Multimedia fingerprinting with noise via signature codes for weighted noisy adder channels and compressed sensing

Elena Egorova¹, Marcel Fernandez², and Moon Ho Lee³

¹ Skolkovo Institute of Science and Technology (Skoltech), Moscow region, Russia
  elena.egorova@skolkovotech.ru
² Universitat Politecnica de Catalunya, Barcelona, Spain
  marcel@entel.upc.edu
³ Division of of Electronics, Chonbuk National University, Republic of Korea
  moonho@jbnu.ac.kr

Abstract. We propose a new coding scheme for multimedia fingerprinting resistant to noise. Our scheme is based on signature codes for weighted noisy adder channel. The scheme (codes) can trace the entire coalition of pirates and provides significantly better rate than previously known fingerprinting schemes. We also establish a relationship between these two problems and the compressed sensing problem.

1 Introduction

There are the following well established concepts of digital fingerprinting codes known as tracing traitors [1] or codes with the identifiable parent property [2], and digital fingerprinting codes [3],[4], dealing with the problem of protection against unauthorized copying of discrete data. A theoretical model for data protection of continuous data was proposed in [5] and [6]. The corresponding codes, called multimedia fingerprinting codes, were investigated in [5] - [11]. First multimedia fingerprinting codes with nonvanishing rate, namely with the rate of order $t^{-2}$, where $t$ is the coalition’s size, were constructed in our paper [12]. Generalizations of results from [12] to the case of presence of noise was done in [13]. All previous considerations of multimedia fingerprinting codes were based on some discretisation, introduced in [5], i.e., only hard decoding of such codes was investigated. In this paper we consider the output of the corresponding channel without discretisation, i.e. we consider soft decoding of multimedia fingerprinting codes. We show that the corresponding model of multimedia fingerprinting channel without discretisation is equivalent to some modification of some model of the adder channel, considered in [14], which we call weighted adder channel. And signature codes for
the weighted real adder channel can be considered as multimedia fingerprinting codes with soft decoding. We show that the rate of multimedia fingerprinting codes with soft decoding is at least $1/t$ what is much larger than for the hard decoding which rate cannot exceed $O(t^{-2} \log t)$ even for the noiseless case, see [12].

2 Channel model of multimedia fingerprinting

Consider, following [5], [6], multimedia content being represented as a real-valued vector $x \in \mathbb{R}^m$, called the host signal. To prevent unauthorized redistribution of $x$, the dealer constructs a set of digital fingerprints using a linear modulation scheme that employs $n$ noise-like orthonormal signals (vectors) \( \{f_i \in \mathbb{R}^m \mid i = 1, \ldots, n, \ n \leq m \} \). The fingerprint $w_j$ of the $j$-th user \((j \in \{1, \ldots, M\})\) is represented as follows:

$$ w_j = \sum_{i=1}^{n} h_{ij} f_i, \quad (1) $$

where $h_{ij} \in \{+1, -1\}$ if for antipodal signals and $h_{ij} \in \{0, 1\}$ for on-off keying type of modulation. Below we consider the case on-off keying type of modulation. The sets of fingerprints \( \{w_j\} \) will be called a fingerprinting code. Equivalently and more convenient is to consider the set of $n$-dimensional binary vectors $h_j = (h_{1j}, \ldots, h_{nj})$ as binary multimedia fingerprinting code of length $n$, cardinality $M$ and rate $R = n^{-1} \log_2 M$.

The dealer distributes to the $j$-th user the vector

$$ y_j = x + w_j, $$

where one assumes that $\|x\|_2 \gg \|w_j\|_2$ in order to be sure that the fingerprinting scheme do not introduce significant changes in the host signal. A group of users, called colluders or pirates, aims to create an unauthorized copy of the contents such that the dealer cannot trace its origins to any of them. An important concept in digital fingerprinting, the Marking Assumption of [3], in the context of multimedia fingerprinting can be expressed in the following way: we assume that the members of the pirate coalition $J \subset \{1, \ldots, M\}$ cannot manipulate individual signals $f_j$, and are limited to linear attacks. By a linear attack we mean that pirates can generate a forged copy $\hat{y}$ of the host content only as a linear combination
of their copies $y_j$ with some coefficients $\lambda_j$

$$\hat{y} = \sum_{j \in J} \lambda_j y_j$$  \hspace{1cm} (2)

where $\lambda_j > 0$ for all $j$ and $\sum_{j \in J} \lambda_j = 1$. Hence

$$\hat{y} = x + \sum_{j \in J} \lambda_j w_j.$$  \hspace{1cm} (3)

The dealer calculates the vector $S = S(J, \{\lambda_j\}) = (s_1, \ldots, s_n)$, where

$$s_k = (\hat{y} - x, f_k) = \left\langle \sum_{i=1}^{n} \sum_{j \in J} \lambda_j h_{ij} f_i, f_k \right\rangle = \sum_{j \in J} \lambda_j h_{kj}$$  \hspace{1cm} (4)

and $\langle \cdot, \cdot \rangle$ denotes the inner product. Equivalently,

$$S = \sum_{j \in J} \lambda_j h_j,$$  \hspace{1cm} (5)

where $h_j = (h_{1j}, \ldots, h_{nj})$. It was suggested in [5], [6] to consider the following discretisation, when the dealer knows only whether $s_k = 0$, or $s_k = 1$, or that $0 < s_k < 1$, but does not know the value of $s_k$ in the last case. Note, that $s_k = 0$ means that $h_{kj} = 0$ for all $j \in J$, $s_k = 1$ means that $h_{kj} = 1$ for all $j \in J$ and finally $0 < s_k < 1$ means that

$$\{\cup_{j \in J} h_{kj}\} = \{0, 1\}$$  \hspace{1cm} (6)

It means that the dealer observes ternary output, i.e., the output of the 2-frequency noiseless multiple-access channel without intensity information [15] (the $A$-channel, for short), see more detailed explanation in the next section. This approach to constructing multimedia fingerprinting codes as signature codes for the $A$-channel was developed in [12].

In almost all previous works on multimedia fingerprinting codes it was assumed that the dealer observes the forged copy $\hat{y}$ without noise. This simplified assumption is not very realistic. Indeed, there are at least two sources of noise: a measurement noise, and a malicious noise, produced by the coalition. Therefore we assume that the dealer observes the following vector as a result of coalition forgery

$$z = x + \sum_{j \in J} \lambda_j w_j + E,$$  \hspace{1cm} (7)
where \( \mathbf{E} = (E_1, \ldots, E_m) \) and let for simplicity \( E_i \) be i.i.d.r.v. Similarly to (4) and (5) the dealer evaluates

\[
s_k(\mathbf{E}) = (\tilde{z} - \mathbf{x}, f_k)
\]

and the following vector

\[
\mathbf{S}(\mathbf{E}) = (s_1(\mathbf{E}), \ldots, s_n(\mathbf{E})) = \sum_{j \in J} \lambda_j \mathbf{h}_j + \mathbf{e}, \tag{8}
\]

where \( \mathbf{e} = (e_1, \ldots, e_n) \) and \( e_k = (\mathbf{E}, f_k) \). Based on the known value of the vector \( \mathbf{S}(\mathbf{E}) \) the dealer tries to reveal (to trace) the whole coalition, which produced this forgery, or at least one of its members. We shall consider \( \mathbf{S}(\mathbf{E}) \) as the output of continuous multimedia fingerprinting channel which is in fact a modification of well known adder channel with noise. We call this channel as weighted adder channel. Indeed, equation (8) with \( \lambda_j \equiv 1 \) and \( \mathbf{e} = \mathbf{0} \) describes the output of the adder channel with binary input in the case of \( t \) active users among \( M \), and \( \lambda_j \) plays the role of weights. We show that multimedia fingerprinting codes capable to trace the whole coalition of size \( t \) are in fact the same as \( t \)-signature code for the weighted adder channel, and the number of users \( M \) equals to the cardinality of the corresponding signature code. Note that an intermediate case of the weighted adder channel \( \lambda_j > 0 \) was firstly considered in [14] (where weights \( \lambda_j \) were called gains) but consideration of noise was restricted in [14] to the very particular case \( \mathbf{e} = b \mathbf{1} \), where \( b \) is a real number. Finally, we establish a relationship between the weighted adder channel and the compressed sensing problem [16],[17].

3 Codes for noiseless weighted adder channel

Recall that the dealer observes the output of the following multiple-access channel, which we called the weighted adder channel (WAC, for short), see (8), with unknown weights \( \lambda_j \) and unknown set \( J \) of active users of WAC, i.e., the set of traitors. The dealer goal is to find the set \( J \), what corresponds to zero-error coding for multiple-access channel (MAC) with partial activity, i.e. not all possible users of MAC are active, but not more than \( t \) of them. We shall consider the set of \( n \)-dimensional binary vectors \( \mathbf{h}_j = (h_{1j}, \ldots, h_{nj}) \) as a binary multimedia fingerprinting code of cardinality \( M \) capable to find any set of \( t \) or less traitors in the
case of s noiseless WAC iff for any subsets $J, J' \subset \{1, \ldots, M\}$ such that $|J| \leq t$, $|J'| \leq t$ the following equality

$$\sum_{j \in J} \lambda_j h_j = \sum_{j \in J'} \lambda'_j h_j$$

implies that $J = J'$ (and $\lambda_j = \lambda'_j$ for all $j$).

It’s easy to see that this condition is equivalent to the linear independence (over real numbers) of any $2t$ vectors $h_j$. Such effective set of vectors is well known in coding theory as columns of a parity-check matrix of a binary BCH code of length $M$ and redundancy $n$, correcting $t$ errors. Indeed, any $2t$ columns are linear independent over the field of residues by module 2, and hence they are independent over the rational numbers and also over the real numbers since in all cases dependency means that the determinant of the corresponding $t \times t$ minor equals to 0. It is not clear if this construction is even weakly optimal, i.e., has the minimal possible order of $n$ as a function of $M$ - for binary BCH-codes it gives $n = t \log_2 M(1 + o(1))$. Anyway we see that in the case of absence of quantization, i.e. soft decision, the rate of the best multimedia fingerprinting code is at least $1/t$ whereas for hard decoding the rate of any multimedia fingerprinting code is $O(t^{-2}\log t)$ [12].

4 Codes for noisy weighted adder channel and the compressed sensing problem

Now we want to construct codes which are capable to recover a set $J$ by its “syndrom” $S(E) = \sum_{j \in J} \lambda_j h_j + e$, see equation (8).

It is very similar to the compressed sensing problem, see [16],[17], with the only three differences:

for “weakly” multimedia fingerprinting code it is sufficient to find at least one $j \in J$ for sure;
for multimedia fingerprinting we need to find only the “error” set $J$, and solution of compressed sending problem means to find $J$ and values $\lambda_j$; vectors $h_j$ are binary.

Consider slightly other statement of the problem, more in the spirit of coding theory, namely, that the number of errors is limited, i.e., $wt(e) \leq T$. A solution of this problem was given in [18], see also [19]. If to omit details (which can be found in [18]) then in order to correct $T$ syndrome’s errors one should “add” $T \log(t \log M)$ redundant symbols what gives the total redundancy $n = t \log_2 M + T \log_2 \log_2 M + T \log_2 t$. It is easy to
check that for $T - \text{const}$ it keeps the same order of rate, namely $R = t^{-1}(1 + o(1))$. Note that a similar technique was used in [20].

5 Conclusion

Let us note in conclusion that the problem of noise in multiple-access channels was almost ignored probably because of the following remark in [15]: “A more sophisticated model taking such errors into account could easily be developed. One method would be to use a noisy channel in cascade with our noiseless channel. It is our contention, however, that although the details are different, the basic ideas are the same in the noisy and noiseless cases.” Our construction is much better than such simple cascade.

Acknowledgments

The work of M. Fernández has been supported by the Spanish Government through projects Consolider Ingenio 2010 CSD2007-00004 “ARES,” and TEC2015-68734-R (MINECO/FEDER) “ANFORA.”

References


