Digital Signatures Based on Invertible Watermarks for Video Authentication

Enrico Hauer[1], Jana Dittmann[2], and Martin Steinebach[1]

[1] Fraunhofer Institute IPSI, Dolivostr. 15, 64293 Darmstadt, Germany
Enrico.hauer@ipsi.fraunhofer.de
[2] Otto-von-Guericke-Unversity, Multimedia and Security Lab (AMSL),
Universitätsplatz 2, 39016 Magdeburg, Germany
Jana.dittmann@iti.cs.uni-magdeburg.de

1 Security Demands and Solution

For verification and authentication of the video material and recovery of the original video several security mechanisms are required. The security techniques to realize this solution are introduced in [1]:

1. The verification of the integrity is verified by hash functions.
2. Authenticity is verified by digital signatures using asymmetric cryptography and hash functions. The introduced scheme from [1] uses RSA signatures. The private key of the digital signature mechanism is used to sign the data and the corresponding public key is used for verification of the encrypted data. If the data can be verified the corresponding private key was used for the digital signature generation and the data seems to be authentic as well integer.
3. Furthermore the original content can be reproduced by inverting of the watermark with the well know techniques of Fridrich et al. [2]. Additional secret key cryptography (symmetric crypt function) protects the reproduction. The invertibility is necessary, because we use a digital watermark to embed the authentication message and signature into the media itself. Digital watermark, in this application fragile watermark, changes the data and the original data cannot be reconstructing. To invert the data, the watermark must be removed and the original data reconstructed. The watermark embeds the information into a non visual or acoustical channel of the data after the original data of the channel were compressed and encrypted. The compression realizes the new space for the watermark consisting of the encrypted selected data and security information.

2 Invertible Watermark for Video Material

In this paper we demonstrate the watermark information for one picture P of the video because the frame index as a part of the information is changed from picture to picture. The picture index controls the order of the frames.

The picture data are split into selected data $P_{selected}$ and remaining data $P_{remaining}$. The selected data are compressed and encrypted symmetrically with the secret

J. Dittmann, S. Katzenbeisser, and A. Uhl (Eds.): CMS 2005, LNCS 3677, pp. 277 – 279, 2005.

key $K_{\sec ret}$. A following encryption establishes the dependency of the encrypted data from with the remaining data $P_{remaining}$. The selected data can only be recovered with no changes at the remaining data. After the decryption of the selected data the integrity of selected data are verified with a message authentication code HMAC with secret key $K_{\sec ret}$. The public authentication of the picture data is realized with a RSA signature, because the signature can be check by the public key K_{public}.

The complete watermark information can be summarized to the following form:

$$\begin{aligned} W = {} & E_{AES}\left(E_{AES}\left(C_{P_{selected}}, K_{\sec ret}\right), K_{H\left(P_{remaining}\right)}\right) \\ & +Index(P) \\ & +MAC_{HMAC}((P_{selected} + Index(P)), K_{\sec ret}) \\ & +S_{RSA}(H(P_{remaining} + Index(P) \\ & \qquad +E_{AES}(E_{AES}(C_{P_{selected}}, K_{\sec ret}), K(_{H(P_{remaining})})) \\ & \qquad +MAC_{HMAC}((P_{selected} + Index(P)), K_{\sec ret})), K_{private}) \end{aligned} \tag{1}$$

Figure 1 demonstrates the embedding procedure. The LSB bits of the blue chrominance values at the DCT block position (5, 5) are the selected data and compressed by RLE to produce the free space to embed the watermark.

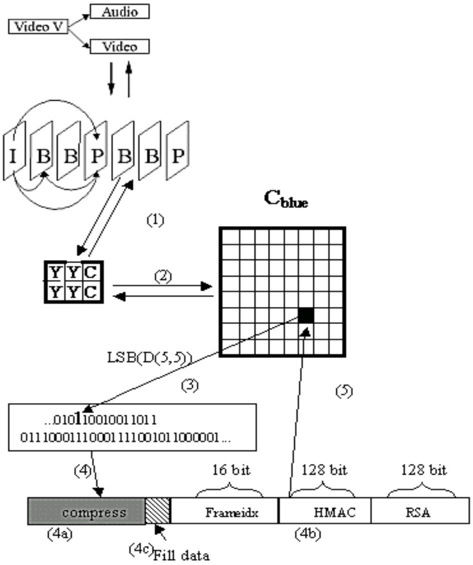

Fig. 1. Watermark embedding procedure

References

1. J. Dittmann., M. Steinebach, L. Ferri. Watermarking protocols for authentication and ownership protection based on timestamps and holograms. In: Proceedings of SPIE Vol. 4675, Security and Watermarking of Multimedia Contents IV, pp.240 - 251, San-Jose, January, ISBN 0-8194-4415-4, 2002
2. J. Fridrich, M. Golian, R.Du: Lossless Data Embedding – New Paradigm in Digital Watermarking, Special Issue on Emerging Applications of Multimedia Data Hiding, Vol. 2002, No.2, February 2002, pp. 185–196