Proceedings of the International Multiconference on
Computer Science and Information Technology pp. 487–491

ISBN 978-83-60810-22-4
ISSN 1896-7094

Collusion-resistant Fingerprints Based on the Use of Superimposed Codes in Real Vector Spaces

Valery Korzhik (Member, IEEE),
Anton Ushmotkin and Artem Razumov
State University of Telecommunications
St. Petersburg, Russia
Email: korzhik@spb.lanck.net

Guillermo Morales-Luna
Computer Science, CINVESTAV-IPN
Mexico City, Mexico
Email: gmorales@cs.cinvestav.mx

Irina Marakova-Begoc
Bretagne Telecom, France
Email: marakova.irina@gmail.com

***Abstract*—In this work we propose the use of random superimposed codes as sequences for collusion-resistant fingerprints. This approach seems to be more suitable in comparison with the use of some other regular sequences (as WBE-sequences) against watermark removal attacks. Sphere decoding algorithm is used for tracing traitors. The performance evaluation of the proposed method is presented. Simulation results show a good efficiency of the proposed codes.**

***Index Terms*—Digital fingerprints, collusion attacks, superimposed codes, sphere decoding algorithm.**

I. Introduction

DIGITAL fingerprinting (FP) provides unique digital signatures associated with legitimate users in multimedia content. Hence each consumer redistributing illegally the content can be traced. These fingerprints are embedded in the original work using watermarking. Unfortunately, this robust watermarking technique is not enough to provide full tracing of traitors (e.g. illegal redistributors of works) under the condition of the so called *collusion attack*.

In last setting a group of dishonest users join their marked versions of the same content in order to produce some transformed work that is resistant to dishonest colluders tracing [1]. There are several types of collusion attacks, but we will consider only one of them namely *linear collusion attack* when colluders synchronize the media signals and average them adding some noise (it has been proved in [1] that the nonlinear attacks can be regarded as attacks by averaging).

There are two main approaches to create fingerprints: pseudo-random generated sequences and modulation coding. Pseudo-randomly generated FP-sequences with correlation detector of colluders do not provide good performances because both probabilities of colluder missing and false colluder detection are not as small as desired even for moderate numbers of colluders. Orthogonal modulation allows to improve slightly an efficiency of traitor tracing but the drawback of the orthogonal fingerprinting is that, when using n orthogonal basic vectors, at most n users can be accommodated. So orthogonal fingerprints are attractive only to applications involving small groups of users.

It seems to be natural to introduce correlation among fingerprints through *anti-collision codes* (ACC). Different types of ACC have been considered in [1] and first of all ACC based on *balanced incomplete block design* (BIBD) codes. Unfortunately they are not very effective if colluders use an averaging attack in combination with additive noise of the optimized power. Besides, the set of BIBD applicable to FP is very limited.

The authors of [2] used the so called *Welch Bound Equality* (WBE) *sequences* as FP. In order to provide good efficiency in traitor tracing it is necessary to use decoding based on minimizing Euclidean distance. This fact requires a guaranteed minimal Euclidean distance between averaged m-sums of FP under the condition that the number of colluders is at most m. On the other hand, WBE sequences taken as FP are able to provide only some known mean square correlation but no tight bounds for minimal Euclidean distances between averaged FP. Even though we try to use a special set of sequences (as those defined by Kasami or Khamaletdinov [3]) with known bounds for the absolute value of correlation, they cannot result in good bounds on Euclidean distance unless m is very small.

Moreover, in order to avoid a trivial attack with FP subtraction from the versions of the watermarked content, it is necessary that FP be secure. It is well known that there are several plausible sets of sequences with small correlation, however the number of such sets is not as large as desired. If we would try to encrypt insecure individual FP's $W_\tau = (w_\tau(\nu))_{\nu=1}^n$, $\tau = 1, 2, \dots, t$, by multiplying them by a key sequence $(k(\nu))_{\nu=1}^n$ we get each individual FP $\tilde{W}_\tau = (k(\nu)w_\tau(\nu))_{\nu=1}^n$. But in this case the key sequence may be recovered as:

$$\forall\nu = 1, 2, \dots, n: \quad k(\nu) = \frac{c_{\tau_1}(\nu) - c_{\tau_0}(\nu)}{w_{\tau_1}(\nu) - w_{\tau_0}(\nu)}$$

for any two different colluders τ_0, τ_1, where $C_\tau = (c_\tau(\nu))_{\nu=1}^n$ is the corresponding watermarked version of the τ-th user, and this is due because the FP's W_{τ_0}, W_{τ_1} are insecure under our assumption. In the case of individual secret keys $(k_\tau(\nu))_{\nu=1}^n$, when masking $\tilde{W}_\tau = (k_\tau(\nu)w_\tau(\nu))_{\nu=1}^n$, then the property of sequences with small correlation may be lost.

The main observation regarding the structure of ACC under the condition of average collusion and additive Gaussian noise attack is that ACC can be taken as an superimposed code in $\mathbb{R}^n$, introduced by Ericson and Györfi [4]. For any subset $A \subseteq \mathbb{R}^n$ let us denote by $\mathcal{F}(A)$ the collection of finite subsets in A, let $|\cdot| : \mathcal{F}(A) \to \mathbb{N}$ be the *cardinality* map and let

$f : \mathcal{F}(A) \to \mathbb{R}^n$, $B \mapsto f(B) = \sum_{x\in B} x$, be the map that associates to each finite set the addition of its elements. Let $\mathcal{F}_m(A) = \{B \in \mathcal{F}(A) | \, |B| \le m\}$ denote the collection of families of vectors in A with at most m members. Let $F^{(m)}(A) = f(\mathcal{F}_m(A))$ be the image of $\mathcal{F}_m(A)$ under map f, and let

$$\begin{aligned} d_0(F^{(m)}(A)) \;\; = \;\; & \min\{\|f(B_1) - f(B_2)\| \mid \\ & B_1, B_2 \in \mathcal{F}_m(A) \,\& \\ & f(B_1) \ne f(B_2)\} \end{aligned} \qquad (1)$$

be the minimal Euclidean distance within $F^{(m)}(A)$. A finite set $\mathbf{C}$ within the unit Euclidean sphere of $\mathbb{R}^n$ is an (n, m, t, d)-SIC (*superimposed code*) if $|\mathbf{C}| = t$ and $d_0(F^{(m)}(\mathbf{C})) \ge d$.

An (n, m, t, d)-SIC is indeed an ACC of dimension n for t users and it can be used against at most m colluders. (The difference in setting unit norm codewords and a simple summing in (1) instead of averaging can be get straightforward.)

Moreover, if colluders apply an additive noise attack jointly with averaging, then the optimal decoder has to find the minimum Euclidean distance over all possible coalitions of size m and the received attack vector (see next section for details). Hence in order to minimize the probability of colluder error detecting, the ACC should have the maximum possible d given m, t and n.

We can adopt the lower bound for t, given n, m and d, proved in [4] (this bound has been improved in [5] for an asymptotic case, but here we are requiring the bound for finite dimension n). Moreover, the lower bound has been derived in [4] as a *random-coding bound* when the code $\mathbf{C}$ is determined by its codeword matrix $X = [x_{ij}]_{1\le i\le t}^{1\le j\le n} \in \mathbb{R}^{t\times n}$, where x_{ij} is the j-th component in the i-th codeword, the entries x_{ij} are chosen pairwise independent, and

$$\Pr\left[x_{ij} = \frac{1}{\sqrt{n}}\right] = \Pr\left[x_{ij} = -\frac{1}{\sqrt{n}}\right] = \frac{1}{2}.$$

It is not surprising that randomly chosen code words give the best code with a large probability. This fact is well known from the theory of error correcting codes [6]. The main drawback of these codes is the fact that they have no a constructive error correcting algorithm because the number of code words in error correcting codes is typically intractable.

In our case, the number t of the words at ACC is equal to the number of users and therefore it is indeed a tractable value. But the number of possible coalitions consisting of m users, $\binom{t}{m}$, can be very large. Fortunately, there does exist the *sphere decoding algorithm* (SDA) providing a polynomial complexity for the cases which are important for practice [7]. Hence, we can adopt a randomly chosen ACC and the SDA as coding/decoding methods.

The rest of the paper is organized as follows: Section II presents the evaluation of the probability of erroneous colluder detection for randomly chosen SIC, in section III we briefly recall the sphere decoding algorithm, the simulating results are presented in section IV, and we conclude the paper in section V.

II. Performance evaluation of ACC

We note that although in [1] there are some formulas for similar probabilities, we present here extensions of probability formulas in terms of signal-to-noise ratios after watermarking and after attack.

Let us consider a family of pairwise distinct watermarks $\{W_\tau\}_{\tau=1}^{t}$, where the τ-th watermark is associated with the τ-th user for the purpose of traitor tracing. Then, the watermarked host signals (the *works*, as they are also known) can be expressed as follows: $\forall \tau \in \{1, \ldots, t\}$, $\nu \in \{1, \ldots, n\}$,

$$c_\tau^{(w)}(\nu) = c(\nu) + w_\tau(\nu)$$

where $C = (c(\nu))_{\nu=1}^n$ is the host signal, n is the number of samples with embedded watermarks. After collusion attack we get

$$\begin{aligned} c^{(wa)}(\nu) \;\; &= \;\; \frac{1}{s}\sum_{\tau\in S} c_\tau^{(w)}(\nu) + \varepsilon(\nu) \\ &= \;\; c(\nu) + \frac{1}{s}\sum_{\tau\in S} w_\tau(\nu) + \varepsilon(\nu) \end{aligned} \qquad (2)$$

where $S \subseteq \{1, \ldots, t\}$ is a coalition of colluders, $s = |S|$ is the number of colluders and $(\varepsilon(\nu))_{\nu=1}^n$ is an additive, sample-independent zero mean Gaussian noise with variance σ_ε^2.

The goal of the host owner is to detect a set of colluders S in the illegally redistributed copy of the host signal . We suppose that the host signal $(c(\nu))_{\nu=1}^n$ is known for the owner. This means that it can be used the so called *informed decoder* for colluders detection.

It is well known (see [1] and others) that the optimal informed collusion decoder for the model (2) is the decoder on minimum Euclidean distance in $\mathbb{R}^n$:

$$\tilde{S} = \underset{S\subseteq\{1,\ldots,t\}}{\text{arg min}} \left\| C^{(wa)} - C - \frac{1}{s}\sum_{\tau\in S} W_\tau \right\| \qquad (3)$$

where $\|\cdot\|$ is the Euclidean norm in $\mathbb{R}^n$. If the number s of colluders is unknown for the owner, then he (or she) can try one by one each $s \in \{1, \ldots, t\}$ and to take the s that provides the minimum value in the right side of (3) (but we will let for simplicity so far that s is known). We can easily transform the right side of (3) and then get:

$$\tilde{S} = \text{arg min} \sum_{\nu=1}^n \left[\left[\frac{1}{s}\sum_{\tau\in S} w_\tau(\nu)\right]^2 + \frac{2}{s} c^{(wa)}(\nu) \sum_{\tau\in S} w_\tau(\nu) \right] \qquad (4)$$

If the following condition holds true

$$\text{Invar}(S) := \sum_{\nu=1}^n \left[\frac{1}{s}\sum_{\tau\in S} w_\tau(\nu)\right]^2 = \text{const} \qquad (5)$$

then it is easy to show that the optimal collusion decoder has to create a variation series

$$\lambda_\tau = \sum_{\nu=1}^n c^{(wa)}(\nu) w_\tau(\nu) \qquad (6)$$

then to put the coefficients in decreasing order, and next to include in the coalition $\tilde{S}$ the users with the numbers corresponding to the first s members of the resulting variation series.

The condition (5) holds true if the watermark signals W_τ are pairwise orthogonal and they have equal norm. In the general case the decoding, rule (4) should be used. Then it is easy to show that the probability of erroneous colluder detection (e.g. to decide the presence of a coalition S', whereas actually a coalition S takes place) is

$$\Pr\left[S'|S\right] = Q\left[\frac{1}{2}\sqrt{\frac{d(S',S)^2}{\sigma_\varepsilon^2}}\right] = Q\left[\frac{d(S',S)}{2\sigma_\varepsilon}\right]$$

where

$$\begin{array}{rcl} d:(U,V) & \mapsto & d(U,V) = \left\| \frac{1}{u}\sum_{\tau\in U} W_\tau - \frac{1}{v}\sum_{\tau\in V} W_\tau \right\| \quad \text{and} \\ Q:x & \mapsto & Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^{+\infty} e^{-\frac{t^2}{2}}\,dt. \end{array}$$

Let the minimum Euclidean distance on the set of WM words be

$$d_0 = \min\{d(U,V)\,|\,U \neq V\}. \tag{7}$$

Then an upper bound for the probability of error is given as

$$P_e = \Pr\left[S'|S\right] \leq Q\left[\frac{d_0}{2\sigma_\varepsilon}\right]. \tag{8}$$

For the case of equally norm orthogonal WM's, say $\omega = \|W_\tau\|$, $1 \leq \tau \leq t$, we get

$$d_0 = \frac{\sqrt{2}}{s}\omega.$$

Unfortunately, as it was said before, this class of WM's is suitable just for a number of users limited by the number n of samples.

Let us consider a randomly chosen SIC $\mathbf{C}$, following [4]. Then the minimum Euclidean distance $d_0(F^{(m)}(\mathbf{C}))$, as given by relation (1), here denoted as $\tilde{d_0}$, is related with t and s by the following inequality [4]:

$$t = e^{n\,E(s,\tilde{d_0})}, \tag{9}$$

where

$$E:(u,d) \mapsto E(u,d) = \max_{\lambda\geq 0}\ \min_{1\leq\ell\leq u}\ \frac{1}{2\ell}\left[\phi_\lambda(\ell) - \lambda\, d^2\right]$$

and

$$\phi_\lambda : \ell \mapsto \phi_\lambda(\ell) = -\log\left[2^{-2\ell}\sum_{\kappa=-\ell}^{\ell}\binom{2\ell}{\ell+\kappa}e^{-4\lambda\kappa^2}\right].$$

Besides,

$$E(s,\tilde{d_0}) \geq A(\tilde{d_0})\ \min_{1\leq\ell\leq s}\ \frac{\log\sqrt{\pi\ell}}{2\ell}$$

where $A : d \mapsto A(d) = \max_{x\in[0,1]}\left[\frac{1-x}{1+x}\,x^{\frac{d^2}{4}}\right]$. Since the sequences considered in [4] are $\left(\pm\frac{1}{\sqrt{n}}\right)$-valued and $d_0(F^{(m)}(\mathbf{C}))$ does not involve any division by s, the connection between $\tilde{d_0}$ and d_0, where the last value is defined for $\mathbf{C}$ as a $(\pm\alpha)$-valued ACC for some real value α, is the following

$$d_0 = \frac{\sqrt{n}}{s}\tilde{d_0}\alpha. \tag{10}$$

We note that since all FP words are chosen truly randomly and pairwise independently, we do not face with a subtraction attack provided that these words are kept by the FP owner in a secret manner.

In order to express the error probability P_e in terms of *signal-to-noise ratio after attack* η_a, we note first of all that the *signal-to-noise ratio just after FP embedding* is

$$\eta_w = \frac{\sigma_C^2}{\alpha^2}$$

where $\sigma_C^2 = \mathrm{Var}(C)$ is the variance of content C. After an attack by averaging and the addition of zero mean noise with variance σ_ε^2 we get the signal-to-noise ratio as

$$\eta_a = \frac{\sigma_C^2}{\sigma_\varepsilon^2 + \frac{\alpha^2}{s}} \tag{11}$$

It is very reasonable for colluders to select σ_ε in such a way that it gives $\eta_w \approx \eta_a$. Then we would have $\sigma_\varepsilon^2 = \alpha^2$ and substituting this value into (8) we would get for the SIC $\mathbf{C}$:

$$P_e \leq Q\left(\frac{\sqrt{n}}{2}\,\frac{\tilde{d_0}}{s}\right).$$

III. Implementation of Sphere Decoding Algorithm

We adopt the *sphere decoding algorithm* (SDA) considered in [2]. It entails the following *integer least squares problem* (ILSP):

$$\text{Calculate} \quad \tilde{\mathbf{s}} = \arg\min_{\mathbf{s}\in\mathbb{Z}^n}\|\mathbf{x} - H\mathbf{s}\| \tag{12}$$

where (in terms of our notations introduced in section II) $\mathbf{x} = C^{(wa)} = \left(c^{(wa)}(\nu)\right)_{\nu=1}^{n}$ and $H \in \mathbb{R}^{n\times t}$ is the matrix whose columns are the SIC codewords multiplied by α and divided by s,

$$\forall\nu \leq n\ ,\ \tau \leq t: \quad h_{\nu\tau} = \frac{\alpha}{s}\,w_\tau(\nu).$$

In order to implement an ILSP solving procedure within SDA, it is necessary to impose the condition $t \leq n$. This condition can be achieved, whenever originally we would have $t > n$, by dropping the $t-n$ codewords producing the smallest values λ_τ according to relation (6) (indeed these $t-n$ users are the most likely innocent ones). Within this modification, the matrix H at (12) becomes of order $n \times n$, and it has full rank with a large probability.

First, let $H = QR$ be the QR-factorization of the matrix H. Then $Q \in \mathbb{R}^{n\times n}$ is an orthogonal matrix and $R \in \mathbb{R}^{n\times n}$ is an upper triangular matrix. In SDA, the ILSP (12) is posed as finding all $\mathbf{s} \in \mathbb{Z}^t$ satisfying

$$\|\mathbf{x} - H\mathbf{s}\| \leq r \tag{13}$$

TABLE I
MINIMUM EUCLIDEAN DISTANCES BETWEEN AVERAGED FP'S OF COLLUDERS FOR DIFFERENT ACC'S.

Type of ACC	s	d_0	d	t
The BIBD-$(7,3,1)$, $t=n=7$	2	2	1.323	2
BIBD-$(16,4,1)$, $t=20$, $n=16$	3	1.633	1.333	4
Randomly chosen SIC with $n=20$, $t=50$	3	1.333	1.491	5
Randomly chosen SIC with $n=100$, $t=200$	4	3.317	2.5	1505

s: size of coalition,
d_0: true minimum Euclidean distance,
d: estimated bound for d_0 according to (10) and (9) for $\alpha=1$ and $\tilde{d}=1$,
t: estimated lower bound for the number t of codewords according to (9)

where $r > 0$ is some given value. Being R upper triangular, by writing $\mathbf{x}' = Q^T\mathbf{x}$, relation (13) is equivalent to

$$r^2 \geq \|\mathbf{x}' - R\mathbf{s}\|^2 = \sum_{\nu=1}^{n}\left[x'_\nu - \sum_{\tau=\nu}^{n} r_{\nu\tau}s_\tau\right]^2. \qquad (14)$$

Obviously, for each $\nu_0 = n, n-1, \ldots, 1$, relation (14) entails

$$\left|x'_{\nu_0} - \sum_{\tau=\nu_0}^{n} r_{\nu_0\tau}s_\tau\right| \leq r, \qquad (15)$$

which allows to characterize recursively the set of feasible solutions $\mathbf{s} \in \mathbb{R}^n$ of relations (15). Indeed, the solution set can be represented by a tree of height n.

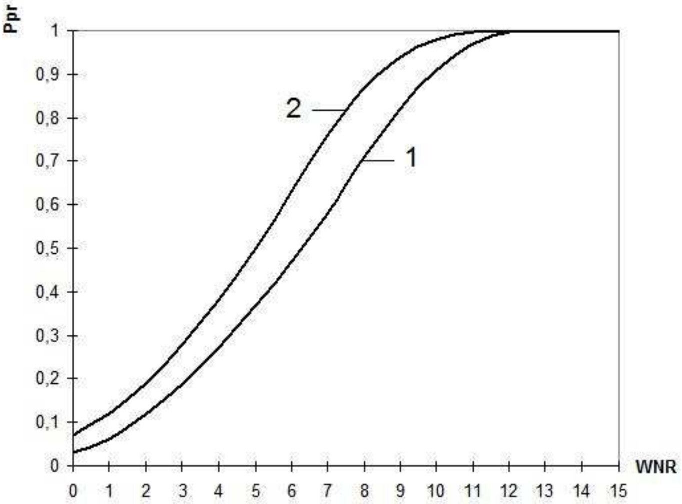
Within this tree, it is possible to perform a tree search algorithm in order to test all feasible points and pick the one with minimum Euclidean distance. Initially, for $s = 1$, let $r = \|W_\tau - (C_\tau^{(wa)} - C)\|$ where τ corresponds to the colluder monad of minimum distance. Increase s and solve (12) using the SDA with the current radius r. If the minimum distance at s is smaller than r, then update r with this minimum. Otherwise, stop.

It has been proved in [8] that for typical signal-to-noise ratio (η_a) values the expected complexity of SDA is polynomial, in fact, quite often roughly cubic.

IV. SIMULATION RESULTS

First of all we have found, according to (7), the minimum Euclidean distance of averaged colluders FP's for ACC's based on two types of BIBD's and one random SIC. The results of these calculations are presented in Table I (we were unable to calculate the value d_0 for a randomly chosen SIC, with $s = 4$, because it requires to test nearly $3 \cdot 10^{15}$ Euclidean distances, but we tested as many as possible among them).

We can see that the experimental values of d_0 are very close to the theoretical ones but the lower bound for the number of users t is much larger than the number of codewords in BIBD-based SIC's.



1) ACC-$(16,4,1)$
2) Randomly chosen SIC ($n = 20$, $t = 50$)

Fig. 1. The performance of the ACC as average fraction of captured colluders versus WNR.

Thereafter we tested the probability of correct detection P_d of a coalition consisting of $s = 3$ users for both BIBD-based codes and randomly chosen SIC's using the sphere decoding algorithm. The results are shown in Figure 1.

WNR (*watermark-to-noise ratio*) is defined as $20\,\log\left[\frac{\alpha}{\sigma_\varepsilon}\right]$. We mentioned before (see equation (11)) that WNR $= 0$ corresponds to maintain after attack the same signal-to-noise ratio η_a that just after watermarking η_w.

If each code symbol is embedded into an m-dimensional vector (say into different pixels of the image) then the WNR should be decreased by the value $20\,\log\sqrt{m}$.

We can see that the use of randomly chosen SIC provides practically the same performance (P_d) than the use of BIBD-based ACC, but the last code embraces much lesser number of users that the first one.

V. CONCLUSIONS AND FUTURE WORK

In this work, we proposed a FP design scheme that uses randomly chosen SIC instead of BIBD-based codes or WBE sequences as the underlying FP codes. This approach allows us a greater number of users to be accommodated for a given amount of FP dimension function (see the last row and column in Table I). On the another hand the proposed code provides a performance (in terms of P_d) even better than other "regular" FP codes and, at the same time, a perfect security against FP estimation attacks. This is a consequence of a random choice of FP and the use of SDA with its polynomial complexity for real scenarios.

In the future we are going to investigate more powerful SIC's using some improvements of SDA in order to provide an opportunity of simulation in reasonable times.

ACKNOWLEDGMENT

The authors would like to thank Prof. V. Ipatov for useful discussions.

Dr. Morales-Luna acknowledges the support of Mexican Conacyt.

This paper has been partially supported by Mexican SEP-CONACyT grant 80965, *Visión por Computadora Evolutiva*, leaded by Dr. Luis de la Fraga.

REFERENCES

[1] K. J. R. Liu, W. Trappe, Z. J. Wang, M. Wu, and H. Zhao, *Multimedia Fingerprinting Forensics for Traitor Tracing*. Hindawi Publishing Corporation, 2005.

[2] Z. Li and W. Trappe, "Collusion-resistant fingerprints from wbe sequence sets," in *IEEE International Conference on Communications (ICC)*, 2005, pp. 477–488.

[3] V. P. Ipatov, *Spread Spectrum and CDMA: Principles and Applications*. Wiley Chichester,, 2005.

[4] T. H. E. Ericson and L. Györfi, "Superimposed codes in R^n," *IEEE Transactions on Information Theory*, vol. 34, no. 4, pp. 877–, 1988.

[5] Z. Füredi and M. Ruszinkó, "An improved upper bound of the rate of euclidean superimposed codes," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 799–802, 1999.

[6] R. G. Gallager, *Information Theory and Reliable Communication*. Wiley, January 1968. [Online]. Available: http://www.amazon.ca/exec/obidos/redirect?tag=citeulike09-20&amp;path=ASIN/0471290483

[7] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Mathematics of Computation*, vol. 44, no. 170, pp. 463–471, 1985. [Online]. Available: http://dx.doi.org/10.2307/2007966

[8] B. Hassibi and H. Vikalo, "On the sphere-decoding algorithm i. expected complexity," *IEEE Transactions on Signal Processing*, vol. 53, no. 8-1, pp. 2806–2818, 2005.