# ANTI-COLLUSION FINGERPRINTING WITH SCALAR COSTA SCHEME (SCS) AND COLLUDER WEIGHT RECOVERY

Byung-Ho Cha and C.-C. Jay Kuo
Ming Hsieh Department of Electrical Engineering and Signal and Image Processing Institute
University of Southern California, Los Angeles, CA 90089-2564
E-mail: byungcha@usc.edu, cckuo@sipi.usc.edu

***Abstract*— An anti-collusion fingerprinting system is developed to protect media files against time-varying collusion attacks based on the scalar Costa scheme (SCS) and colluder weight recovery. We treat the host signal as a parallel Gaussian channel and fingerprints as transmitted user signals. We decompose the Gaussian channel into multiple independent subchannels, and assign different user messages to different subchannels. Then, colluder weights in collusion attacks can be estimated using pilot symbols at the decoder, and all weights can be estimated and compensated. As a result, the decoding region on the parametric space can be recovered as an original format. It is shown by experimental results that the proposed fingerprinting system has excellent performance in colluder detection.**

***Index Terms*— scalar Costa scheme, colluder weight estimation, colluder weight recovery, minimum distance decoding, multimedia fingerprinting**

## I. INTRODUCTION

Fingerprinting is a traitor tracing technique that can be used to identify colluders on multi-cast networks. It is a challenging task for a fingerprinting system to allow high user capacity and good detection capability in the presence of a large number of colluders. Typically, we need many embedding bits to support a large number of users and colluders, and these bits should be designed, embedded and detected systematically.

To achieve this goal, the authors developed a fingerprinting system in [1], [2], which is analogous to a multi-carrier code-division-multi-access (MC-CDMA) communication system with orthogonal spreading codes. An alternative to the CDMA-based embedding method is the quantization index modulation (QIM) [3]. Swaminathan *et al.* [4] explored the possibility of employing QIM for anti-collusion fingerprinting applications, where QIM with dither modulation (DM) or spread transform dither modulation (STDM) was studied. However, its performance was not as good as that of the spread spectrum (SS) method.

In this work, we propose a new framework to design anti-collusion fingerprinting systems based on the scalar Costa scheme (SCS) and colluder weight recovery. This formulates the collusion attack as a parallel Gaussian channel (PGC) where user fingerprints are assigned to consecutive sample groups through user assignment (UA). Then, colluder weights in the collusion attacks are estimated through pilot-assisted colluder weight estimation (PACWE) at the decoder, and all weights are estimated and compensated. This recovery structure regenerates transmitted user messages with an excellent capability in colluder detection and overcomes the limitations of minimum distance decoding. The new fingerprinting system has two main advantages. First, it is robust against time-varying collusion attacks. Second, it offers high colluder capacity (*i.e.*, a higher number of identified colluders).

The rest of this paper is organized as follows. The model of the information embedding and decoding system is provided in Sec. II. The fingerprinting system based on SCS is described in Sec. III. Then, the PACWE module and the corresponding recovery structure at the decoder are presented in Sec. IV. Experimental results are shown in Sec. V. Concluding remarks and future research directions are described in Sec. VI.

## II. SYSTEM MODEL

The information embedding and detection system is shown by Fig. 1. The host signal is represented by a vector, $\mathbf{x} \in \Re^T$. We desire embed message $m$ in $\mathbf{x}$. The embedding function maps host signal $\mathbf{x}$ and message $m$ to composite signal $\mathbf{y}$, $\mathbf{y} \in \Re^T$, via

$$\mathbf{y} = f(\mathbf{x};\ m) \tag{1}$$

where $f(\cdot)$ is an embedding function subject to a distortion constraint. Here, we do not consider a secret key for embedding. The distortion between $\mathbf{x}$ and $\mathbf{y}$ is denoted by $\varepsilon(\mathbf{x},\ \mathbf{y})$, which can be measured by

$$\varepsilon(\mathbf{x},\ \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|^2 \tag{2}$$

where $\|\cdot\|^2$ denotes a squared distance.

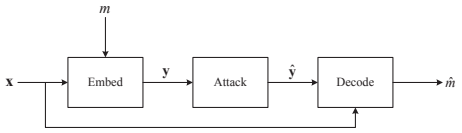


Fig. 1. Model of information embedding and decoding.

The input to the attack module is given by $\mathbf{y}$, which can be viewed as a channel using the analogy of a communication system. The attack channel modifies input $\mathbf{y}$ to generate a new output, $\hat{\mathbf{y}} \in \Re^T$. Here, it is assumed that the dimension of the signal vector is not changed after the attack and the synchronization between the embedder and the decoder is well arranged. The decoder extracts message $\hat{m}$, which is called the estimate of the embedded message from output $\hat{\mathbf{y}}$. It is also assumed that the original host signal, $\mathbf{x}$, is available in the decoder, which is reasonable in the fingerprinting application [5]. Then, by using the minimum distance decoding criterion, one can obtain the estimate of the embedded message as

$$\hat{m} = g(\hat{\mathbf{y}};\ \mathbf{x}) = \arg\min_{m} \|\hat{\mathbf{y}} - \mathbf{y}(\mathbf{x};\ m)\| \tag{3}$$

where $g(\cdot)$ is the decoding function, and $\|\cdot\|$ is a distance between two vectors.

## III. Proposed Fingerprinting System

A theoretical embedding method with the Gaussian source was proposed by Costa [6], which can be used for communications with the side information at the encoder. More recently, in order to implement this theoretical result in practical systems, a distortion-compensated dither modulation (DC-DM) method with the scalar uniform quantizer [3] or the scalar Costa scheme (SCS) [7], [8] was investigated by researchers. In this section, we will study the design of a new family of fingerprints based on ideas along this line.

The overall structure of the proposed fingerprinting system is shown in Fig. 2. It consists of five modules: 1) user ID $u_l$ generation, 2) message $m_l$ embedding using dither vector $\mathbf{d}_l$, 3) user assignment, 4) time-varying collusion attacks denoted by $A(\hat{\mathbf{Y}}|\mathbf{Y})$, and 5) minimum distance decoding and colluder identification. We will discuss modules 2 - 5 in detail below.

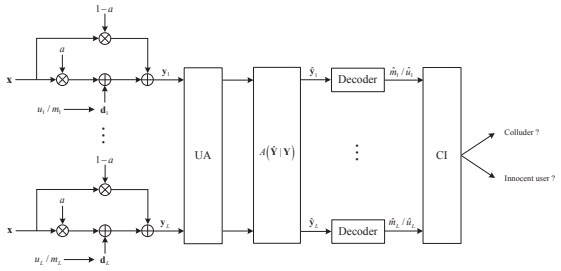


Fig. 2. The proposed fingerprinting system.

### A. Distortion-Constrained Scalar Embedding

Suppose that user $l$ transmit ID $u_l$ of length $U$ for the identification purpose, and the user ID, $u_l$, is mapped to user message $m_l$ of length $M$. Given a sample of host signal $\mathbf{x}$, a scalar Costa embedding function is defined as

$$\mathbf{y}_l = \begin{cases} Q_0\left(a\mathbf{x};\ m_l\right) + (1-a)\mathbf{x}: & m_l = 0 \\ Q_1\left(a\mathbf{x};\ m_l\right) + (1-a)\mathbf{x}: & m_l = 1 \end{cases} \tag{4}$$

where

$$Q_c\left(\mathbf{x}\right) = Q\left(\mathbf{x} + \mathbf{d}_{l,c}\right) - \mathbf{d}_{l,c}, \quad c = 0,\ 1$$

and where $Q\left(\mathbf{x}\right) = \Delta \left\lfloor \mathbf{x}/\Delta \right\rfloor$ ($\Delta$ denotes a step size), $\mathbf{d}_{l,c}$ is a dither vector of length $N_d$ for user $l$, parameter $a \in [0,\ 1]$ is used to compensate the distortion introduced by quantizer. The absolute value of vector $\mathbf{d}_{l,c}$ is usually set to $\Delta/4a$. If $a = 0$, then $\mathbf{y}_l = \mathbf{x}$, which means that no messages are embedded. If $a = 1$, Eq. (4) reduces to the dither modulation (DM) method.

### B. User Assignment

We would like to distribute multimedia files over a network via multi-cast using a fingerprinting technique. It is assumed that the maximum number of users supported by the system is $L$. To achieve this goal, we adopt the user assignment (UA) scheme, which is analogous to wireless multiple-access communication system [9]. Specifically, the fingerprinting system divides samples into $L$ consecutive independent sample-groups and assigns each sample group to one of $L$ users as shown in Fig. 3. Furthermore, each user can have its own pilot symbols for pilot-assisted colluder weight estimation (PACWE). Details will be given in Sec. IV.

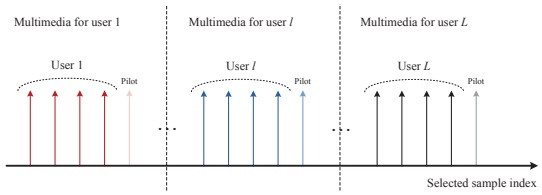


Fig. 3. Illustration of selected sample assignment to different users in the proposed fingerprinting system.

### C. Time-Varying Collusion Attack

We can divide users into two groups: malicious users (or colluders) and innocent users. We use $\Phi$ to denote the set of all users and $\Omega$ the set of colluders. Clearly, $\Omega$ is a subset in $\Phi$. Without loss of generality, we assume that there are $L$ users and $K$ colluders in the system. That is, $|\Phi| = L$ and $|\Omega| = K$. A time-varying collusion attack from $K$ colluders in a set $\Omega$ can be expressed as

$$\hat{y}(i) = \sum_{k \in \Omega} h_k(i) y_k(i) + e(i) \tag{5}$$

where $y_k(i) \in \mathbf{y}_k$ is the host signal for colluder $k$, $h_k(i)$ is the time-varying weight for colluder $k$, $e(i)$ is additive noise and $\hat{y}(i) \in \hat{\mathbf{y}}$ is the colluded signal on $i$th sample. The weights always need to satisfy

$$\sum_{k \in \Omega} h_k(i) = 1 \tag{6}$$

where $h_k(i) \neq 0$ for all $i$. Furthermore, colluders can change their colluder weights sample-by-sample in the same media without the knowledge of embedding and detection algorithms

$$h_k(r; q), \quad r = 0,\ \cdots,\ R(q) - 1 \quad \text{and} \quad q = 1, \cdots, Q \tag{7}$$

where $R(q)$ denotes the number of samples in one segment (which can vary segment-by-segment) and $Q$ represents the number of segments in a media file. Inside one segment, we assume that colluder weights are highly correlated. Thus, the duration of $R(q)$ can represent the coherence time of a collusion attack.

### D. Minimum Distance Decoding and Colluder Identification

We introduce a two-stage colluder identification method: 1) minimum distance decoding and 2) colluder identification. In the first stage, we decode message $\hat{m}_l$ from received attacked signal $\hat{\mathbf{y}}_l$. By applying the minimum distance decoding, we get

$$\hat{m}_l = \arg\min_{m_l} \|a\hat{\mathbf{y}} - \mathbf{y}_l(a\mathbf{x};\ m_l)\| \tag{8}$$

where decoded message $\hat{m}_l$ is mapped to an estimate of user ID $\hat{u}_l$. To identify colluders, we use a binary decision rule that a given criterion satisfies or not in the second stage. The probability function, $\Pr[\hat{u}_k \neq u_k]$ for colluder $k$ can be used as a metric to measure the robustness against time-varying collusion attacks. Mathematically, we can identify a colluder using the following criterion:

$$P_{avg} = \frac{1}{U} \sum_{i=0}^{U-1} \Pr[\hat{u}_k \neq u_k] \tag{9}$$

and

$$\sup P_{avg} \left( A(\hat{\mathbf{Y}}|\mathbf{Y}) \right) \rightarrow 0$$

where sup represents the supremum via the maximum of all possible collusion attack combinations. If Eq. (9) and the above condition hold, user $k$ is identified as a colluder. One critical requirement in the fingerprinting application is not to accuse innocent users as colluders (*i.e.*, the false alarm of innocent users must be extremely small). Thus, it is typical to allow a slightly higher miss rate to yield an extremely low false alarm rate.

## IV. Colluder Weight Estimation and Recovery

Time-varying collusion attacks can be represented as a parallel Gaussian channel (PGC) [10], [11] under the proposed fingerprinting scheme as described in Sec. III. When colluder $k \in \Omega$ chooses its weight $h_k(i)$ and noise term $e_k(i)$, its output can be written as

$$\hat{y}_k(i) = h_k(i) y_k(i) + e_k(i), \quad k \in \Omega. \tag{10}$$

Here, we would like to recover colluder weights $h_k(i),\ k \in \Omega$, from Eq. (10). The colluder weight $h_k(i)$ can be estimated in the same manner as the uplink of wireless multiuser communication. The decoder should have some knowledge of the channel to apply advanced symbol detection techniques. In practice, the channel state information (CSI) is obtained by channel estimation techniques. Once the decoder knows colluder weights, the collusion effect can be properly compensated [7], [12].

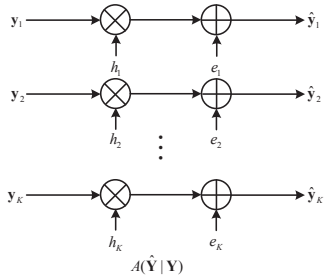


Fig. 4. Illustration of a parallel Gaussian channel.

There exist many channel estimation techniques [13], and one of them is the use of pilot symbols [14]. Based on this idea, we develop a pilot-assisted colluder weight estimation (PACWE) scheme below. The estimated colluder weight can be written as

$$\hat{h}_k(i) = \frac{\hat{y}(i) - x(i)}{P_{P,k}} \tag{11}$$

where $P_{P,k}$ is the power of the pilot symbol for colluder $k$. Using estimate $\hat{h}_k(i)$ obtained from Eq. (11), the recovery structure is given by

$$\hat{y}_R(i) = \frac{1}{\hat{h}_k(i)} \left[ \hat{y}(i) - \left( 1 - \hat{h}_k(i) \right) x(i) \right] \tag{12}$$

where $\hat{y}(i)$ is obtained from Eq. (8). Note that the condition of $\hat{h}_k(i) \neq 0$ is implied by the time-varying collusion attack as shown in Eq. (5).

## V. Experimental Results

The performance of the proposed fingerprinting system against time-variant collusion attacks is evaluated in this section. We use the number of identified colluders as the performance metric. The host signal is randomly generated with integer values from 0 to 255 for each sample. Parameter $a$ is equal to one (*i.e.*, without compensation), step size $\Delta$ is set to 8, the length of the dither vector is $N_d = 4$, the length of user message is $M = 32$ and the total length of a user fingerprint is $T = MN_d = 128$ for every user. $L = 256$ users are supported. Weights in the collusion attack are generated randomly using a Gaussian distribution with the zero mean. Also, we demand that the fingerprinting system does not accuse any innocent user as the colluder. Experimental results are obtained using $10^4$ simulation runs.

We compare the performance of the following three schemes in Fig. 5:

1) the spread transform dither modulation (STDM) fingerprinting scheme in [4] with orthogonal spreading vector support, *i.e.*, all users share the same sample positions by different spreading vectors with length $N_s = 256$, (indicated by the triangle and dashed dot line);
2) the proposed fingerprinting scheme with user assignment by multiplexing only (square and dashed line);
3) the proposed fingerprinting scheme with both user assignment and colluder weights recovery (circle and solid line).

Note that no user assignment and colluder weight recovery is used in STDM (Scheme 1). Scheme 1 gives the worst performance while scheme 3 catches all colluders without accusing innocent users. We see from this example that the colluder weight recovery process at the decoder is very useful in improving the colluder detection rate.

The strength of a collusion attack can be characterized by the fingerprint-to-noise ratio (FNR), which is defined by

$$\zeta = 10 \log_{10} \left( \frac{P_{F,k}}{P_{E,k}} \right) \tag{13}$$

where $P_{F,k}$ is the power of the fingerprint and $P_{E,k}$ is the noise power of colluder $k$. Fig. 6 shows the performance of PACWE parameterized by the FNR value (10, 20, 30 dB and no noise), where the y-axis is the number of identified colluders while the x-axis is the number of colluders involved in the collusion

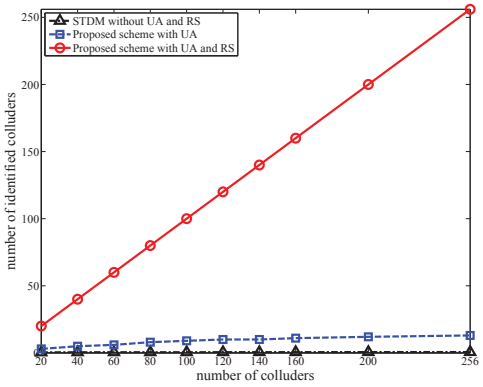


Fig. 5. Performance comparison of three schemes: (1) STDM fingerprinting (2) proposed fingerprinting with user assignment, and (3) proposed fingerprinting with user assignment and colluder weight recovery.

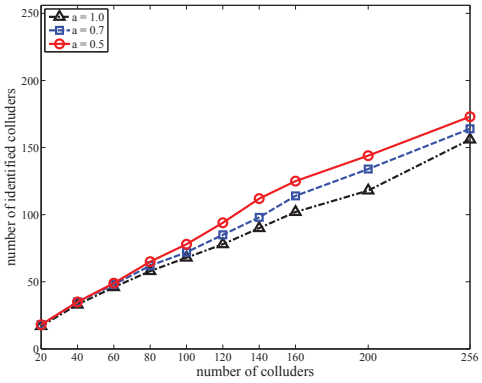


Fig. 7. Comparison of colluder identification performance with respect to the distortion compensation parameter $a$ (1.0, 0.7, and 0.5) with FNR equal to 20 dB.

attack. In the implementation, we apply a pilot symbol of length $N_p = 1$ for each user so that the total length of the user fingerprint is $T = 129$. As shown in the figure, we can identify all colluders when there is no noise. As noise strength becomes larger, the colluder identification performance drops gradually.

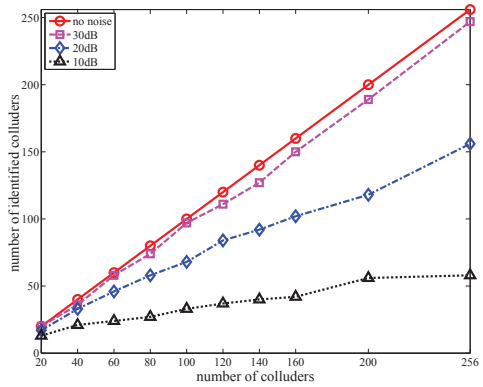


Fig. 6. Colluder identification performance of the PACWE scheme parameterized by the FNR value equal to 10, 20, and 30 dB and the no-noise case.

The performance of proposed anti-collusion fingerprinting system parameterized by the distortion compensation parameter $a$, which is set to 1.0, 0.7 and 0.5, is shown in Fig. 7. The settings of this experiment are basically the same as before except for a fixed FNR level of 20 dB. As shown in the figure, the system can detect more colluders when the distortion compensation parameter $a$ is 0.5. The distortion compensation parameter in the proposed fingerprinting system provides the additional robustness against collusion attacks.

## VI. Conclusion and Future Work

We proposed a new anti-collusion fingerprinting system based on SCS and colluder weight discovery. Under this framework, the host signal is treated as a channel and fingerprints as user signals transmitted over independent parallel subchannels. Then, colluder weights in time-varying collusion attacks can be estimated using pilot symbols at the decoder, and all weights can be estimated and compensated in the recovery structure. It was shown by experiments that the proposed fingerprinting system outperforms many existing techniques in terms of the number of identified colluders. Advanced channel estimation and compensation techniques to improve the performance of colluder identification will be studied further in the future.

## References

[1] B.-H. Cha and C.-C. Jay Kuo, "Design and analysis of high-capacity anti-collusion hiding codes," *Journal of Circuits, Systems, and Signal Processing*, vol. 27, pp. 195–211, March 2008.

[2] B.-H. Cha and C.-C. Jay Kuo, "Advanced colluder detection techniques for OSIFT-based hiding codes," in *Proc. IEEE Int'l Sym. Circuits and Systems*, Seattle, Washington, May 2008, pp. 2961–2964.

[3] B. Chen and G. W. Wornell, "Quantization index modulation a class of provably good methods for digital watermarking and information embedding," *IEEE Transactions on Information Theory*, vol. 47, pp. 1423–1443, May 2001.

[4] A. Swaminathan, S. He, and M. Wu, "Exploring QIM based anti-collusion fingerprinting for multimedia," in *Proc. SPIE Conf. Security, Watermarking, and Steganography*, San Jose, CA, January 2006.

[5] K. J. Ray Liu, W. Trappe, Z. Jane Wang, M. Wu, and H. Zhao, *Multimedia fingerprinting forensics for traitor tracing*, Hindawi, EURASIP on Signal Processing and Communications, New York, NY, 2005.

[6] M. H. M. Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory*, vol. 29, pp. 439–441, May 1983.

[7] J. J. Eggers, R. Bauml, R. Tzchoppe, and B. Girod, "Scalar Costa scheme for information embedding," *IEEE Transactions on Signal Processing*, vol. 51, pp. 1003–1019, April 2003.

[8] P. Moulin and R. Koetter, "Data-hiding codes," *Proceedings of the IEEE*, vol. 93, pp. 2083–2126, December 2006.

[9] D. N. C. Tse and P. Viswanath, *Fundamentals of wireless communication*, Cambridge University Press, Cambridge, UK, 2005.

[10] T. M. Cover and J. A. Thomas, *Elements of information theory*, Wiley, New York, NY, 1991.

[11] P. Moulin and M. K. Mihcak, "The parallel-Gaussian watermarking game," *IEEE Transactions on Information Theory*, vol. 50, pp. 272–289, February 2004.

[12] I. D. Shterev and R. L. Lagendijk, "Amplitude scaling estimation for quantization-based watermarking," *IEEE Transactions on Signal Processing*, vol. 54, pp. 4146–4155, November 2006.

[13] L. Hanzo, M. Munster, B. J. Choi, and T. Keller, *OFDM and MC-CDMA for broadband multi-user communications, WLANs and broadcasting*, John Wiley & Sons, West Sussex, UK, 2004.

[14] Y. Li, "Pilot-symbol-aided channel estimation for OFDM in wireless systems," *IEEE Transactions on Vehicular Technology*, vol. 49, pp. 1207–1215, July 2000.