像素不扩展视觉密码的边缘增强研究

胡 浩 郁 滨 沈 刚
(信息工程大学 郑州 450004)

摘 要 针对像素不扩展视觉密码的边缘恢复失真问题,在分析图像边缘特征的基础上,通过构造LP算子,设计了一种具有可变膨胀倍数的边缘增强算法,并给出了边缘增强的像素不扩展视觉密码方案的设计方法。实验结果表明,该方法有效地改善了边缘的恢复质量,并显著提高了整幅图像的视觉效果。

关键词 视觉密码,像素不扩展,边缘检测,边缘增强
中图法分类号 TP309.7 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.2.022

Edge Enhancement on Size Invariant Visual Cryptography

HU Hao YU Bin SHEN Gang
(PLA Information Engineering University, Zhengzhou 450004, China)

Abstract Considering the problem of edge distortion in size invariant visual cryptography, on the basis of analyzing the characteristics of the image edge, an LP operator was proposed to design an edge enhancement algorithm with variable edge expansion ratio, and the method to design edge enhancement size invariant visual cryptography was given. The experimental results show that the quality of recovery edge can be improved effectively. Furthermore, the whole image can also be significantly improved with better visual effects.

Keywords Visual cryptography, Size invariant, Edge detection, Edge enhancement

1 引言

像素不扩展视觉密码(Size Invariant Visual Cryptography, SIVCS)[1-16]的优势在于恢复图像的像素扩展度 $m=1$,共享份及恢复图像在面积尺寸上与原始秘密图像保持一致,有效减小了共享份与恢复图像的传输及存储开销。典型不扩展视觉密码方案有基于概率法[1,2]、多点加密法[3-7]和随机栅格[8-16]方法。

Ryo等[1]首次提出基于概率法的像素不扩展视觉密码方案(Probabilistic Size Invariant Visual Cryptography Scheme, PVCS),其通过随机选取基矩阵 B_0(B_1)(Basis Matrices)的一列来分享一个原始像素。Yang等[2]在此基础上给出了像素不扩展的(k,n)门限视觉密码方案的一般构造方法,其分享算法和Ryo在本质上是相同的。此类方案对于图像的边缘区域,采用 B_0 进行分享,导致边缘黑像素按白像素的分享算法进行加密、无法产生对比效果,进而影响了边缘区域的恢复。

Hou等[3]提出多点加密的像素不扩展视觉密码方案(Multi-pixel Encryption Size Invariant Visual Cryptography Scheme, MEVCS),实现了在两个参与者之间分享一幅秘密图像。此后,Chen等[4]将多点加密法进一步扩展到(k,n)门限结构,Lin等[5]提高了分享秘密图像的数量,实现了对两幅图像的分享。Yu等[6]通过改变加密方式,采用多点加密、多行扫描的方法解决了恢复图像颗粒较大的问题。Liu等[7]设计了改进的MEVCS,解决了尖锐图像恢复后存在的细线问题。上述方案都不同程度地改善了秘密图像的恢复效果,但由于多点加密法在分享时选取连续的 m 个白(黑)像素,利用基础矩阵 B_0(B_1)的一行来加密,对于边缘交界处的像素采用 B_0 或者 B_1 的部分列进行加密,在边缘密集的区域内不能产生对比效果,导致图像边缘产生粘连等问题。

Kafri等[8]提出了一种基于随机栅格的图像秘密共享方案,Shyu[9]结合这种思想,基于随机栅格设计了两种分享灰度和彩色秘密图像的像素不扩展视觉密码方案(Random Grids Based Size Invariant Visual Cryptography Scheme, RGS),在加密时不需要基矩阵,利用函数 f_{equ},f_{man} 和 f_{com} 设计分享算法,通过随机数生成共享份,减小了基矩阵的存储开销。此后,Shyu[10]、Chen等[11,12]和文献[13]依次提出了存取结构为$(2,n)$,(n,n),(k,n)和GAS(General Access Structures)的RGS的构造方法。Fu等[14]设计了随机栅格到基矩阵 B_0(B_1)的变换,指出RGS是PVCS的基矩阵 B_0(B_1)的算法表示。因此,RGS本质上是PVCS的一个特例,没有结合图像高频区域的特征进行研究,同样存在着边缘区域恢复效果不佳的问题。

综上所述,图像边缘恢复质量不佳直接影响整幅图像的恢复效果,因此增强边缘的恢复质量是不扩展视觉密码的一个重要问题。本文构造二阶微分LP算子,并设计了一种具

到稿日期:2014-03-23 返修日期:2014-06-03 本文受国家自然科学基金(61070086),信息保障技术重点实验室开放基金(KJ-13-107)资助。
胡 浩(1989—),男,硕士生,主要研究方向为视觉密码,E-mail:wjjhh_908@163.com;郁 滨(1964—),男,教授,博士生导师,主要研究方向为视觉密码和网络安全;沈 刚(1986—),男,博士生,主要研究方向为视觉密码。

有可变边缘膨胀倍数的边缘增强算法，在此基础上给出边缘增强的像素不扩展视觉密码(Edge Enhancement Size Invariant Visual Cryptography，ESIVCS)的一般构造方法。实验结果表明，本方法显著提高了不扩展视觉密码方案的恢复效果。

2 图像边缘检测

边缘是指图像周围黑白像素有阶跃变化或屋顶状变化的像素的集合，是图像局部强度变化最显著的部分，如图 1 所示。边缘存在于目标与背景、目标与目标、区域与区域、基元与基元之间，包含了丰富的信息(如方向、阶跃、形状等)，是图像的一种基本特征，能勾画出图像的轮廓，提高对图像信息的识别能力。边缘检测的实质是通过设计算法提取出图像中黑色对象与白色背景间的交界线，由于边缘存在于黑白像素相邻区域之间，是黑白像素不连续(或突变)的结果，这种不连续性可利用图像的一阶或二阶导数方便地检测出来[19]。本文利用二阶导数方向不变性原理，构造了一种 4 邻域系统 LP 算子。具体方法是用算子模板作为核与该图像中的每个像素点做卷积和运算，输出结果可以用来判别图像的边缘。卷积运算是一种邻域运算，图像中某一像素点的运算结果不但与本像素灰度值有关，而且与其邻域像素点灰度有关。运用模板对图像上的每个像素依此进行卷积，即模板上每一个点的值与其在图像上当前位置对应的像素点值相乘后再相加[19]，具体构造原理如下。

图 1 图像及其边缘

设 S 为 $w\times h$ 的秘密图像，$S=\{S_{i,j}\mid S_{i,j}\in\{0,1\}\}$，其中 $0\leqslant i\leqslant h-1, 0\leqslant j\leqslant w-1$，像素点 $S_{i,j}$ 的二阶微分标量为 $\nabla^2 S(i,j)$。

引理 1[19] 对于一幅二值图像，当 $\nabla^2 S(i,j)>0$ 时，像素点 $S_{i,j}$ 被认定为边缘像素。

定理 1 构造算子模板如式(1)所示，对于一个像素点 $S_{i,j}$，与 LP 算子的卷积和 $LP(S(i,j))>0$ 时，被认定为边缘像素。

$$\begin{bmatrix}0 & 1 & 0\\ 1 & -4 & 1\\ 0 & 1 & 0\end{bmatrix} \tag{1}$$

证明：利用算子对像素点 $S_{i,j}$ 做卷积和运算，结果如下：

$$LP(S(i,j))=\begin{bmatrix}0 & 1 & 0\\ 1 & -4 & 1\\ 0 & 1 & 0\end{bmatrix}*\begin{bmatrix}0 & S(i,j+1) & 0\\ S(i-1,j) & S(i,j) & S(i+1,j)\\ 0 & S(i,j-1) & 0\end{bmatrix}$$
$$=S(i+1,j)+S(i-1,j)+S(i,j+1)+S(i,j-1)-4S(i,j)$$

$S_{i,j}$ 对 i 方向上的二阶偏导数如下：

$$\frac{\partial^2 S(i,j)}{\partial i^2}=\frac{\partial(S[i+1,j]-S[i,j])}{\partial i}=\frac{\partial S[i+1,j]}{\partial i}-\frac{\partial S[i,j]}{\partial i}$$
$$=S[i+1,j]-2S[i,j]+S[i-1,j] \tag{2}$$

类似地：

$$\frac{\partial^2 S(i,j)}{\partial j^2}=S[i,j+1]-2S[i,j]+S[i,j-1] \tag{3}$$

因此：

$$LP(S(i,j))=\frac{\partial^2 S(i,j)}{\partial i^2}+\frac{\partial^2 S(i,j)}{\partial j^2}=\nabla^2 S(i,j) \tag{4}$$

结合引理 1 可知，当 $LP(S(i,j))>0$ 时，像素 $S_{i,j}$ 被认定是边缘像素。

3 ESIVCS 设计

本节首先结合 LP 算子设计一种具有可变膨胀倍数 β 的边缘增强算法，在此基础上，给出了 ESIVCS 的秘密分享与恢复流程。

3.1 边缘增强算法

边缘增强算法利用 LP 算子检测边缘像素，连接边缘像素构成秘密图像的轮廓，将边缘像素延梯度方向延拓 β 倍，β 是边缘膨胀倍数，且 $\beta=0,1,2\cdots n$，膨胀后的图像与原始图像相比，其边缘增加了 β 圈黑像素，在此基础上，提取出边缘像素集合 $\{E_{i,j}\mid i\in(0,1,\cdots,h-1), j\in(0,1,\cdots,w-1)\}$。边缘增强的基本思想是通过对加密图像进行前期预处理，突出边缘的特征，使恢复图像的轮廓更加清晰，算法流程如图 2 所示，具体步骤如下。

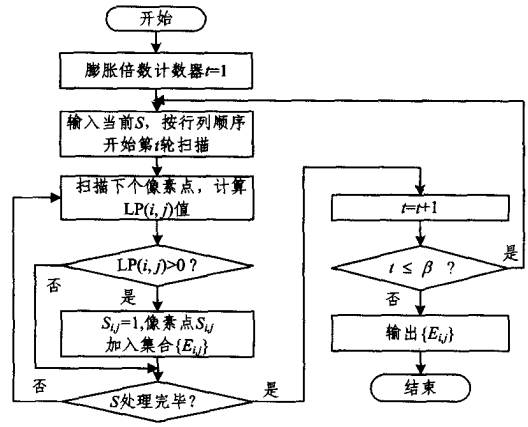


图 2 边缘提取流程

算法输入：大小为 $w\times h$ 的秘密图像 S，边缘膨胀倍数 β。

算法输出：边缘像素集合 $\{E_{i,j}\}$。

Step1 设定膨胀倍数 β，初始化膨胀计数变量 $t=1$；

Step2 输入当前的 S，开始第 t 轮扫描；

Step3 按行列顺序依次扫描秘密图像 S 的每个像素 $S_{i,j}$，统计其 4 邻域像素点的值；

Step4 判断 $LP(i,j)>0$ 是否成立，若是，则 $S_{i,j}=1$，同时将像素 $S_{i,j}$ 加入集合 $\{E_{i,j}\}$ 中，否则结束；

Step5 判断当前像素是否为整幅图像最后一个像素，若是，则令 $t=t+1$，结束该步，否则转到 Step3；

Step6 判断 $t\leqslant\beta$ 是否成立，若是，则转到 Step2，否则算法结束，输出 $\{E_{i,j}\}$。

需要说明的是，针对不同的秘密图像，由于内容复杂程度不同，对于不同的膨胀倍数 β，恢复图像的效果也不一样，可以根据反馈的恢复效果来确定 β 值，并生成方案共享份。

3.2 秘密分享与恢复流程

在秘密分享流程图中，有两点需要说明：

(1)基矩阵 B_0，B_1 的构造是采用其它文献的结果，不是本文的研究重点。本文主要针对现有方案，结合方案的基矩阵并通过 ESIVCS 设计来增强秘密图像的恢复效果。

(2)由于边缘提取算法是在加密前对秘密图像 S 进行预处理，且视觉密码方案的有效性是基于 B_0 和 B_1 的，因此不影响原方案的可行性。

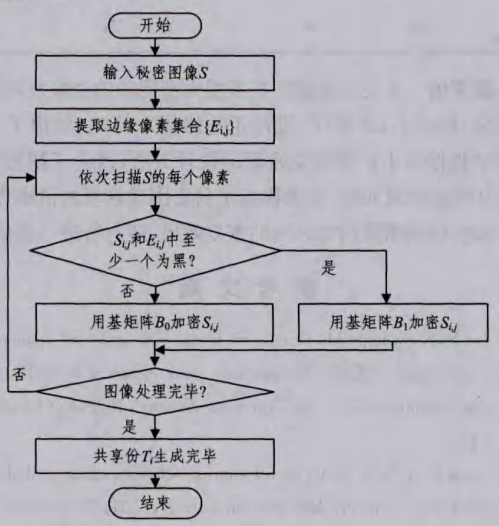


图 3 秘密分享流程

在恢复秘密图像时，只需将共享份简单地叠加即可，如图 4 所示，在恢复秘密图像时，有效的参与者叠加各自的共享份。

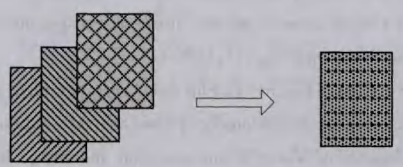
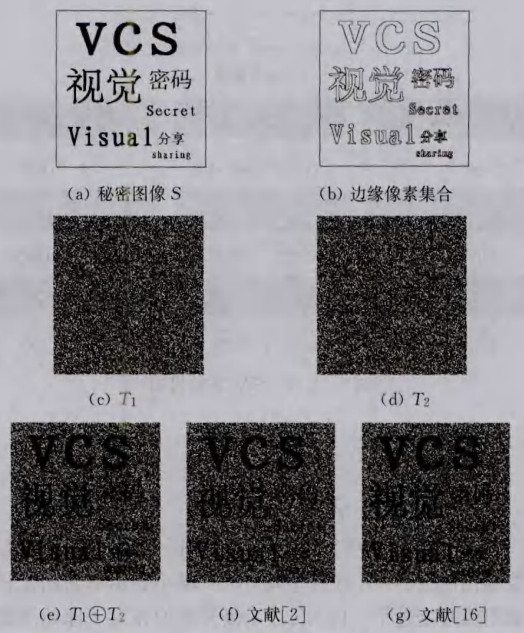


图 4 秘密恢复流程

4 实验分析

4.1 方案有效性分析

以(2,2)方案为例，结合文献[2]的分享算法，验证本文方法的有效性，其中基矩阵 $B_0=\begin{bmatrix}1&0\\1&0\end{bmatrix}$，$B_1=\begin{bmatrix}1&0\\0&1\end{bmatrix}$，设定 $\beta=1$，按照上一节的设计流程，图 5 给出了本文方案和文献[2,16]的实验效果对比。从图中可以看出，共享份(图 5(c)－(d))是杂乱无章的，从中无法得到秘密图像的任何信息。从恢复图像(图 5(e))中能够利用视觉系统分辨出原始图像的信息(图 5(a))，与预期结果相同，因此方案有效。同时可以看出，相比原方案[2]，本方案的细节恢复效果更加清晰；相比另一种边缘增强方案[16]，本方案秘密恢复图像的轮廓相对清楚，例如，恢复字样“密码”更加清晰。



(a) 秘密图像 S　(b) 边缘像素集合

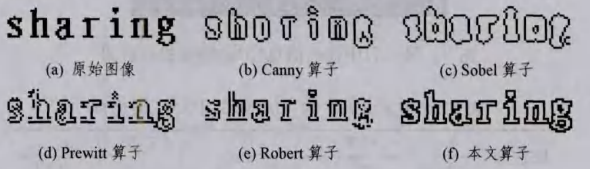
(c) T_1　(d) T_2

(e) $T_1 \oplus T_2$　(f) 文献[2]　(g) 文献[16]

图 5 本文与其他方案的实验效果比较

4.2 LP 算子分析

提取图 5(a)中的‘sharing’图案(82×25pixels)，利用 LP 算子与其他典型边缘检测算子[19]进行实验，图 6 给出了实验效果比较，表 1 给出了图 6 中各算子的边缘检测精度统计分析结果，其中原始图像边缘像素点个数通过统计分析图像矩阵得到。



(a) 原始图像　(b) Canny 算子　(c) Sobel 算子

(d) Prewitt 算子　(e) Robert 算子　(f) 本文算子

图 6 本文与其他算子的边缘检测效果比较

表 1 边缘检测精度比较

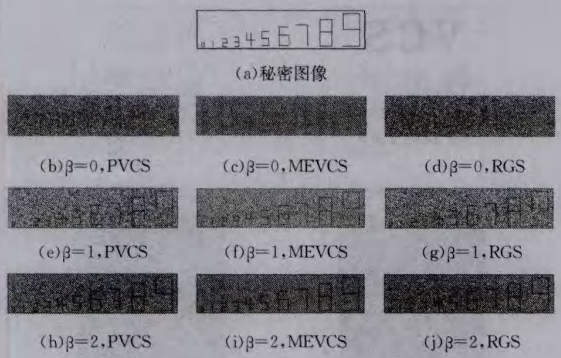
	Canny 算子	Sobel 算子	Prewitt 算子	Robert 算子	本文算子	原始图像
边缘像素个数	267	285	306	320	398	441
边缘完整率	60.5%	64.7%	69.4%	72.6%	87.1%	100%

综合分析实验结果可知，其他算子(见图 6(b)－(e))对于二值图像检测精度不高，边缘不连续，文献[16]中的 Robert 算子的精度为 72.6%，检测边缘不够完整(见图 7(e))，导致恢复图像不清晰(见图 5(g))。相比而言，本文算子的精度高达 87.1%，显示轮廓更加完整(见图 6(f))，对应恢复图像清晰(见图 5(e))。

在计算复杂度方面，对于分享一个尺寸为 $w\times h$ 的秘密图像 S，原分享算法需要 $w\times h$ 次运算，本文算法对每个像素点用 LP 算子进行检测时需要 8 次加运算和 1 次比较运算，对于分享整幅图像则需要增加 $9\cdot(w\times h)$ 次运算。因此，对秘密图像进行预处理会给分享过程增加额外的计算开销，但不会增加原分享算法计算复杂度的阶数。

4.3 边缘增强效果分析

本文方法适用于任意存取结构，且不受分享函数类型限制。为方便说明，设秘密图像 S 是一幅显示“0－9”的数字图像(见图 7(a))，图 7 给出了 3 种典型 ESIVCS[2,3,9]的实验效果。



(a)秘密图像

(b)β=0,PVCS (c)β=0,MEVCS (d)β=0,RGS

(e)β=1,PVCS (f)β=1,MEVCS (g)β=1,RGS

(h)β=2,PVCS (i)β=2,MEVCS (j)β=2,RGS

图 7　3 种 ESIVCS 效果图

$$MSE=\frac{1}{w\times h}\sum_{x=1}^{w}\sum_{y=1}^{h}(S(i,j)-R(i,j))^2$$

$$PSNR=10\times\lg\frac{1}{MSE}$$

MSE 用来评价恢复图像相比原始图像的失真程度，是对图像变化情况的一个统计平均，MSE 越小表示解密图像相对于原图像改变越小。PSNR 表示恢复图像相对于原始图像的增益大小，增益越大，表示图像的噪声越小，恢复效果越好，本文用边缘的失真程度来描述边缘的恢复质量。图 7 中 3 种 ESIVCS 的秘密恢复图像边缘区域的 MSE 和 PSNR 值比较如表 2 所列。为方便描述，图 8 以图 7(f)为例，给出了秘密图案'0'的边缘区域提取效果。

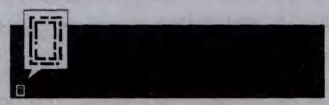


图 8　图 7(f)中秘密信息'0'的边缘提取效果

表 2　3 种 ESIVCS 的边缘 MSE、PSNR 值比较

ESIVCS	MSE			PSNR(dB)		
	β=0	β=1	β=2	β=0	β=1	β=2
PVCS	0.0259	0.0127	0.0019	15.8587	18.9699	27.1917
MEVCS	0.0237	0.0118	0.0002	16.2494	19.2708	37.9897
RGS	0.0258	0.0125	0.0019	15.8838	19.0390	27.2025

综合分析图 7 和表 2 的实验结果可知：

(1)对同一种 ESIVCS，随着膨胀倍数 β 的增加，MSE 逐渐减小，PSNR 逐渐增大，边缘失真程度减小，对应图 7 中恢复图像逐渐清晰。

(2)对于不同 ESIVCS，当 β 相同时，MEVCS 的 MSE 较小，PSNR 较大，而 PVCS 和 RGS 的 MSE 和 PSNR 相差不大，对应图 7 中，MEVCS 的恢复效果更清晰，而 PVCS 及 RGS 的恢复效果相似；当 $\beta=0$ 时，方案退化成文献[2,3,9]的结果，此时边缘失真严重，恢复效果模糊如图 7(b)－(d)所示；当 $\beta=2$ 时，3 种 ESIVCS 的 MSE 接近于 0，边缘失真最小，对应图7(h)－(j)的轮廓清晰，整幅图像恢复效果好，秘密信息识别能力强。

4.4　方案适用性分析

在评价一个视觉密码方案时，像素扩展度和对秘密图像的识别能力是两个关键参数，同时方案所适用的存取结构以及构造的关键技术也是重要的性能指标。本文方案与其他视觉密码方案的比较如表 3 所列。从表中可以看出，在像素扩展度方面，文献[1,2]存在像素扩展。在存取结构方面，在像素不扩展的前提下，仅文献[13]和本文方案适用于 GAS 结构。在关键技术方面，只有本文方案构造不受限于 VC 或者 RG，因此应用范围更广。在恢复图像的视觉效果方面，仅文献[16]和本文方案对秘密图像的识别能力进行了增强，但文献[16]只限制于(2,2)门限结构，而本方案适用 GAS 结构。

表 3　本文方案与其他方案的比较

参数	文献[17]	文献[18]	文献[2]	文献[16]	文献[12]	文献[13]	本文方案
存取结构	(k,n)	(k,n)	(k,n)	(2,2)	(k,n)	GAS	GAS
关键技术	VC	VC	VC	RG	RG	RG	VC RG
像素扩展度	$2^{k-1}\binom{n}{k}$	$\frac{2(n-k+1)}{n}$	1	1	1	1	1
识别增强	N	N	N	Y	N	N	Y

结束语　本文对像素不扩展视觉密码的边缘恢复问题展开研究，构造了 LP 算子，设计了边缘提取算法，给出了一种边缘增强像素不扩展视觉密码的设计方法，改善了秘密图像边缘区域的恢复质量，显著提高了秘密图像恢复的清晰程度。对于如何增强图像内部区域的恢复效果，还有待进一步研究。

参 考 文 献

[1] Ito R, Kuwakado H, Tanaka H. Image size invariant visual cryptography[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, 1999, 82(10): 2172-2177

[2] Yang C N. New visual secret sharing schemes using probabilistic method[J]. Pattern Recognition Letters, 2004, 25: 481-494

[3] Hou Y C, Tu S F. A visual cryptography technique for chromatic images using multi-pixel encoding method[J]. Journal of Research and Practice in Information Technology, 2005, 37(2): 179-191

[4] Chen Y F, Chan Y K, Huang C C, et al. A multiple-level visual secret-sharing scheme without image size expansion[J]. Information Sciences, 2007, 177: 4696-4710

[5] Lin S J, Chen S K, Lin J C. Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast and no expansion [J]. Journal of Visual Communication and Image Representation, 2010, 21(8): 900-916

[6] 郁滨，王翠. 像素不扩展的 MSM 视觉密码方案[J]. 信息工程大学学报，2007，8(2)：156-160

[7] Liu F, Guo T, Wu C K, et al. Improving the visual quality of size invariant visual cryptography scheme[J]. Journal of Visual Communication and Image Representation, 2012, 23: 331-342

[8] Kafri O, Keren E. Encryption of pictures and shapes by random grids[J]. Optics Letters, 1987, 12(6): 377-379

[9] Shyu S J. Image encryption by random grids[J]. Pattern Recognition, 2007, 40: 1014-1031

[10] Shyu S J. Image encryption by multiple random grids[J]. Pattern Recognition, 2009, 42: 1582-1596

[11] Chen T H, Tsao K H. Visual secret sharing by random grids revisited[J]. Pattern Recognition, 2009, 42: 2203-2217

[12] Chen T, Tsao K. Threshold visual secret sharing by random grids[J]. The Journal of Systems and Software, 2011, 84: 1197-1208

[13] Shyu S J. Visual Cryptograms of Random Grids for General Access Structures[J]. Circuits and Systems for Video Technology, 2013,23(3):414-424

[14] Fu Z X, Yu B. Visual Cryptography and Random Grids Schemes [C]// Poceedings of 12th International Workshop on Digital-Forensics and Watermarking. CBD Auckland, New Zealand, Oct 2013:109-122

[15] Wu X T, Sun W. Improving the visual quality of random grid-based visual secret sharing[J]. Signal Processing, 2013, 93(5): 977-995

[16] Chen T H, Lee Y S. A New Random-grid-based Visual Secret Sharing by Edge Enhancement[J]. Journal of Computational Information Systems, 2012, 8(4): 1507-1513

[17] Tuyls P, Hollmann H D L, Lint J H V, et al. XOR-based visual cryptography schemes[J]. Designs, Codes and Cryptography, 2005, 37(1): 169-186

[18] Chao K Y, Lin J C. Secret image sharing: A Boolean operations based approach combining benefits of polynomial-based and fast approaches[J]. International Journal of Pattern Recognition and Artificial Intelligence, 2009, 23(2): 263-285

[19] [美]冈萨雷斯, 等. 数字图像边缘检测(第二版)[M]. 阮秋琦等译. 北京: 电子工业出版社, 2007: 460-479

(上接第 99 页)

点,在签名置入过程和签名验证过程中,标签端仅需两种简单的比特位运算(模 2^m 加(mod 2^m(+))和比特位异或(XOR))以及伪随机数产生(PRNG)[9]操作,这 3 种操作均符合低代价被动 RFID 标签的轻量级运算能力[17]。此外,将计算代价相对较高的盲化操作、脱盲操作以及签名验证操作置于阅读器端进行,由签名发行端执行前向安全盲签名算法[16](FSWBS),在实现轻量级标签运算的同时恰当地控制了整个 RFID 系统的开销。因此,FSWBLAP 协议是利用公钥密码技术实现低代价 RFID 标签轻量级认证的有效方案,适合应用于供应链管理、无线信用卡、电子护照(E-passport)、电子不停车收费系统(ETC)以及电子票(E-ticket)等商业、工业和民用等应用领域的轻量级 RFID 安全访问控制系统以及轻量级 RFID 认证系统,在此应用领域中被动低代价轻量级 RFID 标签需符合 EPC Class-1 Gen-2 标准,能够执行少量等价逻辑门运算和伪随机数产生操作(PRNG)[9]。

结束语 为了解决公钥密码技术大量的计算开销难以实现低代价 RFID 标签的轻量级认证问题,本文提出了一种基于数字签名方案的轻量级 RFID 认证协议(FSWBLAP),其利用数字签名技术成功实现了 RFID 系统的轻量级认证机制。FSWBLAP 协议的突出优势是恰当转化公钥密码技术中代价较高运算的执行位置,在加强 RFID 系统安全性和鲁棒性的同时,成功降低了标签端的计算开销,满足了资源受限设备的轻量级运算需求,其安全性建立在有限域上的离散对数困难问题和伪随机生成器的基础之上。

参 考 文 献

[1] Schneider M. Radio frequency identification (RFID) technology and its applications in the commercial construction industry[D]. University of Kentucky, 2003

[2] Chawla V, Dong-Sam H. An overview of passive RFID[J]. Communications Magazine, IEEE, 2007, 45(9): 11-17

[3] Roussos G, Kostakos V. rfid in pervasive computing: State-of-the-art and outlook[J]. Pervasive and Mobile Computing, 2009, 5(1): 110-131

[4] Want R. The Magic of RFID[J]. Queue, 2004, 2(7): 40-48

[5] Juels A. RFID security and privacy: a research survey[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 381-394

[6] Hlavá č. Known-Plaintext-Only Attack on RSA-CRT with Montgomery Multiplication[C]// Cryptographic Hardware and Embedded Systems(CHES 2009). Springer, 2009: 128-140

[7] Nithyanand R. The evolution of cryptographic protocols in electronic passports: Cryptology ePrint archive[R]. Report 2009/200

[8] Yanjun Z. Survivable RFID Systems: Issues, Challenges, and Techniques[J]. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 2010, 40(4): 406-418

[9] Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, et al. LAMED-A PRNG for EPC Class-1 Generation-2 RFID specification[J]. Comput. Stand. Interfaces. , 2009, 31(1): 88-97

[10] Batina L, Guajardo J, Kerins T, et al. Public-Key Cryptography for RFID-Tags[C]// Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, 2007(PerCom Workshops'07). 2007: 217-222

[11] McLoone M, Robshaw M J B. New Architectures for Low-Cost Public Key Cryptography on RFID Tags[C]// IEEE International Symposium on Circuits and Systems, 2007(ISCAS 2007). 2007: 1827-1830

[12] Hoffstein J, Howgrave-Graham N, Pipher J, et al. NTRUSign: Digital Signatures Using the NTRU Lattice[C]// Joye M, ed. Topics in Cryptology(CT-RSA 2003). Springer Berlin Heidelberg, 2003: 122-140

[13] Hutter M, Feldhofer M, Plos T. An ECDSA Processor for RFID Authentication[C]// Yalcin S O, ed. Radio Frequency Identification: Security and Privacy Issues. Springer Berlin Heidelberg, 2010: 189-202

[14] Calmels B, Canard S, Girault M, et al. Low-Cost Cryptography for Privacy in RFID Systems[C]// Domingo-Ferrer J, Posegga J, Schreckling D, eds. Smart Card Research and Advanced Applications. Springer Berlin Heidelberg, 2006: 237-251

[15] Liang Y, Rong C. RFID System Security Using Identity-Based Cryptography[C]// Presented at the Proceedings of the 5th international conference on Ubiquitous Intelligence and Computing. Oslo, Norway, 2008: 482-489

[16] Liu Ya-li, Qin Xiao-lin, Li Bo-han. Forward-Secure Blind Signature Schemes Based on the Variants of ElGamal[J]. China Communications, 2010, 7(4): 58-64

[17] C Hung-yu. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity[J]. IEEE Transactions on Dependable and Secure Computing, 2007, 4 (4): 337-340