

## COLLUSION-RESISTANT FINGERPRINTS BASED ON REAL SUPERIMPOSED CODES

VALERY KORZHIK, ANTON USHMOTKIN and ARTEM RAZUMOV

*State University of Telecommunications, St. Petersburg, Russia*  
*korzhik@spb.lanck.net*

GUILLERMO MORALES-LUNA

*Computer Science, CINVESTAV-IPN, Mexico City, Mexico*  
*gmorales@cs.cinvestav.mx*  
*http://delta.cs.cinvestav.mx/~gmorales*

IRINA MARAKOVA-BEGOC

*Bretagne Telecom, France*  
*marakova.irina@gmail.com*

We use random superimposed codes as sequences for collusion-resistant fingerprints. This approach is more suitable in comparison with the use of some other regular sequences (as WBE-sequences) against watermark removal attacks and traitor tracing is done through the sphere decoding algorithm. The performance evaluation of the proposed method is presented and the simulation results show an acceptable efficiency.

*Keywords:* Digital fingerprints; collusion attacks; superimposed codes; sphere decoding algorithm.

### 1. Introduction

Digital fingerprinting (FP) provides unique digital signatures associated with legitimate users in multimedia content, thus each consumer redistributing illegally the content can be traced. The fingerprints are embedded in the original work by watermarking. Unfortunately, robust watermarking techniques are not enough to provide full traitor tracing (e.g. illegal redistributors of works) under the so called *collusion attack*: a group of dishonest users join their marked versions of the same content in order to produce some transformed work resistant to dishonest colluders tracing [Liu et al. (2005)]. There are several types of collusion attacks, but we will consider only the *linear collusion attack*: the colluders synchronize their media signals and average them adding some noise (it has been proved in [Liu et al. (2005)] that the nonlinear attacks can be regarded as averaging attacks).

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 the probabilities of colluder missing and of false colluder detection are not sufficiently small even for a moderate number of colluders. Orthogonal modulation allows to improve slightly the efficiency of traitor tracing but in this case, 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 is natural to introduce correlation among fingerprints through *anti-collision codes* (ACC). Different types of ACC have been considered in [Liu *et al.* (2005)] among them the *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. In [Li and Trappe (2005)], the so called *Welch Bound Equality* (WBE) *sequences* are used as FP. In order to provide good efficiency in traitor tracing it is necessary to use decoding based on minimizing Euclidean distances. This entails the existence of a minimal Euclidean distance between the averaged  $m$ -sums of FP whenever there are at most  $m$  colluders. On the other hand, WBE sequences acting as FP provide only some known mean square correlation but no tight bounds for minimal Euclidean distances among averaged FP. Not even the sequences with known bounds for the absolute value of correlation (as those defined by Kasami or Khamaletdinov [Ipatov (2005)]) can provide good bounds on the 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 sequence sets with small correlation, however the number of such sets is small. If one encrypts insecure individual FP's  $W_\tau = (w_\tau(\nu))_{\nu=1}^n$ ,  $\tau = 1, 2, \dots, t$ , by multiplying them by a key sequence  $(k(\nu))_{\nu=1}^n$ , then one gets  $\tilde{W}_\tau = (k(\nu)w_\tau(\nu))_{\nu=1}^n$ . But in this case the key sequence may be recovered as

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

for any two different colluders  $\tau_0, \tau_1$ , where  $C_\tau = (c_\tau(\nu))_{\nu=1}^n$  is the corresponding watermarked version of the  $\tau$ -th user. The FP's  $W_{\tau_0}, W_{\tau_1}$  are thus insecure under our assumption. In the case of individual secret keys  $(k_\tau(\nu))_{\nu=1}^n$  when masking as  $\tilde{W}_\tau = (k_\tau(\nu)w_\tau(\nu))_{\nu=1}^n$ , then the property of sequences with small correlation may be lost.

Our main contribution departs by observing that under the condition of average collusion and additive Gaussian noise attack, the ACC can be taken as a *superimposed code in  $\mathbb{R}^n$*  (introduced at [Ericson and Györfi (1988)]).

For any subset  $A \subseteq \mathbb{R}^n$ , let  $\mathcal{F}(A)$  be the collection of finite subsets in  $A$ , let  $|\cdot| : \mathcal{F}(A) \rightarrow \mathbb{N}$  be the *cardinality* map and let

$$f : \mathcal{F}(A) \rightarrow \mathbb{R}^n \quad , \quad B \mapsto f(B) = \sum_{x \in B} x.$$

Let  $\mathcal{F}_m(A) = \{B \in \mathcal{F}(A) \mid |B| \leq m\}$  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

$$d_0(F^{(m)}(A)) = \min\{\|f(B_1) - f(B_2)\| \mid B_1, B_2 \in \mathcal{F}_m(A) \& f(B_1) \neq f(B_2)\} \quad (1)$$

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  $d_0(F^{(m)}(\mathbf{C})) \geq d$ . 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.

If the colluders apply an additive noise attack jointly with averaging, then the optimal decoder must find the minimum Euclidean distance of the received attack vector to all possible coalitions of size  $m$  (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 may adopt the lower bound for  $t$ , given  $n$ ,  $m$  and  $d$  (estimated in [Ericson and Györfi (1988)] and improved in [Füredi and Ruszinkó (1999)] for an asymptotic case, although here we are requiring the bound for finite dimension  $n$ ). The lower bound is indeed a *random-coding bound* when  $\mathbf{C}$  is given by its generator matrix  $X = [x_{ij}]_{\substack{1 \leq j \leq n \\ 1 \leq i \leq t}} \in \mathbb{R}^{t \times n}$ , 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 (as it is well known from the theory of error correcting codes [Gallager (1968)]). The main drawback of these codes is that they do not have a constructive error correcting algorithm because the number of code words in error correcting codes is typically intractable. In our case, the cardinality  $t$  of the ACC equals the number of users and therefore, however the number of possible coalitions consisting of  $m$  users,  $\binom{t}{m} = O(t^m)$ , can be very large. Fortunately, there does exist the *sphere decoding algorithm* (SDA) providing a polynomial complexity for practical cases [Fincke and M. Pohst (1985)]. Hence, we may adopt a randomly chosen ACC and the SDA as coding/decoding methods.

The rest of the paper is organized as follows: Section 2 presents the evaluation of the probability of erroneous colluder detection for randomly chosen SIC, in section 3 we briefly recall the sphere decoding algorithm, the simulating results are presented in section 4, and we conclude the paper in section 5.

## 2. Performance evaluation of ACC

We note that although in [Liu *et al.* (2005)] 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  $\tau$ -th watermark is associated with the  $\tau$ -th user for the purpose of traitor tracing. The watermarked host signals (or the *works*) are

$$\forall \tau \in \{1, \dots, t\}, \nu \in \{1, \dots, n\} : c_\tau^{(w)}(\nu) = c(\nu) + w_\tau(\nu)$$

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

$$c^{(wa)}(\nu) = \frac{1}{s} \sum_{\tau \in S} c_\tau^{(w)}(\nu) + \varepsilon(\nu) = c(\nu) + \frac{1}{s} \sum_{\tau \in S} w_\tau(\nu) + \varepsilon(\nu) \quad (2)$$

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

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, thus the so called *informed decoder* for colluders detection can be used. It is well known (see e.g. [Liu *et al.* (2005)]) that the optimal informed collusion decoder for the model (2) is the decoder on minimum Euclidean distance in  $\mathbb{R}^n$ :

$$\tilde{S} = \arg \min_{S \subseteq \{1, \dots, t\}} \left\| C^{(wa)} - C - \frac{1}{s} \sum_{\tau \in S} W_\tau \right\|. \quad (3)$$

If the number  $s$  of colluders is unknown for the owner, then the owner may try each  $s \in \{1, \dots, t\}$  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), namely:

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

Let us assume the condition

$$S \mapsto \sum_{\nu=1}^n \left[ \frac{1}{s} \sum_{\tau \in S} w_\tau(\nu) \right]^2 \text{ is a constant map,} \quad (5)$$

with  $S$  varying over the colluder coalitions. Then it is not too difficult to see that the optimal collusion decoder must create a variation series

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

thereafter to order decreasingly the coefficients, and next to include in the coalition  $\tilde{S}$  the users corresponding to the first  $s$  members of the resulting variation series.

The condition (5) holds if the watermark signals  $W_\tau$  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

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

where  $d : (U, V) \mapsto d(U, V) = \left\| \frac{1}{u} \sum_{\tau \in U} W_\tau - \frac{1}{v} \sum_{\tau \in V} W_\tau \right\|$  and  $Q : x \mapsto Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{+\infty} e^{-\frac{t^2}{2}} dt$ . Let the minimum Euclidean distance on the set of WM words be

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

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

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

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 [Ericson and Györfi (1988)]. Then the minimum Euclidean distance  $d_0(F^{(m)}(\mathbf{C}))$ , as given by (1), here denoted as  $\tilde{d}_0$ , is related with  $t$  and  $s$  by the following inequality [Ericson and Györfi (1988)]:

$$t = e^{n E(s, \tilde{d}_0)}, \quad (9)$$

where  $E : (u, d) \mapsto E(u, d) = \max_{\lambda \geq 0} \min_{1 \leq \ell \leq u} \frac{1}{2\ell} [\phi_\lambda(\ell) - \lambda d^2]$  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 [Ericson and Györfi (1988)] 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  $d_0$ , indeed within a  $(\pm\alpha)$ -valued ACC for some  $\alpha \in \mathbb{R}$ , is

$$d_0 = \frac{\sqrt{n}}{s} \tilde{d}_0 \alpha. \quad (10)$$

Since all FP words are chosen truly randomly and pairwise independently, there is no possibility of a subtraction attack provided that these words are kept in secret by the FP owner.

In order to express the error probability  $P_e$  in terms of *signal-to-noise ratio after attack*  $\eta_a$ , let us note that the *signal-to-noise ratio just after FP embedding* is  $\eta_w = \frac{\sigma_C^2}{\alpha^2}$  where  $\sigma_C^2 = \text{Var}(C)$  is the variance of content  $C$ . After an attack by averaging and the addition of zero mean noise with variance  $\sigma_\varepsilon^2$ , the signal-to-noise ratio becomes

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

It is very reasonable for colluders to select  $\sigma_\varepsilon$  in such a way that it gives  $\eta_w \approx \eta_a$ . Then,  $\sigma_\varepsilon^2 = \alpha^2$  and a substitution into (8) gives for the SIC  $\mathbf{C}$ ,  $P_e \leq Q\left(\frac{\sqrt{n}}{2} \frac{\tilde{d}_0}{s}\right)$ .

### 3. Implementation of the sphere decoding algorithm

We adopt the *sphere decoding algorithm* (SDA) considered in [Li and Trappe (2005)]. It entails the following *integer least squares problem* (ILSP):

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

where  $\mathbf{x} = C^{(wa)} = (c^{(wa)}(\nu))_{\nu=1}^n$  and  $H \in \mathbb{R}^{n \times t}$  is the matrix whose columns are the SIC codewords multiplied by  $\alpha$  and divided by  $s$ :  $h_{\nu\tau} = \frac{\alpha}{s} w_\tau(\nu)$ ,  $\forall \nu \leq n$ ,  $\tau \leq t$ . In order to implement an ILSP solving procedure within SDA, it is necessary to impose the condition  $t \leq n$  which can be achieved whenever  $t > n$ , if necessary by dropping the  $t - n$  codewords producing the smallest values  $\lambda_\tau$  according to relation (6) (indeed these  $t - n$  users are seemingly innocent ones). Within this assumption, the matrix  $H$  at (12) has order  $n \times n$ , and it has full rank with a large probability. Let  $H = QR$  be its  $QR$ -factorization. Then  $Q \in \mathbb{R}^{n \times n}$  is orthogonal and  $R \in \mathbb{R}^{n \times n}$  is upper triangular. In SDA, the ILSP (12) is posed as:

$$\text{Find all } \mathbf{s} \in \mathbb{Z}^t \text{ such that } \|\mathbf{x} - H\mathbf{s}\| \leq r \quad (13)$$

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

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

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

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

which allows to characterize recursively the set of feasible solutions  $\mathbf{s} \in \mathbb{R}^n$  of relation (15). Indeed, the solution set can be represented by a tree of height  $n$ . Indeed, in this tree it is possible to perform a tree search algorithm in order to test all feasible points and pick the one having minimum Euclidean distance. Initially, for  $s = 1$ , let  $r = \|W_\tau - (C_\tau^{(wa)} - C)\|$ , where  $\tau$  corresponds to the colluder monad of minimum distance. Then, let us increase  $s$  and solve (12) using the SDA with the current radius  $r$ . If the minimum distance at  $s$  is smaller than  $r$ , then let us update  $r$  with this minimum. Otherwise, let us stop.

It has been proved in [Hassibi and Vikalo (2005)] that for typical signal-to-noise ratio ( $\eta_a$ ) values the expected complexity of SDA is polynomial, in fact, quite often roughly cubic.

Table 1. Minimum Euclidean distances between averaged FP's of colluders for different ACC's.

Type of ACC	$s$	$d_0$	$d_{est}$	$t_{est}$
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,

$d_{est}$ : estimated bound for  $d_0$  according to (10) and (9) for  $\alpha = 1$  and  $\tilde{d} = 1$ ,

$t_{est}$ : estimated lower bound for the number  $t$  of codewords according to (9)

#### 4. Simulation results

First let us introduce in Table 1 an example of a calculation, according to (7), of the minimum Euclidean distance of averaged colluders FP's for ACC's based on two types of BIBD's and one random SIC (although we were unable to calculate the value  $d_0$  for a randomly chosen SIC, with  $s = 4$ , because almost  $3 \cdot 10^{15}$  Euclidean distances should be involved, we tested a representative sample). 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.

Thereafter in Figure 4, 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 is shown.

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  $\eta_a$  that just after watermarking  $\eta_w$ .

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  $20 \log \sqrt{m}$ . The use of randomly chosen SIC provides practically the same performance ( $P_d$ ) as the use of BIBD-based ACC, but the last code embraces a much lower number of users than that of the first one.

#### 5. Conclusions

We have proposed a FP design scheme using randomly chosen SIC instead of BIBD-based codes or WBE sequences as the underlying FP codes. This approach allows us to accommodate a greater number of users for a given amount of FP dimension function (see the last row and column in Table 1). 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

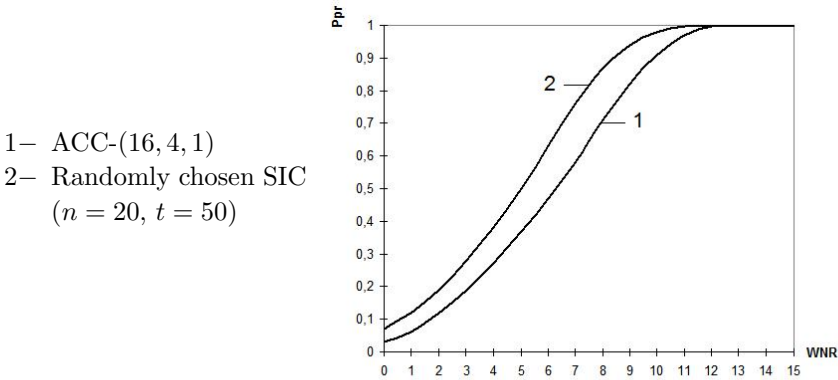


Fig. 1. The performance of the ACC for a coalition consisting of 3 users as an averaged fraction of captured colluders versus WNR.

is a consequence of a random choice of FP and the use of SDA with its polynomial complexity for real scenarios.

### Acknowledgments

The authors would like to thank Prof. V. Ipatov for useful discussions. Dr. Morales-Luna acknowledges the support of Mexican Conacyt.

### References

Ericson, T. H. E., Györfi, L. (1988) Superimposed codes in  $R^n$ , *IEEE Transactions on Information Theory*, **34**: 877–888.

Fincke, U., Pohst, M. (1985) Improved methods for calculating vectors of short length in a lattice, including a complexity analysis, *Mathematics of Computation*, **44**: 463–471. [Online]. Available: <http://dx.doi.org/10.2307/2007966>

Füredi, Z., Ruzinkó, M. (1999), An improved upper bound of the rate of Euclidean superimposed codes, *IEEE Transactions on Information Theory*, **45**: 799–802.

Gallager, R. G. (1968) *Information Theory and Reliable Communication*. Wiley, January.

Hassibi, B., Vikalo, H. (2005) On the sphere-decoding algorithm i. Expected complexity, *IEEE Transactions on Signal Processing*, **53**: 2806–2818.

Ipatov, V. P. (2005) *Spread Spectrum and CDMA: Principles and Applications*. Wiley Chichester.

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

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