An attack on the Domingo-Ferrer and Herrera-Joancomarti fingerprinting scheme

Mike Burmester, Jiangyi Hu, and Yong Cheng

Department of Computer Science
Florida State University
Tallahassee, FL 32306-4530, USA

Domingo-Ferrer and Herrera-Joancomarti proposed recently a short collusion-secure fingerprinting scheme that exploits the properties of dual binary Hamming codes to reduce the length of the fingerprint. We show that this scheme is insecure. In particular, a collusion of any two buyers can frame an innocent buyer.

Introduction: Piracy of digital assets, and in particular multimedia data, is a major concern to industry, particularly since access to such data via the internet is readily available. Protection usually involves the insertion of a digital copyright in the form of a fingerprint in the digital asset, which is used to detect pirate copies. Fingerprinting algorithms introduce a small number of imperceptible errors, called marks in specified positions of the data. The positions marked and their values are kept secret. It should not be possible to remove a fingerprint without affecting significantly the quality of the copyrighted data.

With fingerprinted copies a collusion of buyers can detect some marks by comparing their copies. These marks can then be deleted or flipped. The goal of a collusion is to make pirate copies that either cannot be linked to any particular buyer (e.g. by erasing most of the fingerprint), or that are linked to other buyers. Such buyers are said to be *framed*. A fingerprinting scheme in which innocent buyers are framed is of little practical use. This remark applies even if the set of buyers that are linked to pirate copy includes some of the colluding buyers, provided it is not possible to distinguish the innocent buyers.

The DF-HJ fingerprinting scheme: In a recent Letter [3], Domingo-Ferrer and Herrera-Joancomarti proposed a fingerprinting scheme whose fingerprints are codewords of a dual Hamming code DH_N of length $n = 2^N - 1$ [4]. With this scheme up to n copies can be marked each with a fingerprint of size n. This is a significant saving on the fingerprint scheme proposed by Boneh and Shaw [1]. However the DF-HJ scheme is flawed. We shall show how a collusion of any two buyers X, Y can make a pirate copy that frames an innocent buyer U, by implicating U as a possible conspirator.

An attack on the DF-HJ fingerprinting scheme: DH_N is a linear code of length $n = 2^N - 1$, dimension N, and generating matrix an $N \times n$ matrix with columns all the non-zero binary N-tuples. For this code, every non-zero codeword z has weight $wt(z) = 2^{N-1}$ [4].

Consider a collusion of buyers X, Y whose copies have fingerprints $x, y \in DH_N$. Let $inv(x, y)$ be the tuple consisting of all the bits in the invariant positions of x, y. For DH_N, the length of $inv(x, y)$ is 2^{N-1} and $wt(inv(x, y)) = 2^{N-2}$ [4]. We shall use the invariant positions of x, y to partition the tuple representation of the codewords of DH_N. Each $z \in DH_N$ will be represented by a tuple (z_1, z_2), with z_1 the tuple of bits of z that are in the invariant positions of x, y, and z_2 the tuple of remaining bits. It is easy to see that $z_1 \in DH_{N-1}$ and z_2 belongs to the 1st order Reed-Muller code $\mathcal{R}_{N-1}$ of length 2^{N-1} [4] ($\mathcal{R}_{N-1}$ is the extended binary dual Hamming code of length 2^{N-1}). In this representation, the tuple z_2 uniquely identifies the codeword z. Indeed if $z = (z_1, z_2)$ and $z' = (z_1', z_2')$ are representations of codewords with $z_2 = z_2'$, then $z + z' = (z_1 + z_2, 0^*)$, where 0^* is the 2^{N-1}-tuple of zeros (addition is bitwise xor). Since $z + z'$ must be a codeword of DH_N, and since its weight is less than 2^{N-1} (the length of $z_1 + z_2$ is $2^{N-1} - 1$), it has to be the zero codeword (non-zero codewords have weight 2^{N-1}). It follows that $z = z'$.

The attack has as follows. From their copies, the colluders X, Y can get the tuples x_2, y_2 (but not $x_1 = y_1$). X, Y use this information to make a pirate copy in which the bit value 1 is assigned to all positions in their copies with different bit values in x, y. The fingerprint of the pirate copy is thus $z = (x_1, x_2 + y_2)$, where $x_2 + y_2$ is a 2^{N-1}-bit tuple of 1s.

Earlier we observed that $wt(x_1) = wt(x_2) = wt(y_2) = 2^{N-2}$. So the weight of z is $2^{N-2}+2^{N-1}$, which is greater than 2^{N-1}. Therefore $z \notin DH_N$. However, the (Hamming) distance of z from $x, y, x+y$ is:

$$d(z,x) = d(z,y) = d(x,x+y) = 2^{N-2},$$

since the representation of $x+y$ is $(0^*, x_2+y_2)$, where 0^* is a 2^{N-1}-tuple of zeros. It follows that it is impossible to decide which pair of colluders made the pirate copy with fingerprint z.

Of course, if no copies have been marked with the codeword $x+y \in DH_N$, then X, Y will be traced. However such a constraint reduces significantly the efficiency of the fingerprinting scheme: instead of having n copies with fingerprint size n, we only have m copies, where $n = m + \frac{1}{2}m(m-1) = \frac{1}{2}m(m+1)$ copies. This is less than what we have with the incidence-matrix fingerprinting scheme.

*An incidence-matrix fingerprinting scheme***:** This is based on the incidence-matrix of the largest number of potential colluders. For 2 collusion-security, the incidence-matrix is a binary $m \times n$ matrix, $n = \frac{1}{2}m(m-1)$, with rows corresponding to buyers and columns to unordered pairs of buyers. The entry in row Z and column $\{X, Y\}$ is 1 if and only if $Z \in \{X, Y\}$. Row Z is the fingerprint of buyer Z. So the weight of a fingerprint being $m-1$.

Traitors are traced by taking a tally, for each buyer, of incidences with all pairs $\{X, Y\}$ in the pirate fingerprint. A collusion is traced if there are

2 buyers whose tally is greater than that of any other buyer. Observe that because of the way this scheme is set up, there will always be one extra incidence in the tally of a pair of colluding buyers, since the position of this pair is not known to the colluders.

References

1. D. Boneh and J. Shaw. Collusion-secure fingerprinting for digital data. *IEEE Trans. Inf. Theory*, **IT-44**(95), pp. 1897-1905, 1998.
2. F. Sebe and J. Domingo-Ferrer. Short 3-secure fingerprinting codes for copyright protection. In, L. Batten and J. Seberry (Eds), *ACISP 2002*, Springer, LNCS **2384**, pp. 316-327, 2002
3. J. Domingo-Ferrer and J. Herrera-Joancomarti. Short collusion-secure fingerprints based on dual binary Hamming codes. ElectroniLetters. **36**(20), pp. 1697–1699, 2000
4. F.J. MacWilliams and N.J.A Sloane. The theory of error correcting codes, North-Holland, 1977