Collusion-Secure Fingerprint Watermarking for Real World Applications

Marcel Schäfer, Waldemar Berchtold, Sascha Zmudzinski, Martin Steinebach
Fraunhofer Institut für Sichere Informationssysteme SIT, Darmstadt, Germany*
{schaefer,berchtold,steinebach,zmudzinski}@sit.fraunhofer.de

Margareta Heilmann
Department of Mathematics, Bergische Universität Wuppertal, Germany
margareta.heilmann@math.uni-wuppertal.de

Stefan Katzenbeisser
Department of Computer Science, Technische Universität Darmstadt, Germany
katzenbeisser@seceng.informatik.tu-darmstadt.de

Abstract: Digital transaction watermarking today is a widely accepted mechanism in multimedia security. One major threat on transaction watermarking are collusion attacks. Here multiple individualized copies of the work are mixed to produce a counterfeited or undetectable watermark. One common countermeasure is the usage of so-called fingerprints. Theoretical fingerprint approaches do not consider the inaccuracy of the detection process of watermarking algorithms. In this work we show how an existing fingerprint code can be optimized with respect to code length in order to collaborate with a watermarking algorithm to provide a maximum of reliability with a minimum of payload.

1 Introduction

In the Internet, copies of digital works, ranging from pictures, music, audio books, videos, movies to software, are distributed illegally via various channels. An answer to this challenge of massive copyright infringement are digital watermarking algorithms. Watermarking imperceptibly hides information in multimedia data. This is done, for example, by changing statistical characteristics or quantization properties of multimedia data in a suitable transformed spectral domain. The hidden information is called *watermark message* or just *watermark*.

If a distributor of multimedia, for example in an online shop, wants to prevent his works from being illegally distributed by its customers, he can use transaction watermarking.

*This work was supported by the *CASED Center for Advanced Security Research Darmstadt*, Germany, funded under the *LOEWE* programme by the Hessian state government (*http://www.cased.de*).

Here, the watermark message is an *individual* identifier, e.g. a binary transaction ID, that can distinguish the distributed copies from each other. If the copy appears in an illegal source, the transaction ID allows to trace back to the customer at any later date. In this way customers are discouraged from illegal distribution of their bought copies in the Internet and reminded of their individual responsibility for respecting the copy right [CFNP00].

One specific security attack in a transaction watermarking scenario representing a significant security threat is the so called *collusion attack*. Here, several customers collaborate and can reveal detail about the watermark algorithm by comparing their individually watermarked user copies. The *colluders* can identify the location of the embedded watermark message and create a new copy of a media file by calculating the average among all user copies. The resulting copy may contain a destroyed or counterfeited watermark message.

One countermeasure to collusion attacks are *collusion-secure fingerprints* [BS98]. These are transaction watermark messages designed to be robust against such attacks. Collusion-secure fingerprints are created under specific additional conditions and assumptions which drastically increases the code length of the embedded message. Thus, a serious challenge most existing fingerprinting algorithms have to face is to provide a code length which is not beyond the limitations of the related embedding algorithms in practice.

One promising example still observing satisfying error probabilities is given by *Skoric* et al. in [SKC08]. However, most existing fingerprint coding approaches are based on simulated results and no specific watermark embedding/detector algorithm is considered. That means they act on the assumption, that every bit of the detected watermark has been detected equally reliably. In practice this assumption is no longer true. Many real world watermark detectors, as for example introduced in an earlier work [Ste03], output a goodness value for every bit, which describes how reliable this bit is retrieved to be '1' or '0'. Thus, combining an existing fingerprinting code directly with a real world watermarking algorithm causes an additional error, respectively the estimated theoretical error probabilities are in doubt.

As a solution to this problem we propose a modified version of *Skoric*'s fingerprinting codes [SKC08] by introducing specific *weights* representing the goodness of the watermark detector and apply them them to *Skoric*'s accusation sums. These weights eliminate the additional error and maintain the error probabilities provided by the earlier theoretical approaches. This is achieved with only a slight increment of *Skoric*'s code length. Therewith we create a new fingerprinting code which can be applied to real world watermarking algorithms.

2 Related Work

2.1 Modified Tardos Code for arbitrary alphabet size

The basic idea of the construction is based on *Skoric* [SKC08] and *Tardos* [Tar03]. Here, *Skoric* et al. provide an ε_1-sound and (ε_2,c_0)-complete fingerprinting code. That is, the scheme provides a false positive error rate ε_1 and a false negative error rate ε_2 (see Defini-

tions 9 and 10). The quantity c_0 denotes the maximum number of colluders for which the scheme works.

The basic restriction for the attackers to perform manipulations we assume in this work is the often made *marking assumption*: during the collusion attack, the colluders are only able to change those message bits in the fingerprint where the bits, i.e. the related watermarked content, is different.

The *Tardos* and *Skoric* fingerprinting scheme generates an $n \times m$ matrix X, where n denotes the number of users to be listed in the system and m stands for the length of the distributed fingerprint. Thus, the jth row of the matrix corresponds to the fingerprint which is later embedded in the copy that is released to customer $j \in \{1, ..., n\}$. The entries X_{ji} of the matrix X are generated in two steps:

First, the distributor picks m independent random numbers $\{p_i\}_{i=1}^m$ over the interval $p_i \in [t, 1-t]$, with $t = (300c)^{-1}$, where c is the number of colluders. Each $p_i = \sin^2(r_i)$ is selected by picking uniformly at random the value $r_i \in \left[\bar{t}, \frac{\pi}{2} - \bar{t}\right]$ with $0 < \bar{t} < \frac{\pi}{4}$, where $\sin^2(\bar{t}) = t$. Second, the matrix X is selected, by picking each entry X_{ji} independently from the binary alphabet $\{0, 1\}$ according to $\mathbb{P}[X_{ji} = 1] = p_i$.

Tardos' choice of the distribution for p_i is biased toward the values close to '0' or '1' which is motivated by the *marking condition*. This distribution is realized by a probability density function f which is symmetric around 0.5 and heavily biased towards values of p_i close to the limits of the interval $[t, 1-t]$.

Definition 1 (Tardos' probability density function)

$$f(p) \;=\; \frac{1}{2\arcsin(1-2t)} \frac{1}{\sqrt{p(1-p)}}, \quad p \in [t, 1-t].a \tag{1}$$

If the distributor then receives an unauthorized copy with embedded fingerprint y by chance, he creates the so called accusation sum A_j for each user j out of his given fingerprint X_j and y to identify at least one of the colluders:

Definition 2 (Skoric's accusation sum A_j)

$$A_j(\bar{\boldsymbol{p}}, X, y) \;:=\; \sum_{i=1}^{m} A_j^{(i)}\,, \quad A_j^{(i)} \;:=\; \delta_{y_i X_{ji}} g_1(p_{y_i}^{(i)}) + [1 - \delta_{y_i X_{ji}}] g_0(p_{y_i}^{(i)}). \tag{2}$$

Here, $\delta_{y_i X_{ji}}$ denotes the Kronecker Delta, and $p_{y_i}^{(i)}$ stands for the probability of the entries of the matrix X. The so called accusation functions g_1 and g_0 are as follows:

Definition 3 (The accusation functions g_1, g_0)

$$g_1(p) \;:=\; \sqrt{\frac{1-p}{p}} \qquad g_0(p) \;:=\; -\sqrt{\frac{p}{1-p}}. \tag{3}$$

The accusation functions g_1 and g_0 have specific properties: The more p increases, the smaller becomes $g_1(p)$. This means, the higher the probability of the symbol at this position, the smaller will be the positive amount given to the according accusation sum A_j, and vice versa.

The distributor accuses user j to be guilty, if his accusation sum A_j exceeds a predefined accusation threshold Z depending on the maximum number of colluders c_0 of the scheme.

To conduct the proof of soundness one has to evaluate over the degrees of freedom of the accusation sum. For the proof of completeness one has to average over the fingerprint matrix X_C of the colluders. This is done by averaging over the so called collective accusation sum A_C. Here the index *C* stands for the set of colluders.

Definition 4 (Skoric's collective accusation sum A_C)

$$A_C \;:=\; \sum_{j\in C} A_j \;=\; \sum_{i=1}^{m} A_C^{(i)}\,; \quad A_C^{(i)} \;:=\; b_{y_i}^{(i)} g_1(p_{y_i}^{(i)}) + [c - b_{y_i}^{(i)}] g_0(p_{y_i}^{(i)}). \tag{4}$$

The parameter $c \leq c_0$ represents the number of colluders, while $b_{y_i}^{(i)}$ stands for the number of occurrences of the symbol $y_i \in \{0,1\}$ in X_C at the position i. Thus holds $b_0 = c - b_1$. The requirement on the code length m for a binary alphabet providing ε_1-soundness and (ε_2,c_0)-completeness and requiring $c_0 \geq 10$, is given by

Definition 5 (Code length m and threshold parameter Z)

$$m \;=\; Ac_0^2 \,\ln\left(\varepsilon_1^{-1}\right), \quad Z \;=\; Bc_0 \ln\left(\varepsilon_1^{-1}\right) \tag{5}$$

with code length parameter $A = \pi^2$ and threshold parameter $B = 2\pi$.

2.2 Audio Watermarking

Digital watermarking schemes have been under research and development for various types of multimedia data for many years, including audio formats like PCM, mp3 or MIDI. In this work we focus on digital PCM audio data. Several approaches for PCM audio watermarking have been introduced in the literature, like in [BTH96], in [CMB02] or also [Ste03]. The latter algorithm is the base of this work.

The technique for incorporating the watermark follows a spread spectrum Patchwork approach [BGML96]:

1. As a first step, the algorithm divides the audio signal into segments, known as windows or frames. Then, the PCM source signal in each frame is transformed to the frequency spectrum using a Fast Fourier Transform (FFT).

2. Then, the watermark is incorporated by the deliberate alternation of FFT energy coefficients according to the Patchwork embedding rule: two disjoint subsets A and B

are selected from all energy coefficients. The selection of the coefficients is done pseudo-randomly dependent on a secret key. Depending on the message bit to be a '0' or '1', respectively, all coefficients in A are increased in energy while all in B are decreased, or vice versa, respectively. This introduces a significant difference in the *mean* energies in the two subsets. The degree of the changes in the frequency domain is controlled by a psycho-acoustic model such that audible distortions are avoided as good as possible.

3. In the final step, the algorithm converts the data back into PCM format. In order to prevent noticeable gaps between the segments, special mechanisms are used to fade between marked and unmarked parts of the audio.

The retrieval process consists of the following steps:

1. The marked audio is divided again into frames and the FFT is applied on the PCM samples. Appropriate synchronizations mechanisms to detect the correct file positions are not discussed here.

2. The watermark message bit is then retrieved as follows: If the correct secret key is available, the same subsets A and B of FFT coefficients used during embedding are selected. Now the difference in the mean energies between the two subsets can be analyzed: the sign of this energy difference indicates if the message bit is a '0' or '1'. The absolute value can be considered as a goodness of the detection. We will refer to this as its *detection score* in the following.

3 The Model

In this chapter we introduce a modification of the accusation sum of [SKC08], which allows to include information on the reliability of a detected watermark bit.

Closer analysis shows that for a fixed code length the actual false positive error rate ε_1 increases about a factor of almost 1.6 when applying for example the *Skoric* code with our real world watermarking algorithm. This is because in fingerprinting algorithms based on the *Tardos* Code, small and large absolute values of the detection score would be evaluated equally. In contrast, we introduce that message bits with smaller detection score contribute less to *Skoric*'s accusation sum, (2). Motivated by this, special weights $w^{(i)} \in [0, 1)$ are introduced, representing the goodness of detection.

Definition 6 (Weight function $w^{(i)}$)

$$w^{(i)} := w(score^{(i)}) := 1 - e^{-|score^{(i)}|}, \tag{6}$$

where the function argument is the output of the watermarking algorithm described in Section 2.2, also referred to as the score.

The choice of the weight function $w^{(i)}$ is such that the weights always lie in the range of $[0, 1)$.

In our construction, we include the weights in the accusation sum as follows:

Definition 7 (Weighted accusation sums)

$$\begin{aligned} \tilde{A}_j &:= \sum_{i=1}^{m} \tilde{A}_j^{(i)}\,, \quad \textit{with } \tilde{A}_j^{(i)} := w^{(i)} \left[\delta_{y_i X_{ji}} g_1(p_{y_i}^{(i)}) + (1 - \delta_{y_i X_{ji}}) g_0(p_{y_i}^{(i)})\right] \\ \tilde{A}_C &:= \sum_{i=1}^{m} \tilde{A}_C^{(i)}\,, \quad \textit{with } \tilde{A}_C^{(i)} := w^{(i)} \left[b_{y_i}^{(i)} g_1(p_{y_i}^{(i)}) + (c - b_{y_i}^{(i)}) g_0(p_{y_i}^{(i)})\right] \end{aligned} \tag{7}$$

It can easily be seen, that $\tilde{A}_j^{(i)}$ equals $w^{(i)} \cdot A_j^{(i)}$ of Equation (2), as well as $\tilde{A}_C^{(i)}$ equals $w^{(i)} \cdot A_C^{(i)}$ of Equation (4).

To keep the generality of the scheme, w and its expectation values are held as fixed parameters during all computations. This is done to remain independent of the particular watermarking algorithm (as long it provides a score for every detected message bit) and to give a general statement of this scheme using weights.

Estimating the conditions of soundness and completeness presented in Sections 4.2 and 4.3 against each other we obtain the following theorem according to *Skoric*'s definition of the code length (5).

Theorem 1 *To satisfy the bounds ε_1 and ε_2, the code length parameter A in the proposed scheme can be bounded as*

$$\frac{\pi^2}{\mathbb{E}[w^2]} \left(1 + \sqrt{\frac{1}{c_0} \frac{\ln(\varepsilon_2)}{\ln(\varepsilon_1)}}\right)^2 \;\leq\; A,$$

where $\mathbb{E}[w^{(i)}]$ denotes the expectation value of the weight function.

The proof of **Theorem 1** is given in Section 4. From this it follows directly from (5):

Corollary 2 *The proposed scheme provides ε_1-soundness and (ε_2,c_0)-completeness with a required minimum code length of*

$$m \;\geq\; \frac{\pi^2}{\mathbb{E}[w^2]} \left(1 + \sqrt{\frac{1}{c_0} \frac{\ln(\varepsilon_2)}{\ln(\varepsilon_1)}}\right)^2 c_0^2 \,\ln\left(\varepsilon_1^{-1}\right).$$

To get a more manageable expression for m, the term within the round brackets can be neglected since ε_1 is assumed to be much smaller than ε_2. Thus we have the estimate

$$m \geq \frac{\pi^2}{\mathbb{E}[w^2]} \cdot c_0^2 \ln\left(\varepsilon_1^{-1}\right) \tag{8}$$

for the minimum code length. The threshold Z stays alike Equation (5).

These weighted accusation sums provide a minimum code length which is longer than the results in [SKC08] about only $1/\mathbb{E}[w^{(i)}]$. The difference to [SKC08] is, if the detection process is not really sure if the detected bit is a '1' or a '0', the weight at that position will be close to zero, and therefore it will only contribute of probably unsafe information to the scheme only a little. The *Skoric* Code does not take this into account, and therewith creates an additional error which might falsifies the results.

An explicit example for the code length m is given in table 1. Here the maximum number of colluders, c_0, is set to 10 and $\mathbb{E}[w^2]$ for our weight function equals 0.888.

4 Proofs

This section gives a short insight into the proofs for correctness of our scheme. For a more detailed description see [Sch09].

4.1 Preliminaries

The following subsection shows up premises for the weighted accusation sums to conduct the proof schemes in 4.2 and 4.3 analogously to [SKC08]. Therefore we adopt:

Definition 8 (Definition of soundness) *Let $\varepsilon_1 \in (0,1)$ be a fixed constant and let j be an arbitrary innocent user. The fingerprinting scheme is ε_1-sound if for all collusions $C \subseteq [n]\backslash j$ and for all C-strategies holds*

$$\mathbb{P}[\textit{False positive}] \;=\; \mathbb{P}[j \in \Sigma] < \varepsilon_1. \tag{9}$$

The parameter C is the set of colluders, whereas Σ means the group that is accused as colluders, and n is the number of all users.

Definition 9 (Definition of completeness) *Let $\varepsilon_2 \in (0,1)$ and $c_0 \in \mathbb{N}^+$ be fixed constants. The fingerprint scheme is (c_0, ε_2)-complete if for all collusions C of size $c \leq c_0$ and all strategies holds*

$$\mathbb{P}[\textit{False negative}] \;=\; \mathbb{P}[C \cap \Sigma = \emptyset] < \varepsilon_2. \tag{10}$$

To prove that our scheme is ε_1-sound and (c_0, ε_2)-complete under certain conditions we need further quantities. In a similar way as in [SKC08] we define:

Definition 10

$$\mu_{j,w} \;:=\; \frac{\mathbb{E}_{wyX_p}[\tilde{A}_j]}{m} \;=\; \mathbb{E}_{wyX_p}\left[\tilde{A}_j^{(i)}\right]; \quad \sigma^2_{j,w} \;:=\; \frac{\mathbb{E}_{wyX_p}[\tilde{A}_j^2] - \mathbb{E}^2_{wyX_p}[\tilde{A}_j]}{m} \tag{11}$$

Definition 11

$$\mu_{c,w} := \frac{\mathbb{E}_{wyXp}[\tilde{A}_C]}{m} = \mathbb{E}_{wyXp}\left[\tilde{A}_C^{(i)}\right] ; \sigma_{c,w}^2 := \frac{\mathbb{E}_{wyXp}[\tilde{A}_C^2] - \mathbb{E}_{wyXp}^2[\tilde{A}_C]}{m} \quad (12)$$

Thus, the summarized expectation value $\mathbb{E}_{wyXp}$ consists of $\mathbb{E}_w$ denoting the expectation value of $w^{(i)}$, and $\mathbb{E}_{X_j}$ which is the evaluation over the distributers choice of generating the columns of the matrix X, and $\mathbb{E}_p$ describing the evaluation over $\mathbf{p}^{(i)}$, and the collusions choice of the symbols of the fingerprint $\mathbb{E}_{y_i}$.

Because of the scaled definitions of the mean values and regarding to [SKC08] we can directly state and prove the following two Lemmas:

Lemma 1 $\mu_{j,w} = 0$.

Proof: Starting by first computing the expectation $\mathbb{E}_{X_j}$, we have

$$\mathbb{E}_{X_j}\left[\tilde{A}_j^{(i)}\right] = \mathbb{E}_{X_j}\left[w^{(i)} \cdot A_j^{(i)}\right] = \mathbb{E}_{X_j}\left[w^{(i)}\right]\mathbb{E}_{X_j}\left[A_j^{(i)}\right] = \mathbb{E}_{X_j}\left[w^{(i)}\right] \cdot 0,$$

where $A_j^{(i)}$ represents *Skoric*'s accusation Sum, (2). Thus holds $\mathbb{E}_{wyXp}[\tilde{A}_j] = 0$. □

Lemma 2 $\mu_{c,w} = \frac{2}{\pi} \cdot \mathbb{E}[w]$.

Proof: With the help of *Skoric*'s collective accusation sum and its mean value, $\tilde{\mu} = 2/\pi$, we can quickly complete the proof:

$$\mathbb{E}_{wyXp}\left[\tilde{A}_c^{(i)}\right] = \mathbb{E}_{wyXp}\left[w^{(i)}A_c^{(i)}\right] = \mathbb{E}\left[w\right]\ \mathbb{E}_{yXp}\left[A_c^{(i)}\right] = \mathbb{E}\left[w\right] \cdot \frac{2}{\pi}.$$ □

Lemma 3 $\sigma_{j,w}^2 = \mathbb{E}[w^2]$.

Proof: $\tilde{A}_j^2$ can be described as:

$$\tilde{A}_j^2 = \sum_{i=1}^{m} \{w^{(i)}\}^2 \cdot A_j^2$$

Because of the independence of the columns of X, and by first evaluating over X_j and w, we get

$$\mathbb{E}_{wX_j}[\tilde{A}_j^2] = \mathbb{E}[w^2] \cdot m + 0.$$

From this follows $\mathbb{E}_{wyXp}[\tilde{A}_j^2] = m \cdot \mathbb{E}[w^2]$. Substituting this into the definition of $\sigma_{j,w}^2$ in equation (11) finishes the proof. □

Lemma 4 *The mean $\mu_{c,w}$ and variance $\sigma_{c,w}$ satisfy*

$$\mu_{c,w}^2 \; + \; \sigma_{c,w}^2 \; = \; \mathbb{E}[w^2] \cdot c.$$

Proof: Straight from the definition of $\sigma_{c,w}$, (12), and applying (7) we get

$$\begin{aligned}\sigma_{c,w}^2 \; &= \; m^{-1}\mathbb{E}_{wyXp}[\tilde{A}_C^2] - m\,\mu_{c,w}^2 \\ &= \; \frac{1}{m}\left(\sum_{i=1}^{m}\mathbb{E}_{wyXp}[\{\tilde{A}_C^{(i)}\}^2] + \sum_{i\neq k}\mathbb{E}_{wyXp}[\tilde{A}_C^{(i)}]\mathbb{E}_{wyXp}[\tilde{A}_C^{(k)}]\right) - m\mu_{c,w}^2. \quad (13)\end{aligned}$$

In order to receive an identity for $\mathbb{E}_{wyXp}[\{\tilde{A}_C^{(i)}\}^2]$, by making use of the column symmetry, the properties $p_1 = 1 - p_0$ and $b_1 = c - b_0$, we get

$$\{\tilde{A}_C^{(i)}\}^2 \; = w^2\big[b_1 g_1(p_1) + (c - b_1)g_0(p_1)\big]^2 \quad ,$$

where the column index i on w, y, p and b is omitted for notational simplicity. Thus it holds

$$\mathbb{E}_{wyXp}\left[\{\tilde{A}_C^{(i)}\}^2\right] = \mathbb{E}[w^2]\mathbb{E}_{yXp}\left[\frac{(b_1 - cp_1)^2}{p_1(1-p_1)}\right] = \mathbb{E}[w^2]\; c\,.$$

Now returning to equation (13), with definition (12), both elements of the second sum exactly equal $\mu_{c,w}$. Thus, the expression becomes

$$\sigma_{c,w}^2 = \frac{1}{m}\left(m\mathbb{E}_{wyXp}\left[\{\tilde{A}_C^{(i)}\}^2\right] + (m^2 - m)\mu_{c,w}^2\right) - m\mu_{c,w}^2 = \mathbb{E}[w^2]c - \mu_{c,w}^2. \qquad \square$$

In the following we will make use of the inequalities

$$1 + a < e^a < 1 + a + a^2, \quad \text{where } 0 < a \leq 1.79 \tag{14}$$

and the *Markov* inequality

$$\mathbb{P}(|X| \geq K) \leq \frac{\mathbb{E}(|X|)}{K}, \quad K > 0. \tag{15}$$

4.2 Proof of soundness

With the results of Section 4.1, we are able to derive the conditions under which soundness for the weighted accusation scheme is achieved similar to [SKC08]. According to (9) we have to determine the conditions under which $\mathbb{P}[j \in \Sigma] < \varepsilon_1$ holds true. With an auxiliary variable $\tilde{\alpha}_1$, by using (15) and as the columns of X are independent, we get

$$\mathbb{P}[j \in \Sigma] \; = \; \mathbb{P}[\tilde{A}_j > Z] \; = \; \mathbb{P}[e^{\tilde{\alpha}_1\tilde{A}_j} > e^{\tilde{\alpha}_1 Z}] \; \leq \; \frac{\mathbb{E}_{X_j}[e^{(\tilde{\alpha}_1\tilde{A}_j)}]}{e^{\tilde{\alpha}_1 Z}} = \frac{\{\mathbb{E}_{X_j}[e^{(\tilde{\alpha}_1\tilde{A}_j^{(i)})}]\}^m}{e^{\tilde{\alpha}_1 Z}}. \tag{16}$$

Now we look at $\mathbb{E}_{X_j}[e^{(\tilde{\alpha}_1 \tilde{A}_j^{(i)})}]$. By restricting $\tilde{\alpha}_1$ to $\tilde{\alpha}_1 \in (0, \tilde{\alpha}_1^{max}]$, $\tilde{\alpha}_1^{\max} = \frac{1.79}{g_1(t)}$ we can apply (14) to $\mathbb{E}_{X_j}[e^{(\tilde{\alpha}_1 \tilde{A}_j^{(i)})}]$. Together with lemmas 1 and 3 this leads to

$$\mathbb{E}_{X_j}[e^{\tilde{\alpha}_1 \tilde{A}_j^{(i)}}] \;<\; 1 \;+\; \tilde{\alpha}_1 \mathbb{E}_{X_j}[\tilde{A}_j^{(i)}] \;+\; \tilde{\alpha}_1^2 \mathbb{E}_{X_j}[\{\tilde{A}_j^{(i)}\}^2] \;<\; e^{\tilde{\alpha}_1^2 \mathbb{E}[w^2]}.$$

Substituting this into (16) we derive

$$\mathbb{P}[j \in \Sigma] \;<\; \min_{\tilde{\alpha}_1 \in (0, \tilde{\alpha}_1^{\max}]} e^{\tilde{\alpha}_1 (m \tilde{\alpha}_1 \mathbb{E}[w^2] - Z)}. \tag{17}$$

With the definitions of m and Z in (5) and using the value $\tilde{\alpha}_1^* = \frac{B}{2Ac_0\mathbb{E}[w^2]}$ which minimizes the right side of (17)we get

$$\mathbb{P}[j \in \Sigma] \;<\; \varepsilon_1^{\frac{B^2}{4A\mathbb{E}[w^2]}}.$$

As $\varepsilon_1 \in (0,1)$ this finally gives the conditions for ε_1-soundness

$$\frac{B^2}{4A\mathbb{E}[w^2]} \;\geq\; 1. \tag{18}$$

4.3 Proof of completeness

According to (10) we estimate $\mathbb{P}[C \cap \Sigma \;=\; \emptyset]$ in an appropriate way. Therefore let C be a coalition of size $c \leq c_0$ and $\tilde{\alpha}_2 > 0$ with $-\tilde{\alpha}_2 \tilde{A}_C^{(i)} \leq 1.79$ be an auxiliary variable. Again using (15) we get

$$\mathbb{P}[C \cap \Sigma = \emptyset] \leq \mathbb{P}[\tilde{A}_C \;<\; c_0 Z] < \frac{\mathbb{E}_{wyXp}\left[e^{-\tilde{\alpha}_2 \tilde{A}_C}\right]}{e^{-\tilde{\alpha}_2 c_0 Z}} = \frac{\left\{\mathbb{E}_{wyXp}\left[e^{-\tilde{\alpha}_2 \tilde{A}_C^{(i)}}\right]\right\}^m}{e^{-\tilde{\alpha}_2 c_0 Z}}.$$

Using the right inequality of Equation (14) and definition 11 we may write

$$\begin{aligned}
\mathbb{E}_{wyXp}\left[\exp\left(-\tilde{\alpha}_2 \tilde{A}_C^{(i)}\right)\right] \;&<\; 1 \;-\; \tilde{\alpha}_2 \mathbb{E}_{wyXp}\left[\tilde{A}_C^{(i)}\right] \;+\; \tilde{\alpha}_2^2 \mathbb{E}_{wyXp}\left[\left(\tilde{A}_C^{(i)}\right)^2\right] \\
&< 1 - \tilde{\alpha}_2 \mu_{c,w} + \tilde{\alpha}_2^2 (\mu_{c,w}^2 + \sigma_{c,w}^2) \\
&\leq 1 - \tilde{\alpha}_2 \mathbb{E}[w^2] \left(\frac{2}{\pi} - c_0 \tilde{\alpha}_2\right),
\end{aligned}$$

where we have made use of lemmas 2 and 4 and of the property $\mathbb{E}[w] > \mathbb{E}[w^2]$. As $-\tilde{\alpha}_2 \tilde{A}_C^{(i)} \leq 1.79$, we choose $\tilde{\alpha}_2^{max} = -1.79 \frac{g_0(t)}{c_0}$ to derive

$$\begin{aligned}
\mathbb{P}[\tilde{A}_C < c_0 Z] \;&<\; \min_{\tilde{\alpha}_2 \in (0, \tilde{\alpha}_2^{max}]} \exp\left(-\tilde{\alpha}_2 \left[m\mathbb{E}[w^2](\frac{2}{\pi} - \tilde{\alpha}_2 c_0) - c_0 Z\right]\right) \\
&=\; \exp\left(\ln(\varepsilon_1)\left(\frac{Ac_0\mathbb{E}[w^2]}{\pi^2} + \frac{c_0 B^2}{4A\mathbb{E}[w^2]} - \frac{Bc_0}{\pi}\right)\right) \\
&=\; \varepsilon_1^{\left(\frac{Ac_0\mathbb{E}[w^2]}{\pi^2} + \frac{c_0 B^2}{4A\mathbb{E}[w^2]} - \frac{Bc_0}{\pi}\right)} \;\leq\; \tilde{\alpha}_2
\end{aligned} \tag{19}$$

where we again made use of (14) and applied the minimizing value $\tilde{\alpha}_2^* = 1/(c_0\pi) - Z/(2m\mathbb{E}[w^2])$ and the definitions of m and Z. In order to get the right side of (19) bounded by ε_2 we finally get the condition for completeness,

$$B \leq \frac{2A\mathbb{E}[w^2]}{\pi} - 2\sqrt{\frac{A\mathbb{E}[w^2]}{c_0}\frac{\ln(\varepsilon_2)}{\ln(\varepsilon_1)}}. \tag{20}$$

5 Discussion

After proving the correctness of our approach, we now discuss its impact on real-world applications. The main question is if the resulting fingerprinting codes are sufficiently short to be used together with the watermarking algorithm. Of course this also depends on the length of the audio material to be protected.

Analogue to Section 6 in [SKC08], by assuming a perfectly Gaussian distribution for the collective accusation sum we are able to reduce our code length in (8) about a factor of more than two. Therewith we create a new requirement on the code length $\tilde{m}$ and a new threshold $\tilde{Z}$:

$$\tilde{m} \geq \frac{\pi^2}{2}\frac{\mathbb{E}[w^2]}{\left[\mathbb{E}(w)\right]^2}c_0^2 \ln\left(\frac{1}{\varepsilon_1\sqrt{2\pi}}\right); \quad \tilde{Z} = 2\pi\mathbb{E}[w^2]c_0 \ln\left(\frac{1}{\varepsilon_1\sqrt{2\pi}}\right).$$

An explicit example for $\tilde{m}$ with a maximum number of colluders of $c_0 = 10$ is given in Table 1. Due to our weight function (6) we estimated $\mathbb{E}[w^2]/[\mathbb{E}(w)]^2 \approx 1.083$, which is empirically computed. Closer analysis shows that an increment of the code length by a factor of only 1.083 compensates the actual value for ε_1 which otherwise would increase by a factor of 1.6.

It is not said that the choice of the weight function w has been optimal. Already directly taking the absolute value of the score as the weights may achieve a shorter code length, but as the expectation values of these weights exceed 1, the proof schemes must be adapted.

FP error probability ε_1	code length m	code length $\tilde{m}$
10^{-3}	7678	3201
10^{-4}	10237	4432
10^{-5}	12796	5662

Table 1: code length for $c_0 = 10$

Given the parameters above, we can distinguish a virtually unlimited number of customers under the assumption that only a limited number of attackers collude to attack the watermark. Using a message length of 3201-12796 message bits, resilience against up to 10 colluders can be achieved.

While the required payload is higher than the typical payloads of our algorithm (which range between 32 and 128 bit in practice), they are suited for many types of audio works:

With a typical payload of 7 bits per second, one complete fingerprint can be embedded in 8 to 30 minutes of audio, depending on the accepted false accusation rate. This means, that the approach is well suited for audio books and movie soundtracks.

6 Conclusions

In our work we proposed a fingerprinting algorithm providing required error probabilities that is collusion-secure for a maximum number of colluders $c_0 \geq 10$. Existing fingerprint coding algorithms in the literature are not able to give a well suited statement about the actual error rates when applied to real world watermarking methods. In contrast, our approach can manage this problem and it gives a reliable and trustful statement in a copyright violation charge. This is done by introducing *weights* that represent the goodness of the watermark detection. As a result, we achieve a significantly higher level of accuracy of the accusation. In our work we show that by combining our audio watermarking algorithm and the *Skoric* fingerprinting scheme, with only a slightly increment in the code length, a reliable and comparatively compact fingerprinting solution can be achieved, allowing the protection of movie soundtracks, audio books and music albums.

References

[BGML96] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. Techniques for Data Hiding. *IBM Systems Journal, MIT Media Lab*, 35(3,4):313–336, 1996.

[BS98] D. Boneh and J. Shaw. Collusion-secure fingerprinting for digital data. *IEEE Transactions on Information Theory*, 44(5):1897–1905, Sept. 1998.

[BTH96] L. Boney, A. H. Tewfik, and K. N. Hamdy. Digital Watermarks for Audio Signals. volume Proceedings of MULTIMEDIA 96, pages 473–480, June 1996.

[CFNP00] B. Chor, A. Fiat, M. Naor, and B. Pinkas. Tracing traitors. *IEEE Transactions on Information Theory*, 46(3):893–910, May 2000.

[CMB02] I. J. Cox, M. L. Miller, and J. A. Bloom. *Digital Watermarking*. Morgan Kaufmann, 2002.

[Sch09] M. Schäfer. Optimization of Fingerprinting Encoding Algorithms in the Context of Digital Audio Watermarking Methods. Master's thesis, Bergische Universität Wuppertal, December 2009.

[SKC08] Boris Skorić, Stefan Katzenbeisser, and Mehmet U. Celik. Symmetric Tardos fingerprinting codes for arbitrary alphabet sizes. *Des. Codes Cryptography*, 46(2):137–166, 2008.

[Ste03] Martin Steinebach. *Digitale Wasserzeichen fuer Audiodaten*. PhD thesis, TU Darmstadt, Germany, 2003. ISBN 3832225072.

[Tar03] G. Tardos. Optimal probabilistic fingerprinting codes. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing (STOC), pp. 116-125*, 2003.