Project: Anti-collusion codes (ACCs) tailored to a specific transform domain

Dr. K. Karthik
ECE Department, IITG

Goals:

1) The project aims to identify a suitable anti-collusion code which can be matched with a semi-fragile watermark embedding algorithm.

2) It also involves the search for a parametric transform domain where the fingerprint can be concealed. The choice of transform domain must take into account intricate details such as the erasure characteristics of the semi-fragile watermarks to various forms of collusion operations.

1) Domain-specific Anti-collusion codes for Multimedia Fingerprinting

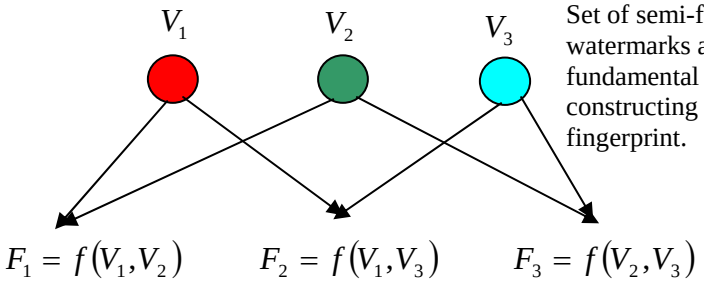
Digital fingerprinting is of paramount importance in tracking illegal distribution of images, electronic documents, audio-clips and video streams. Typical applications are in the infringement of intellectual property rights (IPR) such as leakage of industrial designs and in the illegal resale of expensive digital portraits and video clips of movies. The content to be protected from a copyright violation is first fingerprinted by the distributor by embedding imperceptible signals tailored to the format of the source data which can be in audio, video or even text form.

One of the biggest threats to fingerprints is the outset of a collusion attack in which subsets of users (traitors) illegally fuse their fingerprinted copies to erase traces of the fingerprints. These attacks can be executed in the time, spatial, transform or even compressed bit domains. Since the traitors will be concerned about the quality of the colluded video/audio/image segments, they are likely to execute it in the spatial or time domain so that they can control the intensity of the attacks.

Such attacks can be deterred by using anti-collusion coding schemes designed to track spatial and time domain collusion operations. A fingerprint can be constructed from a set of *v* semi-fragile watermarks $\{V_1, V_2, ..., V_v\}$ (marks) and can be represented as a *v*-bit binary codeword where '1' indicates the presence of a particular mark V_i, $i \in \{1,2,...,v\}$ and '0' its absence. An example of a design for tracking $K=3$ or fewer traitors in a small user space of $n=3$, is shown in Figure 1. The survival of a particular trait to a collusion attack depends on the dominance of that trait amongst the group of colluders. All other traits in minority are not expected to survive.

Based on Figure 1, if users 1 and 2 fused their fingerprinted copies, one would expect trait V_1 (common to users 1 and 2) to survive. On the other hand if users 1 and 3 combine their copies, trait V_2 will survive. This variation in survival characteristics is crucial for traitor tracing as it leaks out the collusion pattern, i.e.,

$(u_1, u_2) \rightarrow V_1$
$(u_2, u_3) \rightarrow V_3$
$(u_1, u_3) \rightarrow V_2$



Set of semi-fragile watermarks as fundamental units for constructing a fingerprint.

Unique inheritance of each user's fingerprint accounts for the varying constitution.

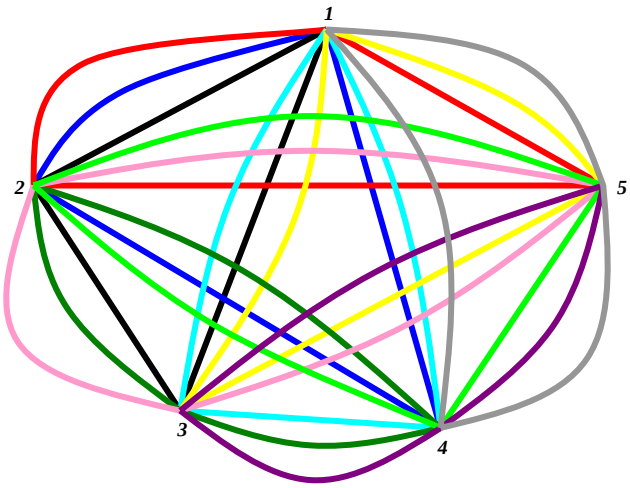
Represented in compact form as a codebook where rows represent fingerprints

$$C(K=3, n=3) = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

Figure 1: Fingerprint design for a small user space of three users. The codebook *C(3,3)* can track any three or fewer traitors.

Challenges: The semi-fragile watermarks must satisfy certain properties,

- Each one must globally dispersed (throughout the image or video).
- All identical in the manner in which they are embedded in a particular domain.
- Mutually orthogonal in the spatial or frequency domains.
- Fragile to collusion but robust to single copy attacks.
- Survival based on dominance of a particular mark amongst the group of colluders. Recessive-ness leads to their erasure.
- Must be preferably concealed using a parametric transform in which the erasure properties are known.
- A careful association must be built across fingerprints as depicted in the (3,5)-code shown in Figure.2. This will make the design robust to collusion operations.
- The positions of the fragile watermarks must not be revealed through a copy-comparison attack. This requires certain anti-symmetry properties to be built into the code-design particularly when one considers a subset of codewords. An example is shown in the shaded form in Figure 2 in columns 3 and 6.



	Dimensions or Marks or Colors									
Code	V_1	V_2	V_3	V_4	V_5	V_6	V_7	V_8	V_9	V_{10}
C_1	1	1	1	1	1					1
C_2	1	1	1			1	1	1		
C_3	1			1	1	1	1		1	
C_4		1		1		1		1	1	1
C_5			1		1		1	1	1	1

Each dimension or color V_i, connects exactly 3 different fingerprints $[C_i, C_j, C_k]$ where $i, j, k \in \{1,2,3,4,5\}$. The blank spots are '0'.

Figure 2: An example of a $(K = 3, n = 5)$ anti-collusion code designed to trace three or fewer traitors out of five.

2) Parametric transforms for image watermarking and encryption

Every signal space has a basis or a set of bases which permit an orthogonal or non-orthogonal decomposition of the signals into a set of components aligned along the basis vectors. The choice of basis is very often tailored towards the characteristics of the signal and designed to provide compact support. Some of the standard transforms (or basis sets) applied to discrete signals are the discrete Fourier transform (DFT), discrete Hadamard transform (DHT) and discrete cosine transform (DCT). Most watermarking techniques do not conceal the transform domain in which the watermark signal is embedded.

Theoretically there are many possible choices of bases which span a given signal space. However only a selective few form an orthogonal basis. If orthogonality is sacrificed and the choice of basis is made arbitrary, there are seemingly infinite possible decompositions of a particular signal. One way to construct a family of basis functions is by parameterizing the standard transforms such as DCT, DFT and DHT. The set of parameters which are used to identify a particular basis within this family form a secret key. Thus through this secret basis one can construct a hidden domain in which a watermark can be concealed.

Very often the concealment of a watermark requires intricate knowledge of the masking properties of the human visual system (HVS) to maximize embedding capacity. Hence one of the challenges in this problem is not just identifying a parametric transform for embedding but also lies in tuning the HVS parameters to suit the secret domain chosen.