, \dots, a_z)$, 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. In order to avoid numerical stability problems, that may appear in the watermark reconstruction phase if polynomials present big coefficients, we minimize the moduli of the numbers involved. According to a statistical analysis of the letters in the English dictionary [14], 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 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 , $1 \leq q \leq n$, with signature s_1^q, \dots, s_l^q , an authorized subset $V \in \Gamma$ performs the following procedure:

1. Consider the trigonometric polynomial²

$$p^q(t) = \sum_{i=1}^l s_i^q \sin(i\omega_0 t) \quad (12)$$

where $\omega_0 \in \mathbb{R}$ is a constant radian frequency.

²As 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.

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

$$T = \frac{2\pi}{\omega_0}$$

$$t_i = \frac{2\pi i}{\omega_0(k^2 - 1)} \quad i = 1, \dots, k^2 - 1 \quad (13)$$

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

$$W_{i,j}^q = \begin{cases} 0 & \text{if } i = j = 1 \\ p^q(t_{j-1})/N & \text{if } i = 1, j = 2, \dots, k \\ p^q(t_{(i-1)k+j-1})/N & \text{otherwise} \end{cases} \quad (14)$$

3. Watermark I by substituting every $J_{i,j}$ with $J_{i,j}(1 + \alpha W_{i,j}^q)$, 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 $I^{\bar{q}}$ be the watermarked copy of I given to the user $u^{\bar{q}}$, $1 \leq \bar{q} \leq n$, possibly decayed. In order to identify $u^{\bar{q}}$, 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 , $1 \leq q \leq n$, with signature s_1^q, \dots, s_l^q , V performs the following procedure (see Figure 3):

1. Apply the DCT transform to $I^{\bar{q}}$ and consider its $k \times k$ submatrix $J^{\bar{q}} = (J_{i,j}^{\bar{q}})$ corresponding to the lowest frequency DCT coefficients.
2. Define $\Delta = (\Delta_{i,j})$ by setting

$$\Delta_{i,j} = J_{i,j}^{\bar{q}} - J_{i,j}(1 + \alpha W_{i,j}^q)$$

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 let $t = 1$.
4. If $\#K(t) < l$, conclude that the signature of u^q is not present in $I^{\bar{q}}$. Otherwise, compute N again as in 3.1.2 and solve the following linear system

$$\begin{aligned} \sum_{i=1}^l s_i^q \sin(i\omega_0 t_{(a-1)k+b-1}) &= \\ &= \left(J_{a,b}^{\bar{q}} / J_{a,b} - 1 \right) \frac{N}{\alpha} \quad \forall (a, b) \in K(t) \end{aligned} \quad (15)$$

in the unknowns s_1^q, \dots, 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 $\#K(t)$. 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 $\#K(t)$ decreases with t .
6. Finally, $V \in \Gamma$ associates $I^{\bar{q}}$ to the user $u^{\bar{q}}$ 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 $I^{\bar{q}}$, V compares the different values of $\#K(t)$ of the corresponding users and associates $I^{\bar{q}}$ to the user $u^{\bar{q}}$ showing the highest $\#K(t)$.

4. Experimental results

In this experimental phase, we implemented our watermarking approach setting $\omega_0 = 2\pi$, $d = 16$, $\alpha = 0.1$ 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 power 10 dB; 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 degree 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 two different experimental scenarios.

The first scenario intends to test the possibility of applying the method independently of the image characteristics. This was done by inserting the same signature on the 70 available different images. The obtained results are summarized in Table 1 with the signature chosen as DITUNITN. In this table, we report the average probability of success (PS), 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 was 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 which 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 inserted signature corresponding to position 35 in the plots.

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 decayed 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. Future work will concern the possibility of designing a non steganographic version of our watermarking method. The possibility of designing a blind version will be also investigated.

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] Joachim Eggers and Bernd 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] H. Choi, H. Kim, and T. Kim. *Robust Sinusoidal Watermark for Images*. Electronics Letters, Vol. 35, No. 15, 1999, 1238–1239.
- [8] 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.
- [9] S. Lang. *Linear Algebra*. Third Edition, Springer, 1987.

- [10] T. Tassa. *Hierarchical Threshold Secret Sharing*. Proc. of the Theory of Cryptography Conference 2004, MIT, Cambridge MA, USA, February 2004, LNCS 2951, Springer-Verlag, 2004, 473–490.
- [11] E. Ballico, G. Boato, C. Fontanari, and F. Granelli. *Multi-path Secret Sharing in Ad Hoc Networks: a Hierarchical Approach via Birkhoff Interpolation*. Technical Report DIT-04-080, Dipartimento di Informatica e Telecomunicazioni, University of Trento, 2004 (<http://eprints.biblio.unitn.it/archive/00000682/>).
- [12] R. A. DeVore and G. G. Lorentz. *Constructive Approximation*. Grundlehren der Mathematischen Wissenschaften 303, Springer-Verlag, Berlin, 1993.
- [13] J.-P. Berrut and L. N. Trefethen. *Barycentric Lagrange Interpolation*. Siam Review, Vol. 46, No. 3, 2004, 501–517.
- [14] <http://www.askoxford.com/asktheexperts/faq/aboutwords/frequency>

List of Figures

Fig. 1. Block diagram illustrating the hierarchical distribution process of the original image.

Fig. 2. Block diagram showing the various steps occurring in the watermark embedding process.

Fig. 3. Block diagram of the watermark reconstruction process.

Fig. 4. Original (a) and watermarked (b) Lena image (PSNR= 43.09).

Fig. 5. Original (a) and watermarked (b) Baboon image (PSNR= 42.99).

Fig. 6. Number of samples found versus signature for Lena image after: (a) additive white Gaussian noise; (b) additive uniform noise; (c) 3×3 moving average; (d) Gaussian lowpass filtering; (e) scaling with a factor of 0.1; (f) rotation of 1.5 degrees; (g) JPEG compression with quality factor equal to 25%.

Fig. 7. Number of samples found versus signature for Baboon image after: (a) additive white Gaussian noise; (b) additive uniform noise; (c) 3×3 moving average; (d) Gaussian lowpass filtering; (e) scaling with a factor of 0.1; (f) rotation of 1.5 degrees; (g) JPEG compression with quality factor equal to 25%.

List of Tables

Table 1. Results obtained for the first experimental scenario (fixed meaningful signature embedded into 70 different images).

Table 2. Results obtained in the second experimental scenario for the Lena image by embedding 70 different random signatures.

Table 3. Results obtained in the second experimental scenario for the Baboon image by embedding 70 different random signatures.

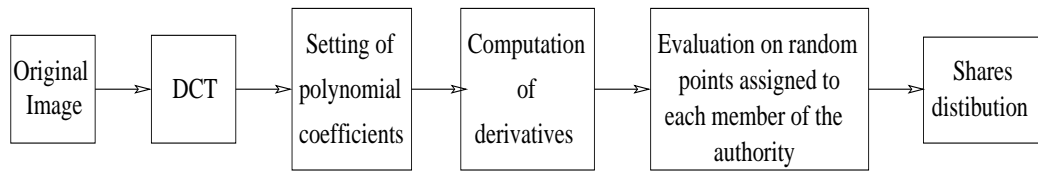


Fig. 1.

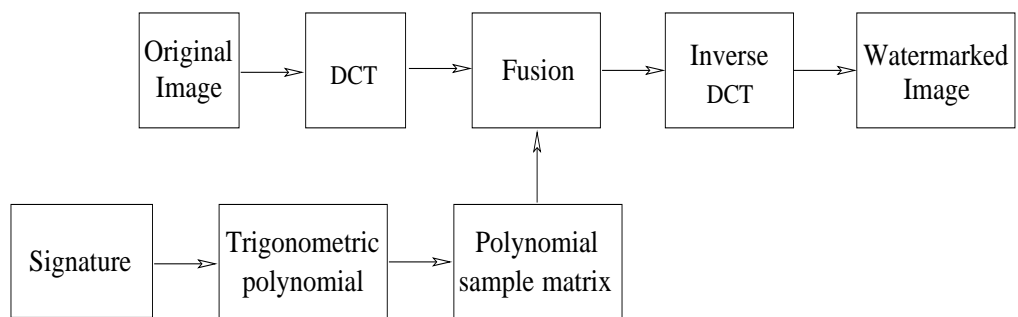


Fig. 2.

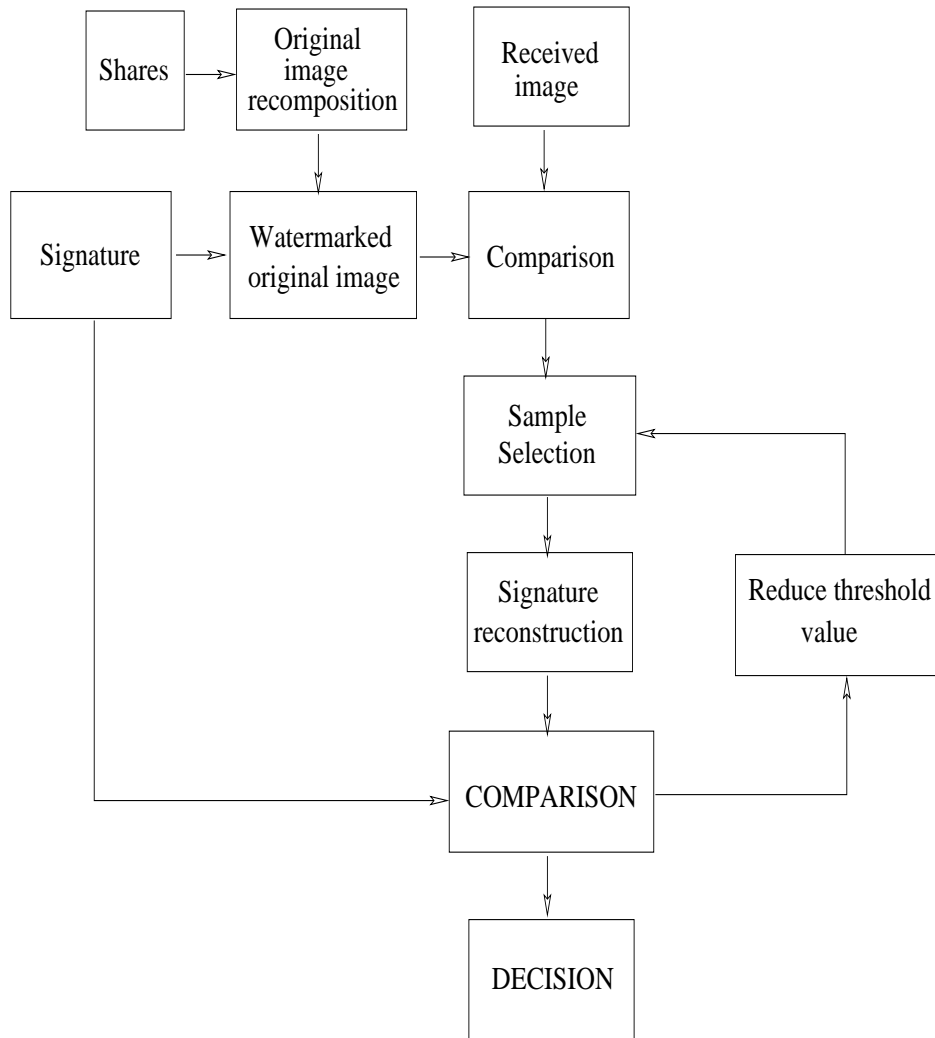


Fig. 3.

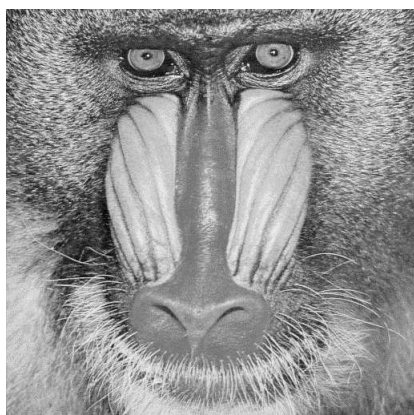


(a)

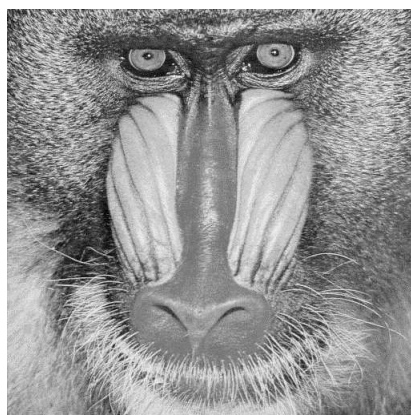


(b)

Fig. 4.

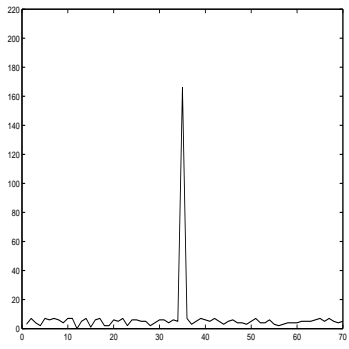


(a)

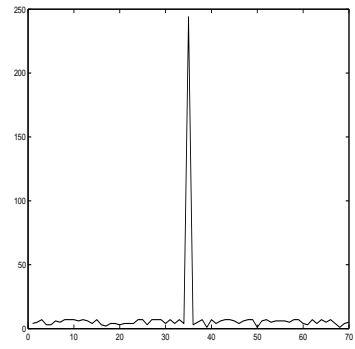


(b)

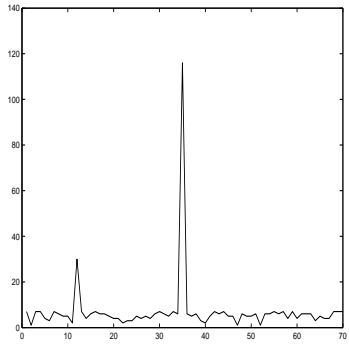
Fig. 5.



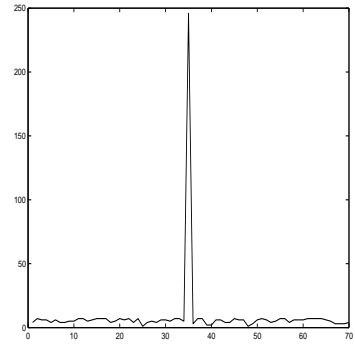
(a)



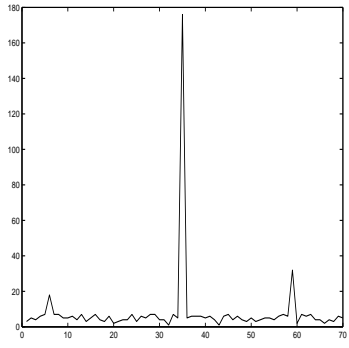
(b)



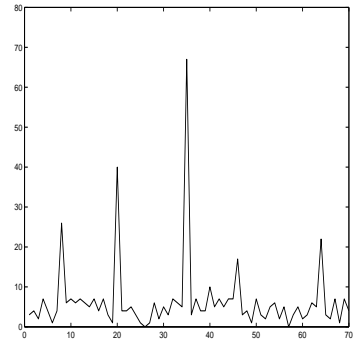
(c)



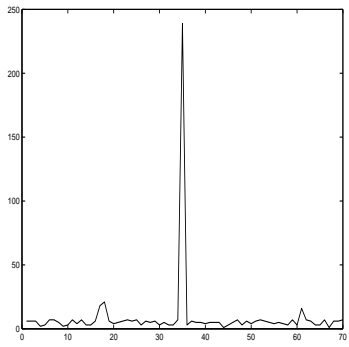
(d)



(e)

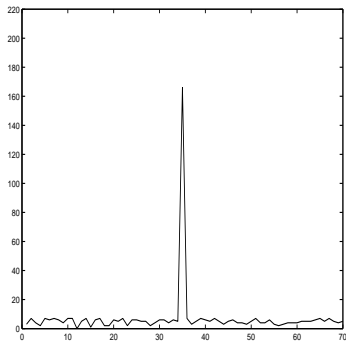


(f)

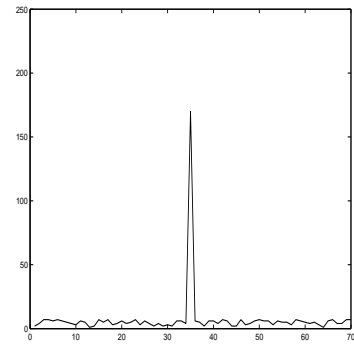


(g)

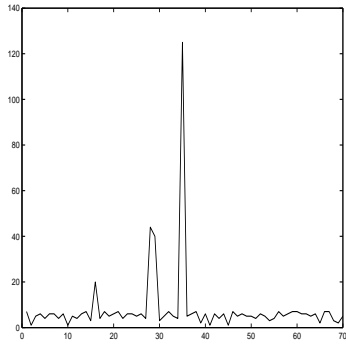
Fig. 6.



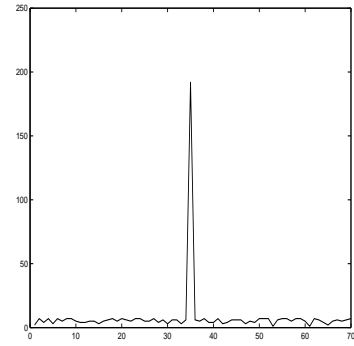
(a)



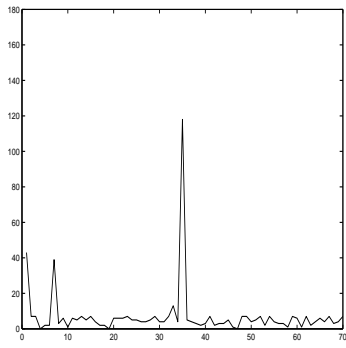
(b)



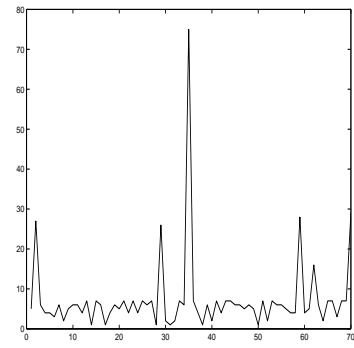
(c)



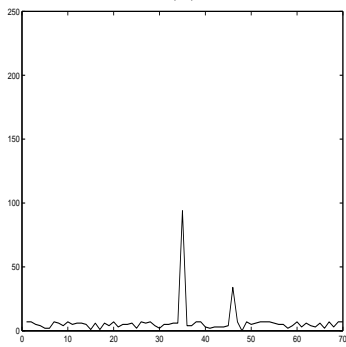
(d)



(e)



(f)



(g)

Fig. 7.

Table 1.

attack	PS	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	PS	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	PS	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