P.O.Box 8718, Beijing 100080, China	Journal of Software Sept 2003,14(9):1645-1651
E-mail: jos@iscas.ac.cn	ISSN 1000-9825, CODEN RUXUEW, CN 11-2560/TP
http://www.jos.org.cn	Copyright © 2003 by The Editorial Department of Journal of Software

零知识水印验证协议

邹潇湘, 戴 琼, 黄 晟, 李锦涛

邹潇湘1,3, 戴 琼2, 黄 晟1, 李锦涛1 1(中国科学院 计算技术研究所,北京 100080)2(中国科学院 软件研究所,北京 100080)3(国家计算机网络与信息安全管理中心,北京 100029)
第一作者: 邹潇湘(1976－),男,湖南望城人,博士,主要研究领域为数字水印技术.
联系人: 邹潇湘 Telephone: 86-10-82990356, E-mail: zxx@mail.nisac.gov.cn
Received 2003-01-10; Accepted 2003-03-13

Abstract
Watermark technology has been developed to tackle the problem of unauthorized copying and distribution of digital data. Several different schemes have been proposed in the last few years, but most of them are symmetric, i.e., the key used for watermark embedding is just the same used for watermark detection. However, in many applications, an asymmetric scheme is needed, where the secrete information used to detect the watermark is not enough to modify, counterfeit or remove the watermark. In this paper, some watermark verification protocols based on bit commitment and zero knowledge proof are proposed. The ownership prover insert the watermark into the host signal using symmetric watermark technology based on spread spectrum. The watermark detect key is sent to the verifier hiding in bit commitment. By the interactive protocol between the prover and the verifier, the verifier can extract the embedded watermark, but he can not modify, counterfeit or remove it. Protocols are proposed to verify one watermark bit and several watermark bits respectively. Those protocols can be used to verify the watermark information inserted into image, audio and video using spread spectrum watermark technology.

Zou XX, Dai Q, Huang C, Li JT. Zero knowledge watermark verification protocols. *Journal of Software*, 2003,14(9):1645~1651.
http://www.jos.org.cn/1000-9825/14/1645.htm

摘要
在数字产品中嵌入数字水印,是对其进行版权保护的一种有力手段.近年来提出了不少数字水印方案,但是它们中大部分都是对称的,即用于水印嵌入和水印检测的密钥是相同的.而许多实际的应用都要求非对称的数字水印方案,即水印检测时所知道的秘密不足以修改、伪造或移去水印.对基于比特承诺和零知识证明的水印验证协议进行了研究.所有权证明者采用基于扩频的对称水印技术,在宿主信号中嵌入水印;水印检测的密钥采用比特承诺的形式提交给验证者,通过证明者和验证者之间的交互协议,验证者可以提取到所嵌入的水印,但无法修改、伪造或移去水印.分别提出了验证一个和多个水印比特的协议,可应用于验证嵌入在图像、音频和视频数据中的扩频水印.

基金项目：Supported by the National High-Tech Research and Development Plan of China under Grant No.2001AA114010 (国家高技术研究发展计划(863))

References:

[1] Craver S, Katzenbeisser S. Copyright protection protocols based on asymmetric watermark: The ticket concept. In: Proceedings of the 6th Conference on Communication and Multimedia Security (CMS 01). 2001. 159~170. http://www.ifip.tu-graz.ac.at/TC6/events/CMS/cms01.htm.

[2] Hartung F, Girod B. Fast public-key watermarking of compressed video. In: Proceedings of the IEEE International Conference on Image Processing (ICIP'97). 1997. 528~531. http://clip.informatik.uni-leipzig.de/~toelke/Watermark/ip971113.pdf.

[3] Schyndel RGV, Tirkel AZ, Svalbe ID. Key independent watermark detection. In: IEEE International Conference on Multimedia Computing and Systems. 1999. 580~585. http://lci.det.unifi.it/Staff/Piva/Watermarking/Docs/icmcs99.html.

[4] Eggers JJ, Su JK, Girod B. Public key watermarking by eigenvectors of linear transforms. In: Proceedings of the European Signal Processing Conference (EUSIPCO 2000). 2000. http://graphics.tu-bs.de/v3d2/pubs.collection/diwa_eus2000eggers.pdf.

[5] Furon T, Duhamel P. Robustness of asymmetric watermarking technique. In: Proceedings of the IEEE International Conference on Image Processing (ICIP 2000). 2000. 21~24. http://lci.det.unifi.it/Staff/Piva/Watermarking/Docs/programicip.html.

[6] Linnartz JPMG, Talstra JC. MPEG PTY-marks: Cheap detection of embedded copyright data in DVD-video. In: Computer Security - ESORICS 98, 5th European Symposium on Research in Computer Security. Lecture Notes in Computer Science 1485, 1998. 221~240. http://buffy.eecs.berkeley.edu/~linnartz/wpapers.html.

[7] Kalker T, Linnartz JP, Dijk MV. Watermark estimation through detector analysis. In: Proceedings of the IEEE International Conference on Image Processing (ICIP'98). 1998. 425~429. http://buffy.eecs.berkeley.edu/~linnartz/wpapers.html.

[8] Craver S. Zero knowledge watermark detection. In: International Workshop on Information Hiding (IHW'99). Lecture Notes in Computer Science 1768, 1999. 101~116. http://citeseer.ist.psu.edu/craver00zero.html.

[9] Craver S, Katzenbeisser S. Security analysis of public-key watermarking schemes. In: Schmalz MS, ed. Mathematics of Data/Image Coding, Compression, and Encryption IV, with Applications. Proceedings of the SPIE Vol. 4475, 2001. 172~182. http://www.dbai.tuwien.ac.at/staff/katzenb/pubs.html.

[10] Gopalakrishnan K, Memon N, Vora P. Protocols for watermark verification. In: Multimedia and Security Workshop at ACM Multimedia'99. 1999. 103~106. http://www.hpl.hp.com/personal/Poorvi_Vora/Pubs/acm99.pdf.

[11] Adelsbach A, Sadeghi AR. Zero-Knowledge watermark detection and proof of ownership. In: International Workshop on Information Hiding (IHW 2001). Lecture Notes in Computer Science 2137, 2001. 273~288. http://www-krypt.cs.uni-sb.de/download/papers/AdSa_01.pdf.

[12] Adelsbach A, Katzenbeisser S, Sadeghi AR. Cryptography meets watermarking: detecting watermarks with minimal or zero knowledge disclosure. In: Proceedings of the European Signal Processing Conference (EUSIPCO 2002). 2002. http://www.dbai.tuwien.ac.at/staff/katzenb/download/eusipco02.ps.gz.

[13] Cox IJ, Kilian J, Leighton T, Shamoon T. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, 1997,6(12):1673~1687.

[14] Hartung F, Girod B. Watermarking of uncompressed and compressed video. Signal Processing, Special issue on Copyright Protection and Access Control for Multimedia services, 1998,66(3):283~301.

[15] Fujisaki E, Okamoto T. A practical and provable secure scheme for publicly verifiable secret sharing and its applications. In: Nyberg K, ed. Advances in Cryptology EUROCRYPT'98. Lecture Notes in Computer Science 1403, 1998. 32~46. http://www.uni-giessen.de/crypto/kryptoag/Bibliothek/Bibliothek.htm.

[16] Schnorr CP. Efficient signature generation by smart cards. Journal of Cryptology, 1991,4(3):161~174.

[17] Cramer R, Damgard I, Schoenmakers B. Proofs of partial knowledge and simplified design of witness hiding protocols. In: Proceedings of the Crypto'94. Lecture Notes in Computer Science 839, 1994. 174~187. http://www.win.tue.nl/~berry/papers/crypto94.pdf.

[18] Craver S, Memon N, Yeo BL, Yeung MM. Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications. IEEE Journal on Selected Area in Communications, 1998,16(4):573~586.