# ACTIVE CONTENT FINGERPRINTING: SHRINKAGE AND LATTICE BASED MODULATIONS

*Farzad Farhadzadeh, Sviatoslav Voloshynovskiy, Taras Holotyak and Fokko Beekhof*

University of Geneva
Computer Science Department
7, Route de Drize, Geneva, CH-1227, Switzerland

## ABSTRACT

In this paper, we extend a new framework introduced as *active content fingerprinting* in [1] [1] that takes the best from the two worlds of content fingerprinting and digital watermarking to overcome some of the fundamental restrictions of these techniques in terms of performance and complexity. In the proposed framework, contents are modified in a way similar to watermarking to extract more robust fingerprints in contrast to conventional content fingerprinting. We investigate the performance of two modulation techniques based on unidimensional shrinkage and multidimensional lattice quantization. The simulation results on real images demonstrate the high efficiency of the proposed methods facing low-quality compression and additive noise.

***Index Terms***— Content identification, content fingerprinting, watermarking, lattice quantization/decoding.

## 1. INTRODUCTION

Content based identification (CBI) systems are facing numerous requirements related to identification accuracy, complexity, privacy, security as well as memory storage [2]. To address the trade–off between these conflicting requirements, *content fingerprints* are used [3], [4]. A content fingerprint is a short, robust and distinctive content description. The main idea behind content fingerprinting consists in the extraction of a lower dimensional representation of the content in a secret subspace, obtained by a projection to a set of secret carriers or a selection of carriers based on a secret key from a commonly used transform that spans the whole space [2], [3], [4].

In conventional content fingerprinting, the fingerprint is extracted directly from the original content and does not require any content modification that preserves the original content quality. In this sense, it can be considered as a *passive content fingerprinting* (pCFP). The extracted fingerprints resemble random codes, for which no efficient decoding algorithm is known as for structured codes. Moreover, the performance of pCFP is not satisfactory due to the high probability of error.

For these reasons, *active content fingerprinting* (aCFP) was proposed in [1], where the basic idea was introduced and a feasibility study revealed higher performance w.r.t. pCFP and digital watermarking. Albeit there are still several open issues such as an optimal modulation scheme in unidimensional case, the decoding complexity based on a bounded distance decoder (BDD) and last but not least, no extension to multidimensional case was considered.

This paper is a continuation of the work begun in [1], where the authors introduced two strategies of modulation: *Additive aCFP* (AddaCFP) and *Quantization–based aCFP* (QbaCFP). In this sequel, we introduce a new modulation scheme which has better performance in terms of distortion and error probability. In the last part of the paper, we extend our work to modulation in multidimensional space to achieve lower complexity and distortion by exploiting lattices. The reasons to exploit lattices is twofold: multidimensional lattices such as Leech-lattice [5] are well known for their low distortion quantization due to the sphere packing property. Secondly, due to the structure of lattices, there exist several low complexity quantization/decoding methods, especially for Leech-lattices [6], [7], [8]. We have investigated the bounded-distance decoder of [7]. Their implementation uses at most $519$ real operations per decoded point. Since their implementation decodes only a finite subset of the Leech lattice, we have slightly modified the implementation to approximate the decoding of the entire Leech lattice. The proposed algorithms are tested on a set of real images from the UCID database [9].

## 2. CONTENT FINGERPRINT IN SECRET SUBSPACE

Since most fingerprinting and digital watermarking systems operate in some transform domain, we define the direct and inverse transforms applied to the content $\mathbf{x} \in \mathcal{X}^N$ as:

$$\begin{cases} \tilde{x}_i = \mathbf{w}_i^T \mathbf{x},\ 1 \le i \le N, \\ \mathbf{x} = \sum_{i=1}^{N} \tilde{x}_i \mathbf{w}_i = \sum_{i \in \mathcal{K}} \tilde{x}_i \mathbf{w}_i + \sum_{i \notin \mathcal{K}} \tilde{x}_i \mathbf{w}_i, \end{cases} \quad (1)$$

The contact author is S. Voloshynovskiy (email: svolos@unige.ch).
This paper was partially supported by SNF projects 200020-134595.

[1] http://cvml.unige.ch/publications/postscript/2012/wifs_2012_acfp.pdf

where $\tilde{x}_i$ indicates the $i$-th element of the projected vector $\tilde{\mathbf{x}}$, $\mathbf{w}_i \in \mathcal{R}^N$, $1 \leq i \leq N$, are the columns of the orthogonal projection matrix $\mathbb{W} \in \mathcal{R}^{N \times N}$, $\mathbb{W} = (\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_N)^T$, and the set $\mathcal{K} = \{i_1, i_2, \cdots, i_L\}$ with cardinality $L$ represents a set of indices defined by the secret key $k$. In the part of theoretical analysis, we will assume that this transform is based on a randomized orthogonal matrix $\mathbb{W}$, i.e. a random projection (RP) transform, whose elements are equally likely $w_{i,j} = \{\pm\frac{1}{\sqrt{N}}\}$. Such a matrix can be considered as an approximate *orthoprojector*, for which $\mathbb{W}\mathbb{W}^T \approx \mathbb{I}_N$, and the basis vectors are of a unit norm [2].

In aCFP, we will consider the modification of the original content in the secret subspace defined by the secret key $k$ with the overall goal to improve the performance of identification in terms of the probabilities of bit–error and overall identification error as well as reducing complexity. For this purpose, we define a general form of aCFP as:

$$\mathbf{v} = \sum_{i \in \mathcal{K}} \varphi_i(\tilde{\mathbf{x}}^*)\mathbf{w}_i + \sum_{i \notin \mathcal{K}} \tilde{x}_i \mathbf{w}_i, \tag{2}$$

where $\mathbf{v}$ is the modified content using the inverse transform, $\tilde{\mathbf{x}}^* = \{\tilde{x}_i\}_{i \in \mathcal{K}}$ denotes the projected coefficients in the secret subspace defined by the secret key $k$, $\varphi(\tilde{\mathbf{x}}^*)$ is the modulation function applied to the vector $\tilde{\mathbf{x}}^*$ and $\varphi_i(\tilde{\mathbf{x}}^*)$ implies the $i$-th element of the modulation output.

**Definition**: $D$ is the *distortion measure per dimension* between sequences $\mathbf{x}$ and $\mathbf{v}$, defined by:

$$D = \frac{1}{N} E\left[\|\mathbf{V} - \mathbf{X}\|_2^2\right] = \frac{1}{N} E\left[\|\mathbf{S}\|_2^2\right], \tag{3}$$

where $\mathbf{S} = \sum_{i \in \mathcal{K}} \left(\varphi_i(\mathbf{X}^*) - \tilde{X}_i^*\right) \mathbf{w}_i$[2] denotes the modulation signal that can be considered as a kind of watermark by analogy to digital watermarking. In the case of pCFP, $D = 0$ while aCFP will be characterized by the distortion determined by the modulation function $\varphi(\cdot)$.

Assuming an additive noise observation channel, in the context of theoretical performance analysis:

$$\mathbf{Y} = \mathbf{V} + \mathbf{Z}, \tag{4}$$

where $\mathbf{Z}$ denotes the channel distortion, one is interested in estimating the level of degradations to the fingerprint extracted from the degraded content $\mathbf{Y}$.

Throughout the theoretical parts of the context, we assume that a content can be modelled as a Gauss-Markov process with variance $\sigma_X^2$ and evaluate the performance of all methods under the additive white Gaussian noise (AWGN) with variance $\sigma_Z^2$.

Given a secret key $k$ and the corresponding set of secret carriers, the query fingerprint extraction is performed as:

$$\mathbf{f}_\mathbf{y} = f(\tilde{\mathbf{y}}^*) = f(\varphi(\tilde{\mathbf{x}}^*) + \tilde{\mathbf{z}}^*) \tag{5}$$

[2]A scalar random variable is denoted by a capital letter $X$, its realization is denoted by the lower case letter $x \in \mathcal{X}$. As for vectors, a boldface capital letter $\mathbf{X}$ denotes a random vector $\mathbf{X} = \{X_i\}_{i=1}^N$, a boldface lower case letter $\mathbf{x}$ represents its realization $\mathbf{x} = \{x_i\}_{i=1}^N \in \mathcal{X}^N$.

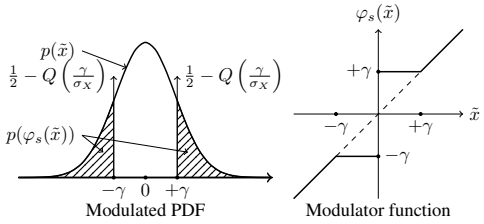


**Fig. 1**: Shrinkage based aCFP.

where $\tilde{\mathbf{z}}^*$ is a collection of projected coefficients of $\tilde{\mathbf{z}}$ in a secret subspace defined by $k$. As shown in [2], applying random projections defined in (1) on the data, which can be modelled by a Gauss-Markov process, makes projected coefficients uncorrelated. Consequently, one can assume that projected coefficients in the secret subspace follow i.i.d. Gaussian distributions, i.e., $\tilde{\mathbf{Z}}^* \sim \mathcal{N}(\mathbf{0}, \sigma_Z^2 \mathbf{I}_L)$ and $\tilde{\mathbf{X}}^* \sim \mathcal{N}(\mathbf{0}, \sigma_X^2 \mathbf{I}_L)$, where $\mathcal{N}(\mu, \sigma^2)$ stands for the Gaussian distribution with mean $\mu$ and variance $\sigma^2$.

The performance metric of CBI is defined by the probability of correct identification $P_{ci}$ based on the bounded distance decoder (BDD):

$$P_{ci} = \sum_{m=1}^{M} \Pr\{d(\mathbf{F}_\mathbf{y}, \mathbf{f}_\mathbf{x}(m)) \leq \theta L \bigcap_{m' \neq m} d(\mathbf{F}_\mathbf{y}, \mathbf{f}_\mathbf{x}(m')) > \theta L | \mathcal{H}_m\} \Pr\{\mathcal{H}_m\}, \tag{6}$$

where $\theta \geq 0$ is a threshold and $L$ is the length of fingerprint, $\mathcal{H}_m$ corresponds to the case that $\mathbf{F}_\mathbf{y}$ is related to the $m^{\text{th}}$ entry of the database, $d(\cdot, \cdot)$ denotes a decoding metric, and we assume that all entries will be queried with the same probability, i.e., $\forall m, \Pr\{\mathcal{H}_m\} = \frac{1}{M}$.

### 2.1. Unidimensional case: Shrinkage based aCFP

To trade–off between the modulation distortion and the bit error rate (BER) along with AddaCFP and QbaCFP introduced in [1], we introduce a new modulation scheme based on shrinking.

**Definition**: *Shrinkage based active content fingerprinting* (SbaCFP) is defined by the scalar modulation function of the form (Fig. 1):

$$\varphi_s(\tilde{x}_i^*) = \begin{cases} \gamma \operatorname{sign}(\tilde{x}_i^*), |\tilde{x}_i^*| \leq \gamma, \\ \tilde{x}_i^* \qquad\qquad , |\tilde{x}_i^*| > \gamma, \end{cases} \tag{7}$$

where $\tilde{x}_i^*$ is the $i$-th element of $\tilde{\mathbf{x}}^*$, and $\gamma \geq 0$. The distortion of SbaCFP per content sample is:

$$D_s = \frac{1}{N} E\left[\|\mathbf{S}_s\|_2^2\right] = 2\frac{L}{N} \int_0^\gamma (\gamma - t)^2 p_{\tilde{X}^*}(t) \mathrm{d}t \tag{8}$$

where $p_{\tilde{X}^*} = \mathcal{N}(0, \sigma_X^2)$. In this scheme, the fingerprint extractor function is just the sign function: $\psi(t) = \operatorname{sign}(t)$. The fingerprint is then calculated during enrollment as:

$$f_{x_i} = \psi(\varphi_s(\tilde{x}_i^*)) = \text{sign}(\varphi_s(\tilde{x}_i^*)),\ i \in \mathcal{K}.$$

The fingerprint computed at the identification stage is:

$$f_{y_i} = \psi(\tilde{y}_i^*) = \text{sign}(\tilde{y}_i^*) = \text{sign}(\varphi_s(\tilde{y}_i^*) + \tilde{z}_i),\ i \in \mathcal{K},$$

where $\tilde{y}_i^*$ similar to $\tilde{x}_i^*$ is a projection coefficient in the secret subspace defined by $k$. The performance of SbaCFP is determined by the BER and is given by:

$$P_{b-\text{SbaCFP}} = \Pr\{\text{sign}(\tilde{X}_i^*) \neq \text{sign}(\tilde{Y}_i^*)\} = E\left[Q\left(\frac{|\varphi_s(\tilde{X}^*)|}{\sigma_Z}\right)\right]$$
$$= 2\int_0^{\gamma} Q\left(\frac{\gamma}{\sigma_Z}\right) p_{\tilde{X}^*}(t)\,\mathrm{d}t + 2\int_{\gamma}^{\infty} Q\left(\frac{t}{\sigma_Z}\right) p_{\tilde{X}^*}(t)\,\mathrm{d}t$$
$$= 2Q\left(\frac{\gamma}{\sigma_Z}\right)\left[\frac{1}{2} - Q\left(\frac{\gamma}{\sigma_x}\right)\right] + 2\int_{\gamma}^{\infty} Q\left(\frac{t}{\sigma_Z}\right) p_{\tilde{X}^*}(t)\,\mathrm{d}t. \tag{9}$$

Finally, the probability of correct identification in the CBI using SbaCFP $P_{ci-\text{SbaCFP}}$ based on the BDD is given by:

$$P_{ci-\text{SbaCFP}} = \frac{1}{M}\sum_{m=1}^{M} \Pr\left\{ d_H(\mathbf{f_x}(m), \mathbf{F_y}) \leq \theta L \right.$$
$$\left. \bigcap_{m' \neq m} d_H(\mathbf{f_x}(m'), \mathbf{F_y}) > \theta L \middle| \mathcal{H}_m \right\}$$
$$\overset{(a)}{=} \sum_{d=0}^{\theta L} \binom{L}{d} \epsilon^d (1-\epsilon)^{L-d} \left[\frac{1}{2^L}\sum_{j=d+1}^{L}\binom{L}{j}\right]^{M-1},$$

where $d_H(\cdot,\cdot)$ denotes the Hamming distance, $\epsilon = P_{b-\text{SbaCFP}}$ is the cross-over probability of the binary symmetric channel between $\mathbf{f_x}(m)$ and $\mathbf{f_y}$ under $\mathcal{H}_m$, $(a)$ follows from the fact that $d_H$ follows $\mathcal{B}(L,\epsilon)$ under $\mathcal{H}_m$, and follows $\mathcal{B}(L, 0.5)$ for other contents. $\mathcal{B}(L,\epsilon)$ denotes a binomial distribution with $L$ trials and probability of success $\epsilon$.

**Remark 1.** For the case that $\theta = 0$, the correct identification occurs when there is an exact match between $\mathbf{f_y}$ and $\mathbf{f_x}(m)$ under $\mathcal{H}_m$. The probability of correct identification is $P_{ci-\text{SbaCFP}} = (1-\epsilon)^L$. Such a decoder corresponds to crypto-like hash matching under the assumption of errorless fingerprinting.

Therefore, the overall goal of a aCFP is to reduce BER to such a level that ensures high $P_{ci}$ without a need of complex fingerprint matching. Table 1 shows BERs for different aCFP schemes and the lower bound (LB) in digital watermarking (DWM) [1]. Fig. 2 compares the BER rate in SbaCFP with other modulations AddaCFP, QbaCFP and LB in watermarking for a fixed Document to Watermark ratio (DWR), DWR $= 10\log_{10}\frac{\sigma_X^2}{D}$ and Document to Noise ratios (DNRs), DNR$= 10\log_{10}\frac{\sigma_X^2}{\sigma_Z^2}$, in a range of $[0, 25]$ dB.

### 2.2. Multidimensional case: Lattice based aCFP

Moreover, to achieve lower decoding complexity and distortion, we extend our analysis to lattice based quantization as a vector modulation function.

**Table 1**: BERs in pCFP and aCFP methods versus lower bound(LB) in DWM.

| | Technique | Distortion $D$ | Probability $P_b$ |
|---|---|---|---|
| DWM | Lower bound (LB) | $\frac{L}{N}\alpha^2$ | $Q\left(\frac{\alpha}{\sigma_Z}\right)$ |
| Fingerprinting | pCFP | 0 | $\frac{1}{\pi}\arctan\left(\frac{\sigma_Z}{\sigma_X}\right)$ |
| | AddaCFP | $\frac{L}{N}\alpha^2$ | $\mathrm{E}\left[Q\left(\frac{\lvert\tilde{X}^*\rvert+\alpha}{\sigma_Z}\right)\right]$ |
| | QbaCFP | $\frac{L}{N}\alpha^2$ | $Q\left(\frac{\eta}{\sigma_Z}\right)$ |
| | SbaCFP | equation (8) | equation (9) |

where $\alpha > 0$ and $\eta = \sigma_X\sqrt{\frac{2}{\pi}}\left(1+\sqrt{1+\frac{\pi}{2}\left(\frac{\alpha^2}{\sigma_X^2}-1\right)}\right)$ [1].

**Definition**: *Lattice based active content fingerprinting* (LbaCFP) is defined by the vector modulation function of the form:

$$\varphi_\Lambda(\tilde{\mathbf{x}}^*) = Q_\Lambda(\tilde{\mathbf{x}}^* + \mathbf{n}) - \mathbf{n}, \tag{10}$$

where $Q_\Lambda(\cdot)$ is the lattice based quantization using the lattice $\Lambda \subset \mathcal{R}^L$ with the generator matrix $\mathbf{G}$ and the fundamental Voronoi region $\mathcal{V}$, and $\mathbf{n}$ is the dither [3], which is Nyquist-$\mathbf{G}$, i.e., $\Phi_{\mathbf{N}}(\mathbf{Ht}) = \delta(\mathbf{t})$, where $\mathbf{H} = 2\pi\mathbf{G}^{-T}$ and $\Phi_{\mathbf{N}}(\cdot)$ is the characteristic function of random vector $\mathbf{N}$ [10].

The distortion of LbaCFP per content sample is:

$$D_\Lambda = \frac{1}{N}E\left[\|\mathbf{S}_\Lambda\|_2^2\right] = \frac{1}{N}E\left[\sum_{i\in\mathcal{K}}(\varphi_{\Lambda_i}(\tilde{\mathbf{X}}^*) - \tilde{X}_i)^2\right]$$
$$= \frac{1}{N}E\left[\sum_{i\in\mathcal{K}} e_i^2\right] = \frac{1}{N}E\left[\|\mathbf{e}\|^2\right] \overset{(a)}{=} \frac{L}{N}G(\Lambda,\mathcal{V})V^{2/L},$$

where $(a)$ follows from the fact that the error vector $\mathbf{e}$ is uniformly distributed over $\mathcal{V}$ [10] and $G(\Lambda,\mathcal{V})$ is the normalized second moment of the lattice $\Lambda$ with the Voronoi region $\mathcal{V}$ and $V = \det(\mathbf{G})$ is the volume of $\mathcal{V}$.

In this scheme, the fingerprint extractor function is the identity function, i.e., $\psi(x) = x$. The fingerprint at the enrollment stage is:

$$\mathbf{f_x} = \psi(\varphi_\Lambda(\tilde{\mathbf{x}}^*)) = \varphi_\Lambda(\tilde{\mathbf{x}}^*).$$

The fingerprint computed at the identification stage is:

$$\mathbf{f_y} = \psi(\varphi_\Lambda(\tilde{\mathbf{y}}^*)) = \varphi_\Lambda(\tilde{\mathbf{y}}^*) = \varphi_\Lambda(\mathbf{f_x} + \tilde{\mathbf{z}}^*),$$

where $\tilde{\mathbf{z}}^*$ is a collection of projected coefficients of $\tilde{\mathbf{z}}$ in a secret subspace defined by $k$ and $\tilde{\mathbf{Z}}^* \sim \mathcal{N}(\mathbf{0}, \sigma_Z^2\mathbf{I}_L)$ [2]. Consequently, one can consider the lattice quantizer as a decoder under AWGN.

The performance of the CBI using LbaCFP can be upper bounded for $P_{ci}$ as follows, for any $\gamma_{\text{eff}} \leq \sigma_Z^2$:

[3] The dither can be key-dependent.

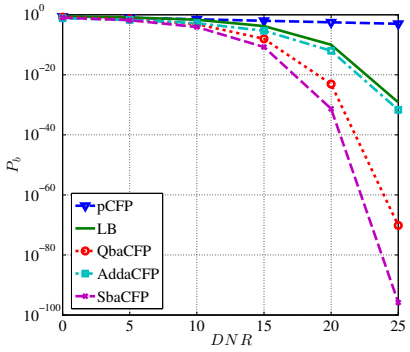


**Fig. 2**: Comparison of different aCFP scheme and Lower Bound (LB) in DWM, with $DWR = 22dB$, $N = 2048$ and $L = 32$.

$$
\begin{aligned}
P_{ci} &= \sum_{m=1}^{M} \Pr\left\{ \sum_{\tilde{\mathbf{y}}^* \in \mathcal{V}(\mathbf{f_x}(m))} p(\tilde{\mathbf{y}}^* | \mathbf{f_x}(m)) \middle| \mathcal{H}_m \right\} \Pr\{\mathcal{H}_m\} \\
&\overset{(a)}{\leq} \frac{1}{M} \sum_{m=1}^{M} \Pr\{\|\mathbf{f_x}(m) - \tilde{\mathbf{Y}}^*\|_2^2 \leq \gamma_{\text{eff}} L | \mathcal{H}_m\} \\
&\overset{(b)}{=} \Pr\{\|\mathbf{f_x}(1) - \mathbf{F_y}\|_2^2 \leq \gamma_{\text{eff}} L | \mathcal{H}_1\} \\
&\overset{(c)}{\leq} \exp\left( -L \left( \frac{\gamma_{\text{eff}}}{2\sigma_Z^2} - 0.5 \ln \frac{\gamma_{\text{eff}} e}{\sigma_Z^2} \right) \right),
\end{aligned}
$$

where $\gamma_{\text{eff}} L$ is the radius of a sphere that has the same volume as the Voronoi region $\mathcal{V}$, $(a)$ holds since the value of the probability density of the AWGN at any point of a sphere of radius $r$ is larger than it is at any point outside of the sphere, $(b)$ follows due to the assumption that $\mathbf{f_x}(i) \neq \mathbf{f_x}(j)$ for all $i \neq j$ and all the Veronoi regions have the same geometry, and $(c)$ follows from the Cramer-Chernoff bound [11].

## 3. NUMERICAL EVALUATION

In this section, we evaluate the performance of CBI using UCID database [9], consisting of 1338 image of size 384 by 512. To extract feature vector from each image, an image is converted to gray scale and divided in 16 by 16 blocks and the 2D DCT of each block is computed. The feature vector is constructed by concatenating the DCT coefficients at the coordinates $(1, 2)$ inside each block [2] resulting in a vector of length $N = 768$. Finally, the fingerprint of length $L$ from each feature vector is extracted by using RP followed by different modulation approaches considered in Section 2. Table 2 shows the parameters of the modulation schemes and their average embedding distortion over all images in UCID based on Peak Signal to Distortion Ratio (PSDR$= 10\log_{10}(\frac{255^2}{D})$) and the average of the mean structural similarity index (MSSIM) [12] to quantitatively evaluate the imperceptibility of the modulations. In order to have a fair comparison between the performance of the modulators in terms of memory storage, embedding rate, and complexity, we investigate their performance for $L = 24$ in LbaCFP (Leech Lattice dimension) and corresponding $L = 192$ in SbaCFP, and we set $\theta = \frac{2}{192}$ for BDD used in SbaCFP to have approximately the same decoding complexity w.r.t. Leech Lattice BDD. Moreover, to evaluate the performance of SbaCFP in low embedding rate, we show also its performance for $L = 24$ and $\theta = 0$. We evaluate the ability of the identification system to correctly identify an image after it has undergone the potential malicious attacks listed in Table 3.

The unidimensional SbaCFP demonstrates remarkable performance for low-rate case ($L = 24$), while for $L = 192$, which corresponds to $L = 24$ in the LbaCFP, the lattice scheme outperforms the unidimensional counterpart. The performance of SbaCFP can be improved by increasing $\theta$. However, it would require higher decoding complexity.

**Table 2**: Different modulation schemes.

| Modulators | Parameters | PSDR | MSSIM |
|---|---|---|---|
| SbaCFP | $L = 192, \gamma = 60$ | 53 dB | 0.999 |
| | $L = 24, \gamma = 125$ | 53 dB | 0.999 |
| LbaCFP | scale$= 70, L = 24$ | 53 dB | 0.999 |

**Table 3**: List of attacks tested and the corresponding probability of correct identification, real $\hat{P}_b$ and predicted $P_b$ BERs.

| Modulators | Attack | Parameters | Performance | | |
|---|---|---|---|---|---|
| | | | $P_{ci}$ | $\hat{P}_b$ | $P_b$ |
| SbaCFP $L = 192$ $\theta = 2/L$ $\gamma = 60$ | AWGN PSNR | 30 dB | 1 | 0 | 0 |
| | | 25 dB | 1 | 0 | 0 |
| | | 20 dB | 0.97 | 0.003 | 0.0026 |
| | | 15 dB | 0.17 | 0.035 | 0.03 |
| | JPEG QF | 40 | 1 | 0 | 0 |
| | | 25 | 1 | 0 | 0 |
| | | 5 | 0.13 | 0.028 | 0.02 |
| LbaCFP | AWGN PSNR | 30 dB | 1 | | |
| | | 25 dB | 1 | | |
| | | 20 dB | 1 | | |
| | | 15 dB | 0.83 | | |
| | JPEG QF | 40 | 1 | | |
| | | 25 | 1 | | |
| | | 5 | 0.95 | | |
| SbaCFP $L = 24$ $\theta = 0$ $\gamma = 125$ | AWGN PSNR | 30 dB | 1 | 0 | 0 |
| | | 25 dB | 1 | 0 | 0 |
| | | 20 dB | 1 | 0 | 0 |
| | | 15 dB | 0.95 | 0.002 | 0.0018 |
| | JPEG QF | 40 | 1 | 0 | 0 |
| | | 25 | 1 | 0 | 0 |
| | | 5 | 0.97 | 0.001 | 0.0006 |

# Conclusions

In this paper, we study the performance-complexity tradeoff in content identification based on aCFP. Both proposed schemes remarkably outperforms QIM. The lattice also offers low identification complexity for broad range of applied distortions. While the unidimensional SbaCFP is well suited for the moderate distortions using low complexity BDD or even direct hash based matching.

## 4. REFERENCES


[1] S. Voloshynovskiy, F. Farhadzadeh, O. Koval, and T. Holotyak, "Active content fingerprinting: a marriage of digital watermarking and content fingerprinting," in *IEEE International Workshop on Information Forensics and Security*, Tenerife , Spain, December 2-5 2012.

[2] F. Farhadzadeh, S. Voloshynovskiy, and O. Koval, "Performance analysis of content-based identification using constrained list-based decoding," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 5, pp. 1652 –1667, oct. 2012.

[3] J. Fridrich, "Robust bit extraction from images," in *MCS*, july 1999, vol. 2, pp. 536 –540.

[4] J. Haitsma and T. Kalker, "A highly robust audio fingerprinting system.," in *ICM Information Retrieval,*, 2002.

[5] J. Leech, "Notes on sphere packings," *Canadian Journal of Mathematics*, 1967.

[6] O. Amrani, Y. Be'ery, A. Vardy, Feng-Wen Sun, and H.C.A. van Tilborg, "The leech lattice and the golay code: bounded-distance decoding and multilevel constructions," *Information Theory, IEEE Transactions on*, vol. 40, no. 4, pp. 1030 –1043, jul 1994.

[7] O. Amrani and Y. Beery, "Efficient bounded-distance decoding of the hexacode and associated decoders for the leech lattice and the golay code," *Communications, IEEE Transactions on*, vol. 44, no. 5, pp. 534 –537, may 1996.

[8] A. Vardy, "Even more efficient bounded-distance decoding of the hexacode, the golay code, and the leech lattice," *Information Theory, IEEE Transactions on*, vol. 41, no. 5, pp. 1495 –1499, sep 1995.

[9] G. Schaefer and M. Stich, "Ucid - an uncompressed colour image database," in *Storage and Retrieval Methods and Applications for Multimedia*, 2004, Proc.of SPIE.

[10] A. Kirac and P.P. Vaidyanathan, "Results on lattice vector quantization with dithering," *Circuits and Systems II: Analog and Digital Signal Processing, IEEE Transactions on*, vol. 43, no. 12, pp. 811 –826, dec 1996.

[11] G. Poltyrev, "Bounds on the decoding error probability of binary linear codes via their spectra," *Information Theory, IEEE Transactions on*, vol. 40, no. 4, pp. 1284 –1292, jul 1994.

[12] Z. Wang, A.C. Bovik, H.R. Sheikh, and E.P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *Image Processing, IEEE Transactions on*, vol. 13, no. 4, pp. 600 –612, april 2004.