计算机应用 2012, 32(03) 669-678 DOI: 10.3724/SP.J.1087.2012.00669 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

视图的秘密分享及其代数编码方法

王晓京,方佳嘉,蔡红亮,王一丁

中国科学院 成都计算机应用研究所, 成都 610041

摘要: 视图的秘密分享是图像信息安全领域独具吸引力的研究问题。寻求秘密视图完全的(Perfect)和理想的(Ideal)门限秘密分享方案(也称图像门限分享的完备方案),则是其中富有挑战性的未决课题。文中引入灰度值域GF(2m)上像素矩阵秘密分享的新观点和相应的代数几何编码方法,实现了数字图像(t,n)门限秘密分享的一种完备方案。该方案能够将一幅或多幅秘密图像编码为n幅各具随机视觉内容,同时又共具(t,n)门限结构的影子图像(或称份额图像)。证明了这种秘密分享方案的(t,n)门限结构不仅是完全的而且也是理想的,并给出了提高像素灰度值域GF(2m)上图像秘密分享算法效率的“m位像素值的分拆与并行”方法。分析表明,该图像秘密分享方法可以应用于高安全等级的秘密图像的网络多路径传输、保密图像信息的分散式存储控制、高维图形码(Bar-code in k dimension)和弹出码(Popcode)等新一代信息载体技术的识读控制等各方面。

关键词: 图像分享 (t,n)门限 像素灰度值域GF(2m) 代数几何编码 m位像素值的分拆与并行

Secret image sharing and its algebraic coding method

WANG Xiao-jing, FANG Jia-jia, CAI Hong-liang, WANG Yi-ding

Chengdu Institute of Computer Applications, Chinese Academy of Sciences, Chengdu Sichuan 610041,China

Abstract: Image sharing is an attractive research subject in computer image information security field. Seeking for Perfect and Ideal image threshold secret sharing scheme (i.e. the complete image sharing scheme) is one of the unresolved challenging problems. By introducing into the methods of pixel matrix secret sharing over pixel value field GF(2m) and algebraic-geometry coding, a complete scheme of image sharing with a (t, n) threshold structure was achieved in this paper. The scheme could encode secret images into n shadow images in such a way that all the shadow images were in a Perfect and Ideal (t, n) threshold structure, while each shadow image had its own visual content assigned at random. This approach to image sharing was able to be applied to the new information carrier technology, e.g. network multipathed transmission of secret image in high security level, distributed storage control of secret image, bar-code in k dimension and Popcode. This paper also presented a method to cut down a great deal of computational time for image sharing based on a pixel field GF (2m), called "partition and paralleling of m-bit pixel".

Keywords: image sharing (t,n) threshold pixel value field GF(2m) algebraic-geometry coding partition and paralleling of m-bit pixel

收稿日期 2011-09-13 **修回日期** 2011-11-29 **网络版发布日期** 2012-03-01

DOI: 10.3724/SP.J.1087.2012.00669

基金项目:

国家863计划项目(2008AAO1Z402);中国科学院知识创新工程项目(2004CB18003)。

通讯作者: 方佳嘉

作者简介: 王晓京(1953-),男,安徽滁州人,研究员,博士,主要研究方向:编码与信息安全;方佳嘉(1985-),男,福建漳州人,博士研究生,主要研究方向:编码与信息安全;蔡红亮(1983-),男,山西临汾人,博士研究生,主要研究方向:编码与信息安全;王一丁(1983-),男,四川成都人,博士,主要研究方向:编码与信息安全。

作者Email: fjjcigar@163.com

参考文献:

[1]SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979,22(11): 612-613.

[2]BLAKLEY G R. Safeguarding cryptographic keys [C]// Proceedings of the National Computer Conference. New York : AFIPS, 1979: 313-317.

[3]DAWSON E, DONOVAN D. The breadth of Shamir's secret-sharing scheme[J]. Computer and Security, 1994, 13(1): 69-78.

[4]van DIJK M. On the information rate of perfect secret sharing schemes[J]. Designs, Codes and Cryptography, 1995, 6(2): 143-169.

[5]CHANG C C, HUANG R J. Sharing secret images using shadow codebooks[J]. Information Sciences, 1998, 111(1/2/3/4): 335-345.

[6]THIEN C C, LIN J C. Secret image sharing [J]. Computers & Graphics, 2002, 26(5): 765-770.

[7]NAOR M, SHAMIR A. Visual cryptography[C]// Proceedings of Eurocrypt '94. Berlin: Springer-Verlag, 1995: 1-12.

[8]ITO R, KUWAKADO H, TANAKA H. Image size invariant visual cryptography[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 1999, E82-A(10): 2172-2177.

[9]HOU Y C, LIN C F, CHANG C Y. Visual cryptography for color images without pixel expansion[J]. Journal of Technology, 2001, 16(4): 595-603.

[10]HOU Y C. Visual cryptography for color images[J]. Pattern Recognition, 2003, 36(7): 1619-1629.

[11]HOU YONGCHANG, DU SHUFEN. Visual cryptography tech-niques for color images without pixel expansion[J]. Journal of Information, Technology and Society, 2004, 109(1): 95-110.

[12]ZHOU Z, ARCE G R, CRESCENZO G D. Halftone visual cryptography[J]. IEEE Transactions on Image Processing, 2006, 15(8): 2441-2453.

[13]HOU YONGCHANG, LIN FANGZHU, ZHANG ZHAOYUAN. A new approach on 256 color secret image sharing technique[J]. MIS Review, 2000(9): 89-105.

[14]苏中民,林行良.图视秘密的任意分存[J].计算机学报,1996, 19(4): 293-299.

[15]ATENIESE G, BLUNDO C, de SANTIS A, et al. Constructions and bounds for visual cryptography [C]// ICALP'96: Proceedings of the 23rd International Colloquium on Automata, Languages and Programming, LNCS 1099. Berlin: Springer-Verlag, 1996: 416-428.

[16]ATENIESE G, BLUNDO C, de SANTIS A, et al. Visual cryptography for general access structures[J]. Information and Computation, 1996, 192(2): 86-106.

[17]ATENIESE G, BLUNDO C, de SANTIS A, et al. Extended capabilities for visual cryptography[J]. Theoretical Computer Science, 2001, 250(1/2): 143-161.

[18]BLUNDO C, de BONIS A, de SANTIS A. Improved schemes for visual cryptography[J]. Designs, Codes and Cryptography, 2001, 24(3): 255-278.

[19]BLUNDO C, de SANTIS A. Visual cryptography schemes with perfect reconstruction of black pixels [J]. Computer & Graphics, 1998, 12(4): 449-455.

[20]BLUNDO C, de SANTIS A, NAOR M. Visual cryptography for grey level images[J]. Information Processing Letters, 2000, 75(6): 255-259.

[21]WANG DAOSHUN, ZHANG LEI, MA NING, et al. Two secret sharing schemes based on Boolean operations[J]. Pattern Recognition, 2007, 40(10): 277-278.

[22]SHYU S J. Efficient visual secret sharing scheme for color images[J]. Pattern Recognition, 2006, 39 (5): 866-880.

[23]CIMATO S, de PRISCO R, de SANTIS A. Probabilistic visual cryptography schemes[J]. The Computer Journal, 2006,49(1): 97-107.

[24]YANG C-N. New visual secret sharing schemes using probabilistic method[J]. Pattern Recognition Letters, 2004, 25(4): 481-494.

[25]TSAI C-S, CHANG C-C. A generalized secret image sharing and recovery scheme[C]// Proceedings of the 2nd IEEE Pacific Rim Conference on Multimedia, LNCS 2195. Berlin: Springer-Verlag, 2001:963-968.

[26]LIN T. An image-sharing method with user-friendly shadow images[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(12): 1161-1169.

[27]WU Y-S, THIEN C-C, LIN J-C. Sharing and hiding secret images with size constraint[J]. Pattern Recognition, 2004, 37(7): 1377-1385.

[28]CHANG C-C, LIN C-C, LIN C-H, et al. A novel secret image sharing scheme in color images using small shadow images[J]. Information Sciences: an International Journal, 2008, 178(11): 2433-2447.

[29]TSAI C-S, CHANG C-C, CHEN T-S. Sharing multiple secrets in digital images[J]. Journal of Systems and Software, 2002, 64(2): 163-170.

[30]FENG J-B, WU H-C, TSAI C-S, et al. A new multi-secret images sharing scheme using Largrange's interpolation[J]. Journal of Systems and Software, 2005, 76(3): 327-339.

[31]WANG R-Z, SU C-H. Secret image sharing with smaller shadow images[J]. Pattern Recognition, 2006, 27(6): 551-555.

[32]ALVAREZ G, ENCINAS A A, ENCINAS L H, et al. A secure scheme to share secret color images[J]. Computer Physics Communications, 2005, 173(1/2): 9-16.

[33]THIEN C-C, FANG W-P, LIN J-C. Sharing secret images by using base-transform and small-size host images[J]. International Journal of Computer Science and Network Security, 2006, 6(6): 219-225.

[34]MASSEY J L. Minimal codewords and secret sharing[C]// Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory. Piscataway, NJ: IEEE Press, 1993: 276-279.

[35]BLAKLEY G R, KABATIANSKI G A. Ideal perfect threshold schemes and MDS codes [C]// ISIT'95: Proceedings of IEEE International Symposium on Information Theory. Piscataway, NJ: IEEE Press, 1995: 488.

[36]McELIECE R J, SARWATE D V. On sharing secrets and Reed-Solomon codes[J]. Communications of the ACM, 1981, 24(9): 583-584.

[37]MacWILLIAMS F J, SLOANE N J A. The theory of error-correcting code[M]. New York: North-Holland Publishing Company, 1977.

[38]LIN S, COSTELLO D. Error control coding[M]. Englewood Cliffs, NJ: Prentice-Hall, 1983.

[39]HOHOLDT T, van LINT J H, PELLIKAAN R, et al. Algebraic geometric codes[J]. IEEE Transactions on Information Theory, 1998, 44(6).

[40]WU H-C, WANG H-C, YU R-W. Color visual cryptography scheme using meaningful shares[C]// ISDA'08: Proceedings of the 8th International Conference on Intelligent Systems Design and Applications. Piscataway, NJ: IEEE Press, 2008: 173-178.

[41]CHANG C-C, LIN I-C. A new (t,n) threshold image hiding scheme for sharing a secret color image [C]// ICCT 2003: International Conference on Communication Technology Proceedings. Piscataway, NJ: IEEE Press, 2003: 196-202.

[42]KATEZENBEISSER S, PETITCOLAS F. Information hiding techniques for steganography and digital watermarking[M]. London: Artech House, Inc., 2009.

[43]CHANG C C, LIN M H, HU Y C. A fast and secure image hiding scheme based on LSB substitution [J]. International Journal of Pattern Recognition and Artificial Intelligence, 2002, 16(4): 399-416.

[44]ZHOU W, BOVIK A C, SHEIKH H R, et al. Image quality assessment: From error visibility to

structural similarity[J]. IEEE Transactions on Image Processing, 2004,13(4): 600-612.

[45]RUDOLF L, HARALD N. Finite fields[M]. 2nd ed. Cambridge: Cambridge University Press, 1997.

[46]SHEIKH H R, BOVIK A C. Image information and visual quality[J]. IEEE Transactions on Image Processing, 2006, 15(2): 430-444.

[47]BOSE R. Information theory, coding and cryptography[M]. Singapore: McGraw-Hill, 2003.

[48]郝柏林.从抛物线谈起:混沌动力学引论[M].上海: 上海科技出版社, 1993.

本刊中的类似文章

1．罗捷 严飞 余发江 张焕国.可信计算平台模块密码机制研究[J]. 计算机应用, 2008,28(8): 1907-0911

2．符晓芳 张福金 王鸿绪.基于(tx, fx)扩展的Vague集之间的相似度量及其应用[J]. 计算机应用, 2008,28(6): 1595-1597

3．殷凤梅 侯整风.可选子密钥的门限多秘密共享方案[J]. 计算机应用, 2007,27(9): 2187-2188

4．杨曦 侯整风.一种可定期更新的多秘密共享方案[J]. 计算机应用, 2007,27(7): 1609-1610

5．叶永飞 余梅生.基于簇结构的Ad Hoc网络安全密钥管理方案[J]. 计算机应用, 2007,27(3): 611-613

6．李彬;郝克刚.一种基于双线性配对的可验证秘密分享方案[J]. 计算机应用, 2006,26(4): 809-811