Multimedia asymmetric watermarking and encryption

G. Boato, N. Conci, V. Conotter, F.G.B. De Natale and C. Fontanari

An asymmetric watermarking algorithm is presented, involving a private key for embedding and a public key for detection, joint with a suitable encryption scheme, thus achieving a double security level for digital data protection. A commutative scheme is designed based on linear algebra and on a secret random permutation, allowing both to cipher watermarked data and to mark encrypted data without interfering with the watermark detection process.

Introduction: In the age of information technology, the problem of ensuring copyright protection to multimedia contents has been addressed by two different means, namely, media encryption and digital watermarking. The former scrambles data in order to make them unintelligible to any unauthorised user and ensures confidentiality. The latter embeds imperceptible information such as copyright into media data, providing authentication of the content. As pointed out in the recent enlightening contribution [1], watermarking and cryptography have often been confused in the communication security literature by emphasising their superficial analogies, especially in the case of asymmetric watermarking. It is demonstrated that many of these similarities are misleading or incorrect, and it is strongly suggested that secure watermarking systems are designed via a layered approach. From this point of view, we distinguish between secure watermark detection (which protects against watermark removal by a cheating verifier) and secure watermark embedding (which allows protection of both the original content and the watermark even if the insertion is operated by a non-trusted embedder). For secure watermark detection two different solutions are available: asymmetric watermarking and zero-knowledge [2]. Existing methods combining watermarking and cryptography involve a sequence of protection operations. To save computational cost a commutative property is necessary in many applications, i.e. a watermark can be embedded in and detected from an encrypted or unencrypted file [3]. As suggested in [4], here we detail both theoretically and experimentally a digital watermarking scheme designed to be both asymmetric and commutative with a suitable encryption procedure. We adapt our watermarking method based on linear algebra, following the line started in [5], and we apply the easiest possible encryption method, i.e. we scramble coefficients according to a random secret permutation. In this proof of concept, the watermarking and the encryption scheme are admittedly very simple and limited in security. Nevertheless, to the best of our knowledge, this is the first attempt to match asymmetric watermarking with cryptography, thus preventing from a fair comparison with different methods but opening the road towards more sophisticated joint schemes.

Watermark embedding and ciphering: Basic set-up: Let V be a feature space of dimension d and consider an original feature $\phi = (\phi_1, \ldots, \phi_d)$. If π is a secret random permutation of $\{1, \ldots, d\}$, we can define the encryption function $f_E(\phi) = \phi_\pi = (\phi_{\pi(1)}, \ldots, \phi_{\pi(d)})$. Now let $s = (s_1, \ldots, s_d)$ be a digital signature and let $w = (\alpha_1 s_1, \ldots, \alpha_d s_d)$ be the corresponding imperceptible watermark, where $\alpha_1, \ldots, \alpha_d \in R$ are suitable scaling factors with $0 < \alpha_i \ll 1$ for all i. The embedding function is defined by $f_W(\phi, w) = \psi = \phi + w$. On the one hand, we can introduce the watermarked encrypted feature obtained by embedding the encrypted mark into the encrypted original as

$$\xi = f_W(f_E(\phi), \quad f_E(w)) = f_E(\phi) + f_E(w) = \phi_\pi + w_\pi \tag{1}$$

where $w_\pi = (\alpha_{\pi(1)} s_{\pi(1)}, \ldots, \alpha_{\pi(d)} s_{\pi(d)})$ denotes the scrambled watermark. On the other hand, we can define the encrypted watermarked feature as

$$\begin{aligned}\chi = f_E(f_w(\phi, w)) = f_E(\phi + w) = f_E(\phi) + f_E(w) = \phi_\pi + w_\pi \\ = f_W(f_E(\phi), \quad f_E(w)) = \xi\end{aligned} \tag{2}$$

Definition of auxiliary matrices: To construct the public detection key, we need to introduce some auxiliary matrices. Let M be a secret $d \times d$ orthogonal matrix and consider $\phi = Mv$, $\psi = My$, $\xi = Mx$, (i.e. v, y, x are the co-ordinates of ϕ ψ, ξ, respectively, in the basis given by the columns of M). Let $B = (b_1, b_2, \ldots, b_d)$ be an orthonormal basis of R^d such that $< b_1, b_2 > = < y, x >$ (where $< \ldots >$ denotes linear span). To construct B, first complete (y, x) to an arbitrary basis of R^d and then apply the Gram-Schmidt orthonormalisation process. If N is the matrix with b_t^T as the tth column ($t = 1, \ldots, d$), then let $A = \Delta N^T$, where:

$$\Delta = \begin{pmatrix} r & 0 & \cdots & & & & \\ 0 & s & 0 & \cdots & & & \\ 0 & & K & \cdots & & & \\ \vdots & & & \ddots & & & \\ 0 & \cdots & & & K & 0 & \cdots \\ 0 & \cdots & & & & 0 & \cdots \\ \vdots & & & & & \vdots & \ddots \end{pmatrix} \tag{3}$$

with $K \gg 1$ an integer appearing k times and $1 < r, s \ll K$ two secret real parameters.

Public key releasing: Finally, we can release the public detection key $D = AM^T$. Note that, since A is not invertible, the secret matrix M cannot be reconstructed from D and if r and s are kept secret, then no sensitive information about the original feature can be deduced from a knowledge of D.

Watermark detection: Let now $\phi_\in$ be an extracted feature. The watermark detection is accomplished by the decision function

$$\delta(\phi_e) = \begin{cases} 1 & \text{if } |sim(D\phi_e)| \geq \varepsilon \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

where $0 \leq \varepsilon \ll 1$ is a suitable threshold and

$$sim(D\phi_e) = \frac{(e_1^T D\phi_e) + (e_2^T D\phi_e)}{\|D\phi_e\|^2} \tag{5}$$

where e_i ($i = 1, 2$) denotes the ith vector of the canonical basis of R^d. Definitions (4) and (5) for the detector are motivated by the following mathematical consequences.

Theorem: We have $sim(D\psi) = sim(D\xi) = sim(D\chi) = 1$, i.e. the watermark is always detected into the watermarked, the watermarked encrypted, and the encrypted watermarked images. Moreover, if the integer K is big enough, then $sim(D\phi)$ and $sim(D\phi_\pi)$ is arbitrarily close to zero, i.e. the watermark is not detected into the original and the just encrypted images.

Proof: By definition of B, we have $< D\psi, b_i > = < D\xi, b_i > = < D\chi, b_i > = 0$ for every $i = 3, \ldots, d$, hence the first claim follows from (5). Next, if $M^T\phi = \sum_{t=1}^d c_t b_t$ and $M^T\phi = \sum_{t=1}^d g_t b_t$, then by (5)

$$sim(D\phi) = sim\left(\sum_{t=1}^d c_t A b_t\right) = \frac{r^2 c_1^2 + s^2 c_2^2}{r^2 c_1^2 + s^2 c_2^2 + K^2 \sum_{t=3}^{k+2} c_t^2} \tag{6}$$

$$sim(D\phi_\pi) = sim\left(\sum_{t=1}^d g_t A b_t\right) = \frac{r^2 g_1^2 + s^2 g_2^2}{r^2 g_1^2 + s^2 g_2^2 + K^2 \sum_{t=3}^{k+2} g_t^2} \tag{7}$$

In particular,

$$\lim_{k\to\infty} sim(D\phi) = \lim_{k\to\infty} sim(D\phi_\pi) = 0 \tag{8}$$

and also the second claim holds.

Simulations: We choose as a feature space the space R^d corresponding to the entries in the top left 25×25 DCT coefficients of a digital image excluding the DC component and as a watermark a random sequence of length $d = 624$. We set $K = 10^3$ and $k = 15$, and we randomly select $r = 1.3587$ and $s = 0.8945$. Fig. 1 shows the false positive probability (P_{fa}) measured on a sample of 200 different watermarks against the threshold ε. According to this graph, we can reasonably set $\varepsilon = 0.3$ and correspondingly evaluate the detection probability (P_d). Performance for white Gaussian noise (WGN) addition is shown in Fig. 2. We stress the robustness of the proposed method: the embedded mark can be perfectly detected in the watermarked image down to PSNR of 31 dB, but also in the encrypted domain down to PSNR of 34 dB. Fig. 3 shows experimental results for resizing, which provides

a realistic example of processing for jointly watermarked and encrypted images.

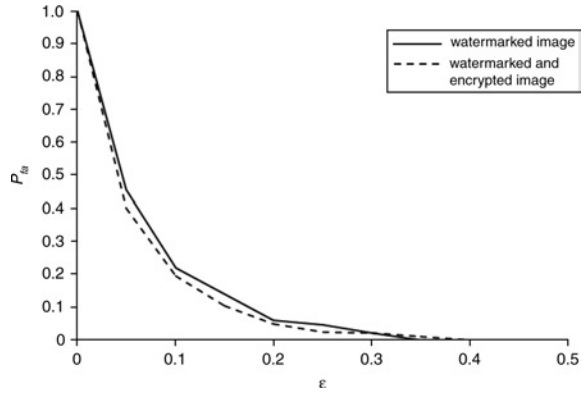

Fig. 1 *False positive probability P_{fa} against threshold ε*

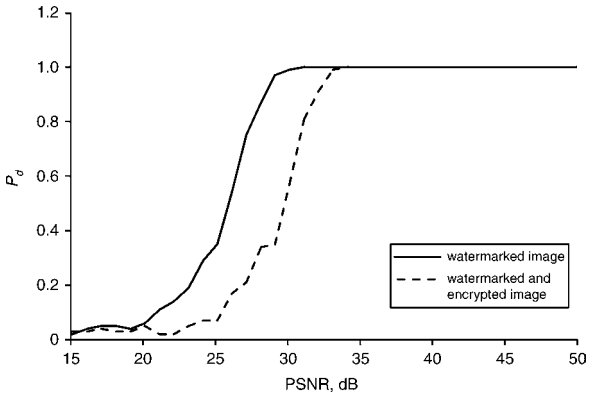

Fig. 2 *Detection probability P_d against white Gaussian noise addition in terms of PSNR*

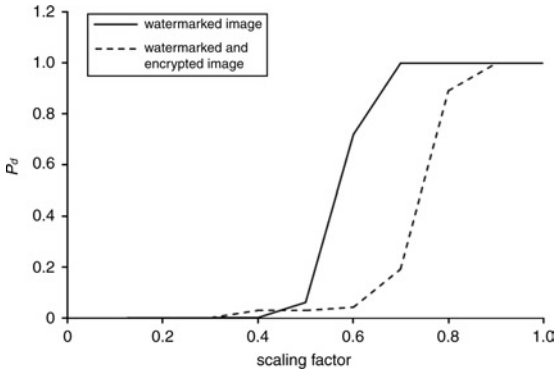

Fig. 3 *Detection probability P_d against scaling factor*

Conclusions: We present an asymmetric watermarking scheme integrated with an encryption method in such a way that the whole system is commutative, namely, it allows both to cipher watermarked data and to mark encrypted data by requiring just one single detector. Future work will be devoted to the specific case of video applications.

22 February 2008
Electronics Letters online no: 20080492
doi: 10.1049/el:20080492

G. Boato, N. Conci, V. Conotter and F.G.B. De Natale (*Department of Information Engineering and Computer Science, University of Trento, Via Sommarive 14, Trento I-38050, Italy*)

E-mail: boato@disi.unitn.it

C. Fontanari (*Department of Mathematics, School of Information Technologies, Politecnico di Torino, Corso Duca degli Abruzzi 24, Torino I-10129, Italy*)

References

1 Cox, I.J., Doerr, G., and Furon, T.: 'Watermarking is not cryptography'. Proc. Int. Workshop on Digital Watermarking 2006, LNCS 4283, pp. 1–15
2 Sadeghi, A.-R.: 'The marriage of cryptography and watermarking-beneficial and challenging for secure watermarking and detection'. Proc. Int. Workshop on Digital Watermarking 2007, pp. 2–18
3 Lian, S., Liu, Z., and Wang, H.: 'Commutative encryption and watermarking in video compression', *IEEE Trans. Circuits Syst. Video Technol.*, 2007, **17**, (6), pp. 774–778,
4 Boato, G., Conotter, V., De Natale, F.G.B., and Fontanari, C.: 'A joint asymmetric watermarking and image encryption scheme'. Proc. IS&T/SPIE Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, January 2008
5 Boato, G., De Natale, F.G.B., and Fontanari, C.: 'An improved asymmetric watermarking scheme suitable for copy protection', *IEEE Trans. Signal Process.*, 2006, **54**, (7), pp. 2833–2834