A novel anti-collusion coding scheme tailored to track linear collusions

Kannan Karthik and Dimitrios Hatzinakos
University of Toronto
Dept. of Electrical and Computer Engineering
10 Kings College St., Ontario, M5S 3G4, Canada
{karthik, dimitris}@comm.utoronto.ca

Abstract

A set of semi-fragile watermarks $W_{Fr} = \{V_1, V_2, .., V_v\}$ can be used as building blocks for constructing any digital fingerprint. One such family, is obtained by modulating the sign bits alone of selective DCT-AC coefficients, where, each V_j represents the positions of a disjoint subset of modulated coefficients. We show that a linear collusion of $K < n$ sign fingerprinted images neatly translates into a majority bit vote of K corresponding binary strings and in this binary output, '1' represents survival of a particular block V_j and '0' its erasure. By design, each block V_j is unperturbed by specific collusion patterns and so by facilitating complementary coverage of each newly added block V_{j+1}, a compact anti-collusion code (ACC) for tracking linear collusions can be constructed.

1 Introduction

A digital fingerprint is either a precipitate of an access control operation or a covert piece of information embedded in the content to track its users or may represent a blueprint of the content whose preservation implies authenticity. Its significance is explained through the following examples.

Ex 1: Inviting collusions within joint access scenarios [3]- In joint diagnosis, n doctors are expected to put together their respective shares $Sh_1, Sh_2, ..Sh_n$ of a key K_E to a highly confidential medical record. The record can be viewed clearly when all the n shares are put together. If $K < n$ shares are fused, the reconstruction is poor rendering further diagnosis impossible. In addition, a perceptible fingerprint identifying the illegitimate coalition of traitors, is embedded in the distorted medical record. This dual protection role is possible only if the shares are non-perfect [6] (i.e the entropy $H(K_E/Sh_i) < H(K_E)$) and there exists a unique association between every K-subset of shares.

Ex 2: Authentication and tracing of copies of digital portraits- A fingerprint in this application has three pieces of information: (I_1) To link the buyer with the creator, (I_2) A blueprint of the original as a fragile watermark, (I_3) Traitor tracing properties to counter a collusion attack. A restriction on the maximum amount of information that can be imperceptibly concealed, the implicit redundancy in $[I_1, I_2, I_3]$ and the varying robustness/fragility requirements of I_1, I_2, I_3 makes the design process challenging.

Ex 3: The Multicast fingerprinting problem- Since the very purpose of fingerprinting is to impart a unique identity to each copy of an image or video I in circulation, it makes the process of simultaneous dissemination of n copies less efficient. The challenge in multicast environments stems from the need for a balance between efficient multicast delivery and good tracking resolution (or fingerprint robustness). The joint fingerprinting and decryption (JFD) architecture[4], [5] and the source based architecture with a group oriented structure [9] are two extreme but suboptimal solutions to this complex problem. In this framework, some K out of n users $\{p_1, p_2, .., p_K\} \subset \{1, 2, ..n\}$ may indulge in an act of piracy by fusing their respective fingerprinted copies $I_{p1}, I_{p2}, ..I_{pK}$ through a process called collusion with a common goal to dissolve their identities. Much of the current literature focusses on spatial domain attacks in which a set of pixels from a particular video frame or image location are chosen from different legal copies and then linearly [8] or non-linearly [10] combined.

Leading to the problem of imparting collusion resistance to fingerprints, Boneh and Shah [1] were the first to describe a fingerprint as a composition of v marks in which each mark may reside in one of 's' possible states. They showed that it was not possible to design totally collusion-secure codes but was possible to detect atleast one colluder with a high probability out of $K = log(n)$ traitors. From a practical viewpoint, they did not discuss how watermark modulation schemes could be designed to complement the coding methodology.

Dittmann et al. [2] through their projective geometry approach presented an intuitive solution for spatial domain collusion. Each mark was a deliberate manipulation of a se-

lective group of pixels in an image. A total of $N+1$ marks represented $N+1$ points in an N-dimensional space. A fingerprint constituted a subset of N points, which formed a subspace. The ingenuity of the scheme lay in the fact that these subspaces were constructed such that an intersection of any N or fewer subspaces would result in a unique set of points. So, the seed for code-modulation was sown here. One of the issues was that the number of unique document marking positions increased linearly as the number of users which made implementation difficult for images with low texture. Apart from a need for generalization, further insight was required regarding the behavior of code-modulation schemes for different collusion attack models.

Code-modulation applied to digital fingerprinting was finally formalized by Trappe et al. [7]. In their approach each fingerprint was expressed as $F_i = \sum_{j=1}^{j=v} b_{ij} U_j$ where, U_j is the basis vector and $b_{ij} \in \{-1, 1\}$ is obtained from an ACC matrix. Their ACC matrix was constructed using (v, k, λ)-balanced incomplete block designs (BIBDs) based on the assumption that a linear collusion of fingerprinted copies can be approximated as a logical AND of codewords from the ACC matrix. Although their approach resulted in the creation of codewords with $v \approx O(\sqrt{n})$ basis vectors, the logical AND assumption is incorrect when the number of traitors is greater than two.

The fingerprint modulation strategy, the ACC book which governs the mark distribution across users and the collusion attack model are very closely knit. In this paper, a symbiosis of sign bit modulation (SBM) of selective discrete cosine transform (DCT) AC coefficients and a specifically tailored ACC is used for tracking linear collusions.

2 Effect of linear collusion on sign bit modulated fingerprints

SBM fingerprints were used in the JFD architecture [4] for secure multicast for the following reasons:

1. The sign bits alone of perceptually significant DCT AC coefficients represent crucial phase information in the DCT domain.
2. The sign bits also have a high entropy. This implies that any two adjacent 8×8 blocks with slightly different textures will have very different sign signatures.
3. Spatially orthogonal SBM fingerprints are highly fragile to collusion (specifically linear collusion).

Properties 1 and 3 imply that it is possible to build each fingerprint F_i from a subset of v spatially orthogonal SBM watermarks (or marks) $W_{Fr} = \{V_1, V_2, .., V_v\}$. Property 2 indicates that the original un-watermarked sign plane and the fingerprinted sign plane are likely to be statistically similar which is important from the point of view of secrecy.

Let $U = \{1, 2, ...n\}$ represent the user space and $SC = \{p_1, p_1, ..p_K\} \subset U$ the set of traitors. Fig. 1 gives an overview of the sign bit modulation process. X represents the sign matrix extracted for embedding which is partitioned into $v+1$ disjoint segments, $X(P_1), X(P_2), ..., X(P_v), X(P_{NF})$ out of which the first v constitute the watermark embedding region and $X(P_{NF})$ represents the portion which is left untouched. The randomly chosen sets $P_1, ..P_v$ indicate the positions of the coefficients where these v marks will be embedded, known only to the source. For a $n \times v$ codebook $c_{ij} \in \mathbf{C}$, the fingerprinted sign plane of user i is given by,

$$X_{Fi} = \begin{bmatrix} X_1^i & X_2^i & \cdots & X_v^i & X_{NF} \end{bmatrix}^T \tag{1}$$

where, $X_j^i = s_{i,j} X(P_j)$ for $j = 1, 2, ..v$. Since the discrete cosine transform is a linear transform, the averaging of any K pirated images $I_{p_1}, I_{p_2}, .., I_{p_K}$ is equivalent to,

$$\begin{aligned} \text{i.e.} \quad & \frac{I_{p_1} + .. + I_{p_K}}{K} \\ \iff & \frac{X_{F(p_1)} + .. + X_{F(p_K)}}{K} \\ \iff & \frac{1}{K} \begin{bmatrix} \sum_{i=1}^{i=K} X_1^{p_i} \\ \sum_i X_2^{p_i} \\ \vdots \\ \sum_i X_v^{p_i} \\ X_{NF} \end{bmatrix} = \frac{1}{K} \begin{bmatrix} X(P_1) \sum_i s_{p_i,1} \\ X(P_2) \sum_i s_{p_i,2} \\ \vdots \\ X(P_v) \sum_i s_{p_i,v} \\ X_{NF} \end{bmatrix} \end{aligned}$$

$$I_{lincol(SC)} \iff X_{Fcol} = \begin{bmatrix} X(P_1) Z_1 \\ X(P_2) Z_2 \\ \vdots \\ X(P_v) Z_v \\ X_{NF} \end{bmatrix} \tag{2}$$

where,

$$Z_j = \sum_{i=1}^{i=K} s_{p_i,j} \tag{3}$$

The source is assumed to have the original unwatermarked image. Having acquired the pirated copy while in circulation, the tracing process begins by first extracting the sign plane X_{Fcol} from the manipulated image. The marks are detected through a sign comparison with the unwatermarked sign plane X.

$$\begin{aligned} \text{SignDiff}(X, X_{Fcol}) = & \quad \text{Sign} \begin{bmatrix} Z_1 & Z_2 & \cdots & Z_v \end{bmatrix}^T \\ = & \begin{bmatrix} \text{MAJ}(s_{p_1,1}, s_{p_2,1}, .., s_{p_K,1}) \\ \text{MAJ}(s_{p_1,2}, s_{p_2,2}, .., s_{p_K,2}) \\ \vdots \\ \text{MAJ}(s_{p_1,v}, s_{p_2,v}, .., s_{p_K,v}) \end{bmatrix} \\ = & \quad \text{MAJ}(\overline{S}_{p_1}, \overline{S}_{p_2}, .., \overline{S}_{p_K}) \\ \iff & \quad \overline{C}_R = \text{MAJ}(\overline{C}_{p_1}, .., \overline{C}_{p_K}) \end{aligned} \tag{4}$$

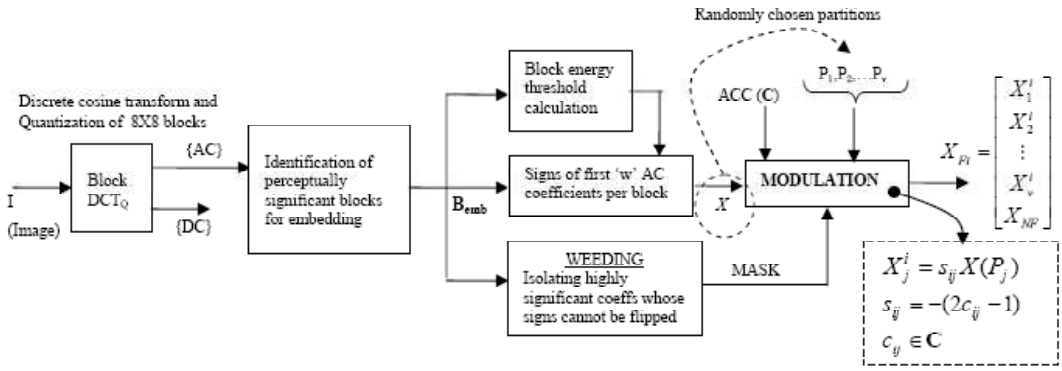

Figure 1. Overview of sign bit modulation scheme for fingerprinting

where, $\overline{S}_{p_i} = [s_{p_i,1}, s_{p_i,2}, .., s_{p_i,v}]^T$, $\overline{C}_{p_i}$ represents the row vectors in the codebook C (with $c_{p_i,j} = \frac{1-s_{p_i,j}}{2}$) and MAJ represents the majority bit vote operation.

To track all linear collusions involving K or fewer traitors, the ACC must be constructed in such a way that the retrieved codeword $\overline{C}_R$ is unique. For example, a codebook designed to track all possible collusions within the small group of three users ($n = 3, v = 3, K = 3$) is,

$$C_{3,3} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \tag{5}$$

3 Collusion invariants

When a set of colluders SC fuse their sign fingerprinted copies, some of the marks $\{V_{i1}, V_{i2}, ..\} \subset W_{Fr}$ are preserved. So by design, each mark V_i is expected to survive a particular set of collusion patterns and can be termed as an 'invariant' to this set of patterns $CP(V_i)$ (e.g. V_1 in the $C_{3,3}$ codebook survives $CP(V_1)$ = {(1), (2), (1, 2), (1, 2, 3)}). Each subsequently added mark $V_{i+1}, V_{i+2}..., V_v$ is distributed amongst the users to cover the collusion patterns not survived by $\{V_1..V_i\}$. To create a compact codebook, each step i in the construction process entails the insertion of a column vector col_i of a particular hamming weight (hwt) w_i, such that the sum of symmetric differences represented by the parameter,

$$COVER_i = \sum_{j=1}^{i-1} |CP(V_i) \triangle CP(V_j)| \tag{6}$$

is maximized. The process is illustrated in Fig. 2. At any point of time during the construction process, the total coverage depends on just two parameters: (1) The hamming weights $w_1, w_2, ..$ and (2) Hamming distances between any two columns ($d_{c(ij)} = d_H(col_i, col_j)$).

The choice of hamming weight w_i is critical. Consider a single column vector with weight w and length n. The number of patterns covered by this vector is,

$$|CP_w| = \underbrace{\binom{w}{1}}_{\text{users}} + \underbrace{\binom{w}{2}}_{\text{2-cols}} + \underbrace{\binom{w}{2} \times \binom{n-w}{1} + \binom{w}{3}}_{\text{3-cols}} + \underbrace{\binom{w}{3} \times \binom{n-w}{1} + \binom{w}{4}}_{\text{4-cols}} + ... \tag{7}$$

For a specific (n, K), $|CP_w|$ increases with w. So, if $w_i << n$, the coverage will be poor and a large number of marks will be required (Note that $w_{i(min)} = floor(K/2) + 1$). But merely this observation is insufficient to surmise that w must be large, since the other parameter (i.e. $d_{c(ij)}$) also decides the rate of growth of the function $COVER_i$.

If, $w_i \approx n$, $COVER_i$ will grow very slowly resulting in a large v. Results are tabulated for $(n = 11, K = 4), w \geq 3$ in Table. 1. Thus, good convergence rates are possible if w_i is chosen around $n/2$ atleast for the first few iterations.

3.1 Algorithm description

The construction is carried by serially adding columns selected based on certain criteria. The first column col_1 in the codebook is chosen as any vector with hamming weight $w_1 \approx n/2$ for reasons mentioned in the previous section. This weight is kept constant for the first few iterations (upto $i = r$). The value of r is chosen in such a way that the largest possible string of maximally equidistant columns with weight w_1 is created to maximize collusion coverage.

col_2 is chosen with $w_2 = w_1$ so that $d_{c(2,1)}$ is maximum. For each iteration, $i \geq 3$, from the codebook ACC(i-1) with $i - 1$ columns, the average of all $N_i = \binom{i-1}{2}$ inter-column distances $d_{c(ij)}$ is first calculated.

$$d_{av(i)} = \frac{1}{N_i} \sum_{(p,q)} d_{c(pq)} \tag{8}$$

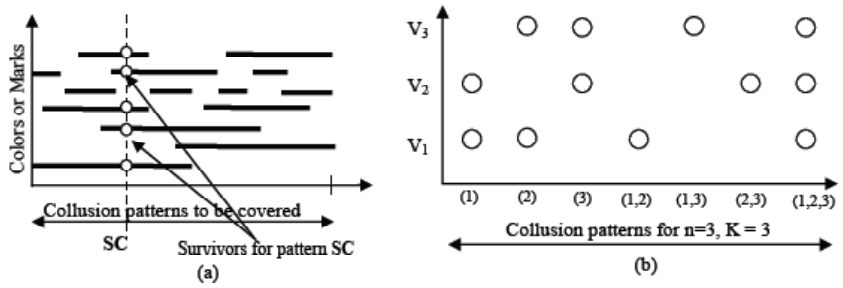

Figure 2. (a) A general construction example. (b) Coverage using C(n=3,K=3) codebook (Eqn 5)

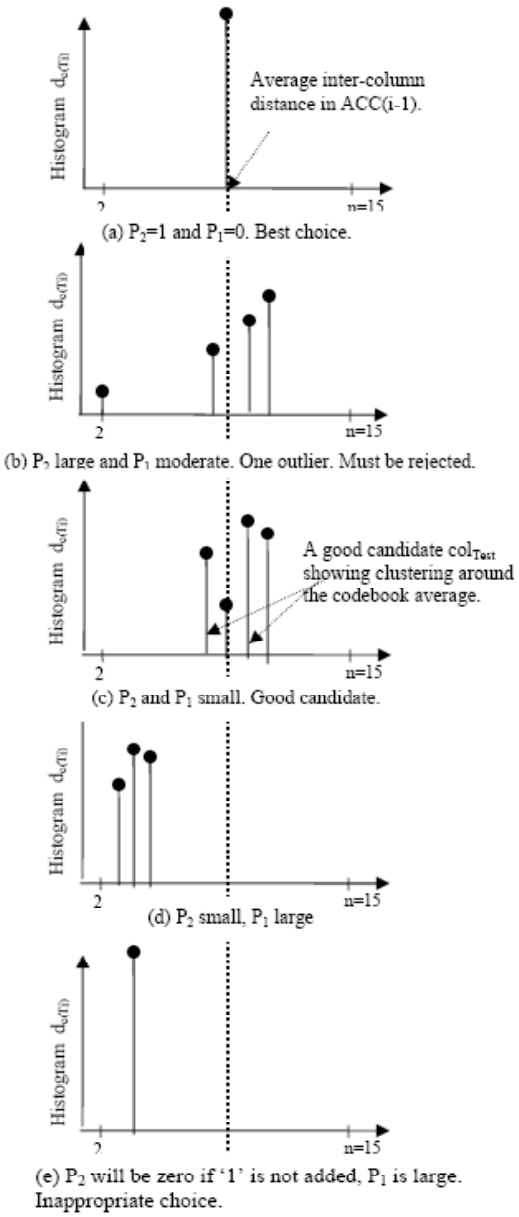

Figure 3. Significance of parameters P_1, P_2

where, $1 \leq p, q \leq i-1$ and $p \neq q$. The column space from which these vectors col_i are picked is given by,

$$\begin{aligned} Q_{select} &= \{\bar{c} \text{ s.t. } hwt(\bar{c}) = w_1\}(\text{ IF } i \leq r) \\ &= \{\bar{c} \text{ s.t. } hwt(\bar{c}) \in \{w_{min}, .., w_{max}\}\}(\text{ IF } i > r) \end{aligned}$$

where, $w_{min} \approx n/2$. For each potential candidate $col_{Test} \in Q_{select(i)}$, the distance,

$$d_{c(Tj)} = d_H(col_{Test}, col_j) \tag{9}$$

is computed for $j = 1, 2, ..i-1$. We now define two important parameters,

$$P_1 = \frac{1}{N_a} \sum_{j=1}^{i-1} (d_{c(Tj)} - d_{av(i)})^{k_1} \tag{10}$$

where, $N_a = i-1$ and k_1 is chosen as 4. Minimization of P_1 ensures that most of the new candidate's distances $d_{c(Tj)}, j = 1, .., i-1$ are close to average inter-column distance in ACC(i-1) ($d_{av(i)}$). But, P_1 alone does not guarantee clustering of distances $d_{c(Tj)}$ about $d_{av(i)}$ (See Fig. 3(b)).

So we need another parameter which strings together these distance values $d_{c(Tj)}$ and forces the clusters to form around the average value. This can be done by introducing some symmetry in the construction process through a parameter P_2. So minimization of P_2 enforces $d_{c(Tp)} \approx d_{c(Tq)}$ with $p, q \in \{1, ..i-1\}$. Fig. 3(d) shows why condition P_2 alone does not suffice. Also note that the first column is left out of the P_2 calculation as it tends to upset the construction of long strings of equidistant columns.

$$P_2 = \mathbf{1} + \frac{1}{N_b} \sum_{(p,q)} (d_{c(Tp)} - d_{c(Tq)})^2 \tag{11}$$

where, $p \neq q, 2 \leq p, q \leq i-1$ and $N_b = \binom{i-2}{2}$. Combining P_1, P_2 we require col_{Test} which minimizes (Fig. 3(a,c)),

$$R_i = P_1 \cdot P_2 \tag{12}$$

Fig. 3(e) points out the importance of adding '1' to the P_2 term (otherwise, $R_i = 0$). This whole column by column insertion process is repeated till the 'uniqueness' requirement is met in iteration i by ACC(i) (i.e. majority vote of any $K \leq n$ codewords results in a unique value).

3.2 Fingerprint detection

Partial collusion coverage implies abrupt truncation of the codebook even though the (n, K) uniqueness constraint is not satisfied as per the majority bit vote. This in turn does not imply that certain combinations of traitors will go completely undetected. This only means that there is more than one group of suspects $\widehat{SC}_1$,..,$\widehat{SC}_t$ corresponding to the bit pattern $\overline{C}_R$ retrieved from the pirated copy $I_{col(SC)}$. Given $\overline{C}_R$ and the available list of codewords $\overline{C}_1, .., \overline{C}_n$, the following approach is taken:

Histogram based classification- First evaluate $d_i = d_H(\overline{C}_R, \overline{C}_i)$ for $i = 1, 2, ..n$, and then plot a histogram of d_i. The graph is highly likely to be of bi-modal type, in which one hump corresponds to the suspects ($\widehat{SC}$) and the other to the set of innocent users. The valley point can be chosen as the threshold (d_{Th}) for classification, i.e. Suspects, $\widehat{SC} = \{\text{Users } i \text{ s.t. } d_i \leq d_{Th}\}$. If discrimination is not possible, threshold is set as $d_{Th} = d_{i(min)}$.

4 Simulation results

The codebook has been tested by subjecting sign fingerprinted copies of a 256×256 Lena image to four different types of collusion attacks (one linear and three non-linear operations in which median, min and max values of pixels from different copies are calculated). For simulations, $n = 15$ and the codebook C_m has been designed for $K \leq 4$ which requires $v = 28$ columns (Fig. 4). Tests are conducted for four different codebooks: C_m, two derived by truncating C_m and one using Hadamard 2-designs [3]).

Out of a total of $B_{embed} = 662$ blocks in Lena with significant texture, $B_{weed} = 357$ were shortlisted for weeding. Two of the most significant AC coefficients from each block in B_{weed} were identified and then masked (no sign flips would be performed on these coefficients). The size of the sign plane X extracted was 11916 bits from which approximately $L = 1000$ can be flipped. So, if the codebook has v columns, the payload per mark is $PM = L/v$, i.e. 35 bits (when $v = 28$), 66 bits ($v = 15$) and 100bits ($v = 10$).

In the sign modulation scheme, each semi-fragile mark is simply a repetition of PM sign differences, a majority of which must be preserved after collusion, for the mark to be detected. Hence, although traceability strongly depends on the size and structure of the ACC, PM influences the robustness of the marks to single copy attacks and also provides some stability during a collusion operation.

Tracing results for $K = 4$, in which the traitors were randomly chosen amongst 15 users as $SC = \{2, 5, 7, 12\}$, are in Table. 2. Effect of truncation is noticeable as false positives when only 10 columns in C_m are used. Table. 3 investigates the impact when more than the design specified number K traitors collude. It is seen that when six traitors collude, a subset can be detected accurately in three of the codebooks ($C_m, C_{m(v=15)}, C(HAD-2)$). One false positive is obtained when $C_{m(v=10)}$ is used. Fig. 5 shows the impact of collusion on the perceptual quality of the copies. Effect of linear collusion (Fig. 5(c)) is a 2dB increase in PSNR which emphasizes the fragility of sign bit modulated fingerprints, a property which allows better traceability.

5 Conclusions

Watermarks created by sign modulation of selective block DCT AC coefficients serve as excellent building blocks for constructing collusion resistant fingerprints. By cleverly reusing and distributing the blocks in W_{Fr} amongst n users to create unique associations between the fingerprints, any partial fingerprint erasure can be traced back to a subset of colluders. More specifically, a linear collusion of a sign fingerprinted copies has been shown to reflect as a majority bit vote of fingerprint codewords, which forms the basis of our ACC construction. Simulations confirm that this holds good for some non-linear collusion operations also.

References

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

[2] J. Dittmann, A. Behr, M. Stabenau, P. Schmitt, J. Schwenk, and J. Uederberg. Combining digital watermarks and collusion secure fingerprints for digital images. *SPIE Intl. Conf. Electronic Imaging*, 41:171–182, 1999.

[3] K. Karthik. Methodologies for access control and fingerprinting of multimedia. *Ph.D. Thesis, University of Toronto*, 2006.

[4] K. Karthik and D. Hatzinakos. Decryption Key Design for Joint Fingerprinting and Decryption in the Sign Bit Plane for Multicast content protection. *International journal of Network Security*, 4(3):254–265, May 2007.

[5] D. Kundur and K. Karthik. Video Fingerprinting and Encryption Principles for Digital Rights Management. *Proceedings of the IEEE*, 92(6):918–932, June 2004.

[6] K. Kurosawa, K. Okada, K. Sakano, W. Ogata, and S. Tsujii. Nonperfect secret sharing schemes and matroids. *Lecture Notes in Computer Science*, 765:126–141, 1994.

[7] W. Trappe, M. Wu, J. Zang, and K. J. R. Liu. Anti-collusion Fingerprinting for Multimedia. *IEEE Transactions on Signal Processing*, 51(4):1069–1087, April 2003.

[8] Z. J. Wang, M. Wu, H. Zhao, W. Trappe, and K. J. R. Liu. Anti-Collusion Forensics of Multimedia Fingerprinting Using Orthogonal Modulation. *IEEE Transactions on Image Processing*, 14(6):804–821, June 2005.

[9] H. V. Zhao and K. J. R. Liu. Fingerprint Multicast for Secure Video Streaming. *IEEE Transactions on Image Processing*, 15(1):12–29, Jan 2006.

[10] H. V. Zhao, M. Wu, Z. J. Wang, and K. J. R. Liu. Forensic Analysis of Nonlinear Collusion Attacks for Multimedia Fingerprinting. *IEEE Transactions on Image Processing*, 14(5):646–661, May 2005.

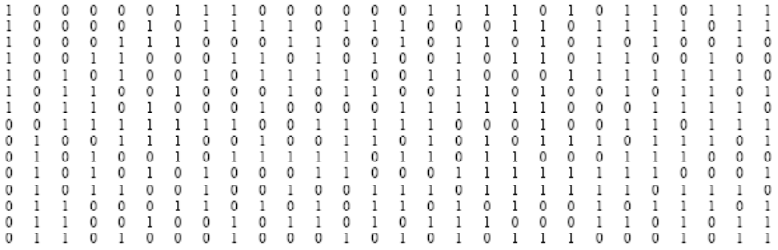

Figure 4. (15,4)-ACC constructed using parameters $w_1 = 7$, $r = 10$ and $w_{(it>r)} \in \{5, 6, ..11\}$.

(a) (b) (c) (d)

Figure 5. (a) Original, (b) Fingerprinted (PSNR = 32.10dB), (c) Attack LC: SC = {4,10,14} (34.37dB), (d) Attack NL_{min}: SC = {4,10,14} (31.91dB)

Table 1. Codelength v for $(11, 4)$ ACC as a function of hamming weight w using Algo. in Sect. 3.1.

w	3	4	5	6	7	8	9	10	11
v_{min}	53	32	21	27	24	26	40	NC	NC

NC $\Rightarrow$ no convergence. Best for $w = 5$.

Table 2. Tracing results for $SC = \{2, 5, 7, 12\}$

	Detection results with different codebooks			
Collusion Attacks	$\widehat{SC}(C_m)$	$\widehat{SC}(C_{m(v=15)})$	$\widehat{SC}(C_{m(v=10)})$	$\widehat{SC}(HAD-2)$
LC	{2,5,7,12} $d_{th} = 10$	{2} $d_{th} = 4$	{**1***,2,**4**,5,7,**13**} $d_{th} = 4$	{12} $d_{th} = 4$
NL_{med}	{2,5,7,12} $d_{th} = 10$	{2,5} $d_{th} = 4$	{**1**,2,**4**,5,7,**13**} $d_{th} = 4$	{12} $d_{th} = 4$
NL_{min}	{2,5,7,12} $d_{th} = 10$	{2} $d_{th} = 4$	{2,**4**,5,7} $d_{th} = 3$	{12} $d_{th} = 4$
NL_{max}	{2,5,7,12} $d_{th} = 10$	{2} $d_{th} = 4$	{2,**4**,5,7} $d_{th} = 3$	{12} $d_{th} = 4$

* Bold face indicates false positive.
LC: Linear collusion, NL_{med}: Median operation, NL_{min}: Min value of pixels, NL_{max}: Max value
Main codebook, C_m: (15,4)-ACC with $v = 28$.
HAD-2: Codebook based on Hadamard-2 designs [3].

Table 3. Effects when $t = 6 > K$ traitors collude. Results for $SC = \{2, 7, 8, 9, 10, 15\}$

	Detection results with different codebooks			
Collusion Attacks	$\widehat{SC}(C_m)$	$\widehat{SC}(C_{m(v=15)})$	$\widehat{SC}(C_{m(v=10)})$	$\widehat{SC}(HAD-2)$
LC	{2} $d_{th} = 8$	{2} $d_{th} = 4$	{2,**14**} $d_{th} = 3$	{7,8,9,10} $d_{th} = 6$
NL_{med}	{2} $d_{th} = 8$	{2,9,15} $d_{th} = 5$	{2,**14**} $d_{th} = 3$	{7,8,9,10} $d_{th} = 6$
NL_{min}	{2,7,8,9,15} $d_{th} = 10$	{2} $d_{th} = 4$	{2,**14**} $d_{th} = 3$	{9} $d_{th} = 5$
NL_{max}	{2,7,8,9} $d_{th} = 10$	{2} $d_{th} = 4$	{2,**14**} $d_{th} = 3$	{2,7,9} $d_{th} = 6$