Critique to Burmester and Le attack to Sebé and Domingo-Ferrer fingerprinting scheme

F. Sebé and J. Domingo-Ferrer

Burmester and Le claimed in a very recent Letter that the 3-secure fingerprinting scheme proposed by Sebé and Domingo-Ferrer was vulnerable to an attack in which a collusion of any three buyers could frame an innocent buyer. The authors show that the assumptions made by Burmester and Le in their attack cannot be made in practice.

Introduction: Fingerprinting is a copyright protection technique that consists of introducing small modifications (marks) to the content to be distributed. These modifications are different for each copy sold and allow embedding of a different fingerprint for each buyer. In this way, in case of finding an illegal copy, the fingerprint will be extracted and the dishonest buyer who redistributed the copy will be identified.

In a collusion attack, a set of attackers compare their copies to locate differences and try to compose a new copy so that its embedded fingerprint does not permit their identification.

The design of collusion-secure fingerprinting codes is based on the so-called 'marking assumption' [1]. This assumption states that the marked positions and their values are kept secret. In this way, the attackers can only locate and alter those marks that differ between the compared copies.

In [4, 5] Sebé and Domingo-Ferrer presented a fingerprinting scheme proven to be secure against collusions of up to three attackers. This scheme was very recently claimed to be weak in [2]. In that Letter, an attack is presented that would allow collusion of three members to destroy the fingerprint.

Sebé and Domingo-Ferrer fingerprinting scheme: In a nutshell, the construction of the 3-secure fingerprints in [4, 5] is as follows:

1. Take a dual binary Hamming code, DH(n), as outer code.
2. Take a scattering code, SC(s, t), as inner code to encode the bits of codewords in the outer code.
3. Permute the bits of the resulting composed codewords using a secret permutation Π.

The resulting codewords have a length $(2t+1)(2^n-1)s$. Each codeword is assigned to a different buyer and constitutes the buyer's fingerprint.

Critique of Burmester and Le attack: In the attack presented in [2], several colluding buyers detect the differences in their fingerprints by comparing their fingerprinted copies. Further, it is assumed that colluders can generate a new copy in which the bit value 0 is assigned to all positions in which their fingerprints differ.

We claim that this cannot be done in practice. Comparison of fingerprinted copies can indeed reveal differences between marks in them, but assuming that colluders know the mapping between each mark version and its corresponding embedded fingerprint bit value is not realistic. Without this assumption, the colluders cannot force a bit value 0 in a position in the fingerprint, which makes the Burmester and Le attack infeasible.

To illustrate, let us consider a fingerprinting scheme for textual content in which fingerprint bits are embedded by using pairs of synonyms in some places of the text. Assume three buyers compare their copies and see that two of them have the word 'nevertheless' at a certain place in the text, while the third buyer has the synonym 'however' at the same place. Now, this does not imply that colluders can decide whether 'nevertheless' embeds a 0 fingerprint bit and 'however' a 1 bit or whether it is the other way round. To mount the Burmester and Le attack, colluders need to know which synonym embeds 0.

An additional argument for the practical infeasibility of colluders being able to force particular fingerprint bits is that, in order to make the marking assumption realistic, fingerprints are normally embedded using an underlying watermarking system. The watermarking system protects the fingerprint against single-user attacks so that, as required by the marking assumption, the fingerprinting system only needs to care about collusion attacks. Now, precisely to avoid non-random manipulation of the embedded marks, most watermarking systems use a secret key as a parameter for the mark embedding and recovery processes [3]. The secret key is used to encrypt the information to be embedded and to decide the location of marks.

Thus, in the practical setting of a fingerprinting system sitting on top of a watermarking system, the encryption performed at the watermarking level prevents colluders from being able to force 0 bit values at the fingerprinting level.

Bit-selectable scenarios and encrypted fingerprints: In the (unlikely) scenarios that no underlying watermarking encryption is used and/or colluders can select the fingerprint bit values, we can always add an

encryption step at the fingerprinting level. In the case of the Sebé and Domingo-Ferrer scheme this would mean adding a fourth step to the three steps sketched above.

4. Generate a secret random $(2t+1)(2^n-1)s$-bit sequence S and use it to stream-cipher the permuted codewords.

With this additional step, the fingerprint is encrypted before embedding, so colluders can at most force a bit value for the encrypted fingerprint, but not for the cleartext fingerprint. Decoding is now as follows:

1. Stream-decipher the fingerprint extracted from the content using the random sequence S.
2. Undo the permutation Π.
3. Decode the inner scattering codes.
4. Decode the Dual Hamming codeword by minimum distance.

Acknowledgment: This work was partly supported by the Spanish Ministry of Science and Technology and the European FEDER fund through Project No. TIC2001-0633-C03-01 'STREAMOBILE'.

© IEE 2004
18 May 2004
Electronics Letters online no: 20045449
doi: 10.1049/el:20045449

F. Sebé and J. Domingo-Ferrer (*Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, Av. Països Catalans 26, Tarragona E-43007, Catalonia, Spain*)

E-mail: fsebe@etse.urv.es

References

1 Boneh, D., and Shaw, J.: 'Collusion-secure fingerprinting for digital data', *IEEE Trans. Inf. Theory*, 1998, **IT-44**, (95), pp. 1897–1905
2 Burmester, M., and Le, T.: 'Attack on Sebé, Domingo-Ferrer and Herrera-Joancomartí fingerprinting schemes', *Electron. Lett.*, 2004, **40**, (5), pp. 172–173
3 Katzenbeisser, S., and Petitcolas, F.A.P.: 'Information hiding: techniques for steganography and digital watermarking' (Artech House, Norwood, MA, 2000)
4 Sebé, F., and Domingo-Ferrer, J.: 'Short 3-secure fingerprinting codes for copyright protection'. ACISP 2002 (Springer 2002), LNCS 2384, pp. 316–327
5 Sebé, F., and Domingo-Ferrer, J.: 'Scattering codes to implement short 3-secure fingerprinting for copyright protection', *Electron. Lett.*, 2002, **38**, (17), pp. 958–959