P.O.Box 8718, Beijing 100080, China	Journal of Software, Sept. 2005,16(9):1606-1616
E-mail: jos@iscas.ac.cn	ISSN 1000-9825, CODEN RUXUEW, CN 11-2560/TP
http://www.jos.org.cn	Copyright © 2005 by The Editorial Department of *Journal of Software*

公开可验证的零知识水印检测

何永忠, 武传坤, 冯登国

何永忠1,2, 武传坤1, 冯登国1
1(信息安全国家重点实验室(中国科学院 软件研究所),北京 100080)
2(中国科学院 研究生院,北京 100049)
作者简介: 何永忠(1969－),男,重庆人,博士生,主要研究领域为密码学,系统安全;武传坤(1964－),男,博士,研究员,博士生导师,主要研究领域为密码学;冯登国(1965－),男,博士,研究员,博士生导师,主要研究领域为密码学.
联系人: 何永忠 Phn: +86-10-62528254 ext 803, E-mail: yzhe@is.iscas.ac.cn

Received 2004-01-05; Accepted 2004-06-10

Abstract
As the detection key in symmetric watermarking scheme can be used to forge or remove watermarks from digital works, it is required that the detection key be secret in watermark detection procedures. Based on zero-knowledge and proof of knowledge concepts and protocols in Cryptology, zero-knowledge watermark detection protocols can make the verifier believe the presence of a watermark in a disputed digital work while not compromising the detection key. The security requirements of a publicly verifiable zero-knowledge watermark detection scheme are outlined in this paper. Then a publicly verifiable commitment scheme and a zero-knowledge proof of knowledge protocol which proves knowing the discrete logarithm of a committed value are presented. Finally, using the above scheme and protocol as building blocks, a publicly verifiable zero-knowledge watermark detection protocol is proposed and its security considerations are addressed.

He YZ, Wu CK, Feng DG. Publicly verifiable zero-knowledge watermark detection. *Journal of Software*, 2005,16(9):1606-1616.
DOI: 10.1360/jos161606
http://www.jos.org.cn/1000-9825/16/1606.htm

摘要
对称水印方案的水印检测密钥可以被用来伪造和移去水印,因此要求它在检测过程中也是保密的.零知识的水印检测方案利用密码学中零知识和知识证明的思想和算法,实现在水印检测时使得验证者确信水印存在性的同时又不泄漏水印检测密钥.提出了公开可验证的零知识水印检测的安全需求,给出一个公开可验证的承诺方案和一个证明知道被承诺值的离散对数的零知识知识证明协议.在此基础上提出了一个公开可验证的零知识水印方案,并讨论了它的安全性.

基金项目：Supported by the National Natural Science Foundation of China under Grant Nos.60025205, 90304007 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2004AA147070 (国家高技术研究发展计划(863))

References:

[1] Kalker T, Linnartz JP, Dijk MV. Watermark estimation through detector analysis. In: Proc. of the IEEE Int'l Conf. on Image Processing (ICIP'98). Los Alamitos: IEEE Computer Society Press, 1998. 425-429.

[2] Kinoshita H. An image digital signature system with zkip for the graph isomorphism problem. In: Proc. of the IEEE Conf. on Image Processing (ICIP'96), Vol 3. Los Alamitos: IEEE Computer Society Press, 1996. 247(250.

[3] Gopalakrishnan K, Memon N, Vora P. Protocols for watermark verification: Multimedia and security. IEEE Multimedia, 2001,8(4): 66-70.

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

[5] Craver S. Zero knowledge watermark detection. In: Information Hiding: The 3rd Int'l Workshop. LNCS 1768, Berlin: Springer-Verlag, 2000. 101-116.

[6] Adelsbach A, Katzenbeisser S, Sadeghi AR. Watermark detection with zero-knowledge disclosure. ACM Multimedia Systems Journal, 2003,9(3):266-278.

[7] Adelsbach A, Katzenbeisser S, Sadeghi AR. Cryptography meets watermarking: Detecting watermarks with minimal or zero knowledge disclosure. In: Proc. of the European Signal Processing Conf. (EUSIPCO 2002). 2002. 446-449.

[8] Adelsbach A, Sadeghi R. Zero knowledge watermark detection and proof of ownership. In: Information Hiding: The 4th Int'l Workshop. LNCS 2137, Berlin: Springer Verlag, 2001. 273-287.

[9] Zou XX, Dai Q, Huang C, Li JT. Zero-Knowledge watermark verification protocols. Journal of Software, 2003,14(9):1645-1651 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1645.pdf

[10] 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.

[11] Bellare M, Goldreich O. On defining proofs of knowledge. In: Advances in Cryptology, Crypto'92. LNCS 740, Berlin: Springer-Verlag, 1993. 390-420.

[12] Goldreich O, Oren J. Definitions and properties of zero-knowledge proof systems. Journal of Cryptology, 1994,7(1):1-32.

[13] Pedersen TP. Non-Interactive and information-theoretic secure verifiable secret sharing. In: Advances in Cryptology, CRYPTO'91. Berlin: Springer-Verlag, 1991. 129-140.

[14] Fujisaki E, Okamoto T. A practical and provably secure scheme for publicly verifiable secret sharing and its applications. In: Advances in Cryptology?EUROCRYPT'98. LNCS 1403, Berlin: Springer-Verlag, 1996. 32-46.

[15] Pan CD, Pan CB. Elememtary Number Theory. Beijing: Peking University Press, 1992 (in Chinese).

[16] Song YY. Number Theory for Computing. Berlin: Springer-Verlag, 2000.

[17] Bach E. Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms. Cambridge: MIT Press, 1985.

[18] Goldreich O. Foundations of Cryptography. Cambridge: Cambridge University Press, 2001.

[19] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In: Proc. of the1st ACM Conf. on Computer and Communications Security. New York: ACM Press, 1993. 62-73.

[20] Boudot F. Efficient proofs that a committed number lies in an interval. In: Advances in Cryptology, Eurocrypt 2000. LNCS 1807, Berlin: Springer-Verlag, 2000. 431-444.

[21] Ramkumar M, Akansu A. Image watermarks and counterfeit attacks: Some problems and solutions. In: Proc. of the Symp. on Content Security and Data Hiding in Digital Media. Newark: New Jersey Institute of Technology, 1999. 102-112.

附中文参考文献:

[9] 邹萧湘,戴琼,黄晟,李锦涛.零知识水印验证协议.软件学报,2003,14(9):1645-1651. http://www.jos.org.cn/1000-9825/14/1645.pdf

[15] 潘承洞,潘承彪.初等数论.北京:北京大学出版社,1992.