具有伪装图案的操作式多秘密视觉密码

付正欣 郁 滨 房礼国
(信息工程大学电子技术学院 郑州 450004)

摘 要 将环形共享份划分为伪装区域和秘密区域,结合(2,2)单秘密视觉密码方案的基础矩阵,设计了一种具有伪装图案的操作式多秘密视觉密码方案。该方案不仅能够分享任意数量的秘密图像,而且改善了同类方案的像素扩展度和相对差,更重要的是共享份呈现出有意义的伪装图案,从而降低了攻击者对共享份的威胁。

关键词 视觉密码,多秘密分享,环形共享份,伪装图案
中图法分类号 TP309.7 **文献标识码** A

Operation-based Multi-secret Visual Cryptography Scheme with Disguised Patterns

FU Zheng-xin YU Bin FANG Li-guo
(Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004, China)

Abstract The ring shares were divided into the disguised area and the tagged secret areas. Combining with the basic matrices of (2,2) single secret visual cryptography, an operation-based multi-secret visual cryptography scheme with disguised images was designed. The proposed scheme not only makes the number of secret images boundless, but also improves the pixel expansion and the relative difference of previous schemes. Furthermore, the meaningful disguised patterns can reduce the attackers' threats to shares.

Keywords Visual cryptography, Multi-secret sharing, Ring share, Disguised patterns

1 引言

视觉密码(Visual Cryptography)是一种新的秘密共享技术,它将图像分享至若干个共享份,恢复图像时只需将一定数目的共享份叠加即可。该技术具有"一次一密"[1]的安全性和秘密恢复的简单性,因此一经提出就引起广大学者的重视和研究兴趣[1-10]。多秘密视觉密码方案(Multi-secret Visual Cryptography Scheme)是视觉密码的一个重要研究内容,使每个参与者保存一个共享份即可恢复多个秘密。按照秘密恢复的方式,目前多秘密视觉密码主要包括以下两类方案:存取式(Access-based MVCS)和操作式(Operation-based MVCS)。

AMVCS通过不同的参与者集合来恢复不同的秘密图像。Yu等人[11]的方案中,任意 k 个参与者组成的集合只能恢复一个秘密图像,而任意 $k-1$ 个参与者可以根据不同的组合分享不同的秘密图像,因此最多可分享 $C(n,k-1)+1$ 个秘密图像。王道顺等人[12]对一般存取结构下的AMVCS进行了研究,得出了更具一般性的结论。OMVCS则通过共享份的旋转或平移等方法来实现多个秘密的分享。Chen等人[13]提出的一种方案将两个秘密图像 S_1 和 S_2 分享到两个共享份 A 和 B。恢复时,将两个共享份叠合可以恢复秘密 S_1,然后将共享份 B 旋转90°,180°或270°,再与 A 叠合,则得到秘密 S_2。Feng等人[14]在首尾相接的环形共享份的基础上,设计了4种分享模式,实现了恢复任意数量的秘密图像。

在一般的MVCS中,共享份是杂乱无章的。而在实际应用中,类似噪声的共享份容易引起攻击者的注意[1]。王道顺等人[15]研究了使共享份呈现伪装图案的EVCS(Extended VCS),并讨论了应用于AMVCS的情况。但由于AMVCS和OMVCS的设计方法不同,王的方案并不适用于OMVCS,因此具有伪装图案的OMVCS有待进一步研究。

本文将环形共享份划分为秘密区域和伪装区域,结合(2,2)单秘密视觉密码方案,设计了OMVCS的秘密分享与恢复流程,并证明了方案的有效性。本方案使共享份可以呈现出伪装图案,同时,方案的像素扩展度和相对差与无伪装图案的OMVCS相比有改善。

2 基本概念

不失一般性,设伪装图案为 D_1,D_2,秘密图像为 S_1,S_2,…,S_n,它们的大小一致,均为 $a\times b$,且 $b \bmod n\equiv 0$。在本方案中,共享份 A 和 B 都由 $a\times b$ 个子像素块组成,一个子像素块对应的所有图像在同一位置的一个像素。

定义1 每个子像素块用 $2\times(n+1)$ 的布尔矩阵来表示。记第一列2个像素为区域1,依次类推,直到区域 $n+1$。其中前 n 个区域称为秘密区域,第 $n+1$ 个区域称为伪装区域,如图1所示。

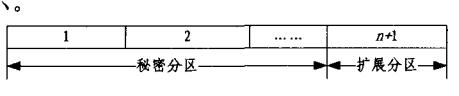


图1 子像素块的区域划分

每幅秘密图像的像素按列标记,具体如图2所示。

到稿日期:2010-07-16 返修日期:2010-11-09 本文受国家自然科学基金(61070086),河南省杰出青年科学基金(094100510002)资助。
付正欣(1986-),男,博士生,主要研究方向为视觉密码,E-mail:fzx2515@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。

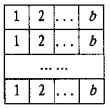


图 2　秘密图像的像素标记

共享份 A 和 B 的秘密区域都有各自的标记，每个区域 i ($1\leqslant i\leqslant n$)根据标记对应秘密图像 S_i 中的一个像素。在共享份 A 中，所有区域 i 的标记与 S_i 中的像素标记顺序一致，而在共享份 B 中，所有区域 i 的标记如图 3 所示。当 $i=1$ 时，共享份 B 区域 i 的标记与 S_i 中的像素标记顺序一致。

共享份各区域的标记由各秘密图像的标记决定，图 4 和图 5 是完全标记后的共享份 A 和 B。

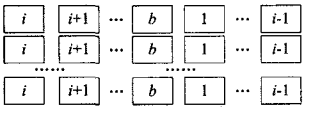


图 3　共享份 B 中所有区域 i 的标记

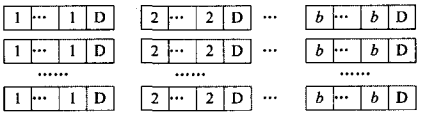


图 4　完全标记的共享份 A

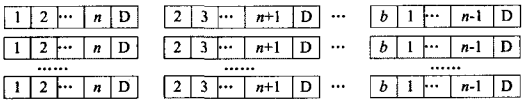


图 5　完全标记的共享份 B

其中 D 表示伪装区域。

定义 2　记 $R(B,i-1)$为循环右移函数，表示将共享份 B 以子像素块为单位，循环右移 $i-1$ 次($i(1\leqslant i\leqslant n)$)。

显然，$R(B,i-1)$与共享份 A 叠加时，两者在秘密区域 i 上的标记是一致的。

3　方案设计

本节设计了 OMVCS 的秘密分享和恢复流程，并对方案的有效性进行了证明。

3.1　秘密分享流程

秘密分享流程包括两部分：伪装区域和秘密区域的赋值。伪装区域的处理较为简单，而秘密区域则由对应秘密图像的像素决定。整个秘密分享的流程如图 6 所示。

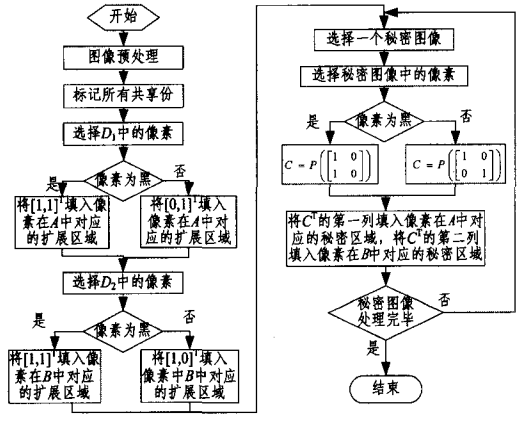


图 6　秘密分享流程图

图像预处理是指，若秘密图像的宽度 b 不能被秘密图像的数量 n 整除，需要对秘密图像的宽度进行扩充。$\begin{bmatrix}1&0\\1&0\end{bmatrix}$和$\begin{bmatrix}1&0\\0&1\end{bmatrix}$是(2,2)单秘密视觉密码方案的基础矩阵，$P(X)$表示对矩阵 X 进行随机列排序。

3.2　秘密恢复流程

与秘密分享相比，秘密恢复比较简单。在恢复秘密图像 S_i 时，旋转首尾相接的共享份 A 和 B，使两者的第 i 区域标记一致即可，如图 7 所示。

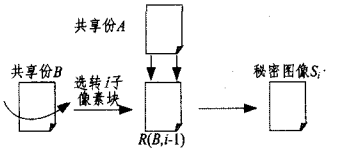


图 7　秘密恢复示意图

3.3　方案有效性证明

本方案的有效性包括安全性、伪装性和对比性。安全性是指单个共享份不会泄露秘密图像的信息；伪装性是指共享份呈现出指定的伪装图案；对比性则是指恢复的秘密图像可以被辨别。

由秘密分享流程可知，共享份的秘密区域均由 $P([0,1])^T$ 组成，与秘密图像的像素颜色无关，因此，通过单个共享份无法得到秘密图像的信息，即方案的安全性可以得到保证。

定理 1(伪装性)　共享份 A 和 B 分别呈现出伪装图案 D_1 和 D_2，且 A 和 B 叠加时伪装图案不会影响秘密图像的恢复。

证明：1)设 $v(1,A)(v(0,A))$分别表示伪装图案 D_1 中黑(白)像素对应的子像素块的汉明重量。由秘密分享流程可知，D_1 中黑像素对应的子像素块由 $2n$ 个 $P([0,1])^T$ 和 1 个 $[1,1]^T$ 组成，而 D_1 中白像素对应的子像素块则由 $2n$ 个 $P([0,1])^T$ 和 1 个$[0,1]^T$ 组成。因此，$v(1,A)-v(0,A)=2n+2-(2n+1)=1$，表示共享份 A 中子像素块的汉明重量随 D_1 中像素颜色的改变而不同，故共享份 A 会呈现 D_1 的图像。同理，共享份 B 会呈现 D_2 的图像。

2)由于共享份 A 中子像素块的伪装区域为$[c_A,1]^T$，共享份 B 中子像素块的伪装区域为$[1,c_B]^T$，其中 $c_A,c_B\in\{0,1\}$，因此，共享份 A 和 B 叠加后，所有伪装区域均变为$[1,1]^T$，故伪装图案不会影响秘密图像的恢复。

引理 1　当共享份 A 和旋转后的共享份 B 叠加时，若二者秘密区域 i 的标记不一致，那么叠加后所有秘密区域 i 的汉明重量期望为 3/2。

证明：由秘密分享流程可知，秘密区域 i 的标记与秘密图像 S_i 的标记一一对应，故 A 和 B 秘密区域 i 的标记不一致表示 2 个秘密区域对应的像素标记不同。不妨设 A 的秘密区域 i 为$[0,1]^T$，无论 2 个秘密区域 i 对应的像素颜色是否相同，根据基础矩阵的随机列排序特性，B 的秘密区域 i 以 1/2 的概率为$[0,1]^T$，以 1/2 的概率为$[1,0]^T$，因此 A 和 B 叠加后，秘密区域 i 的汉明重量的期望为 3/2。

定理 2(对比性)　共享份 A 和 $R(B,i-1)$叠加后，可以恢复秘密图像 S_i。

证明：设 $w(0,i,j)(w(1,i,j))$表示共享份 A 和 $R(B,i-1)$叠加后秘密图像 S_i 中白(黑)像素对应的子像素块中区域 j 的汉明重量，$E[w(0,i,j)](E[w(1,i,j)])$表示共享份 A 和 R

$(B,i-1)$叠加后 S_i 中白(黑)像素对应的子像素块中区域 j 的汉明重量的期望值，$E[w(0,i,\Sigma)](E[w(1,i,\Sigma)])$表示共享份 A 和 $R(B,i-1)$叠加后 S_i 中白(黑)像素对应的子像素块的汉明重量的期望值，因此有

$$E[w(0,i,\Sigma)]=2+\sum_{j=1}^{n}E[w(0,i,j)]$$

$$E[w(1,i,\Sigma)]=2+\sum_{j=1}^{n}E[w(1,i,j)]$$

式中，伪装区域的汉明重量为 2，$1\leqslant i,j\leqslant n$。

按照秘密分享与恢复流程，在共享份 A 和 $R(B,i-1)$中，标记一致的秘密区域只有区域 i。根据引理 1 及基础矩阵 C 的特点，则有

$$E[w(0,i,\Sigma)]=E[w(0,i,i)]+\sum_{j=1,j\neq i}^{n}E[w(0,i,j)]+2$$
$$=1+3(n-1)/2+2=3(n-1)/2+3$$

$$E[w(1,i,\Sigma)]=E[w(1,i,i)]+\sum_{j=1,j\neq i}^{n}E[w(1,i,j)]+2$$
$$=2+3(n-1)/2+2=3(n-1)/2+4$$

因此 $E[w(1,i,\Sigma)]-E[w(0,i,\Sigma)]=1$，表示 S_i 中黑像素比白像素对应的子像素块的汉明重量期望值大 1，在恢复的图像中体现为 S_i 的黑像素比白像素对应的子像素块更黑，故共享份 A 和 $R(B,i-1)$叠加可以恢复秘密图像 S_i。

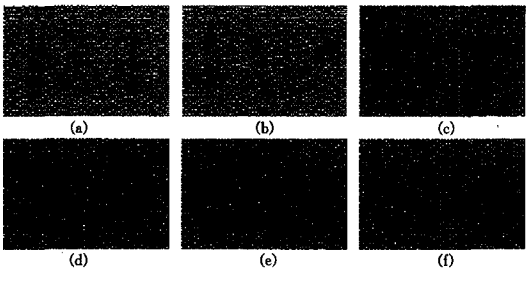
4 实验分析

在视觉密码方案中，像素扩展度是原始像素在共享份中被扩展成子像素的数目，相对差是恢复图像中原始黑白像素对应的灰度差值同扩展度的比值，它们是评价方案的两个重要参数。在本方案中，由于原图像的一个像素对应恢复后的 $2n+2$ 个像素，而原黑白像素对应的子像素块的汉明重量期望值相差 1，因此本文方案的像素扩展度为 $2n+2$，相对差为 $1/(2n+2)$。表 1 是本方案与其他 OMVCS 的一个综合对比。

表 1 本方案与其他 OMVCS 的参数对比

	秘密数量	像素扩展度	相对差	伪装图案
文献[13]	2	4	1/4	无
文献[14]	n	3n	1/(3n)	无
本文方案	n	2n+2	1/(2n+2)	有

图 8 2 幅伪装图案和 4 幅秘密图像



(a)共享份 A；(b)共享份 B；(c)－(f) 恢复后的 4 幅秘密图像

图 9 共享份及恢复效果

下面以 2 幅伪装图案和 4 幅秘密图像为例，对本文方案进行验证。图 8 给出了伪装图案和秘密图像，图 9 则包括 2 个共享份的平面图和恢复后的 4 个秘密图像。

从图 9 中可以看出，共享份 A 和 B 分别显示了 2 幅伪装图案，而且它们通过不同的叠加位置恢复出的 4 幅秘密图像，便于人眼直接观察，这也证实了本文方案的可行性。

结束语 本文提出了一种具有伪装图案的操作式多秘密视觉密码方案，使共享份可以呈现有意义的图案，一定程度上减小了被关注的概率。本文方案将共享份划分为伪装区域和可标记的秘密区域，利用区域标记和(2,2)单秘密视觉密码的基础矩阵设计了秘密分享与恢复的流程，其不仅可以确保方案的安全性、伪装性和对比性，而且恢复多幅图像时具有较好的恢复效果。由于本方案仍局限于两个共享份，因此如何扩展到(k,n)门限结构有待进一步研究。

参 考 文 献

[1] Naor M, Shamir A. Visual Cryptography [C]// Advances in Cryptology-Eurocrypt'94. Berlin, 1995, LNCS 950: 1-12

[2] Ateniese G, Blundo C, De Santis A, et al. Visual Cryptography for General Access Structures [J]. Information and Computation, 1996, 129(2): 86-106

[3] 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

[4] Cimato S, De Prisco R, De Santis A. Optimal colored threshold visual cryptography schemes [J]. Designs, Codes and Cryptography, 2005, 35(3): 311-335

[5] Fang Li-guo, Yu Bin. Research on pixel expansion of (2, n) visual threshold scheme [C]// 1st International Symposium on Pervasive Computing and Applications Proceedings (SPCA06). Ningbo, 2006: 856-860

[6] 黄东平，王道顺，黄连生，等. 一种新的(k,n)阈值可视密钥分存方案[J]. 电子学报，2006，34(3)：503-507

[7] 石润华. 一种新的彩色可视秘密共享方案[J]. 计算机应用研究，2006，23(1)：120-121，124

[8] Yang Ching-nung, Wang Chung-chun, Chen T-S. Visual cryptography schemes with reversing [J]. The Computer Journal, 2008, bxm118: 1-13

[9] Yang Ching-nung, Chen Tse-shih. Colored visual cryptography scheme based on additive color mixing [J]. Pattern Recognition, 2008, 41(10): 3114-3129

[10] Ng F Y, Wong D S. On the security of a visual cryptography scheme for color images [J]. Pattern Recognition, 2009, 42(5): 929-940

[11] Yu Bin, Xu Xiao-hui, Fang Li-guo. Multi-secret sharing threshold visual cryptography scheme [C]// 2007 International Conference on Computational Intelligence and Security (CIS 2007). Harbin, 2007: 815-818

[12] 易枫，王道顺，戴一奇. 一般存取结构的多密图彩色可视分存方案[J]. 自然科学进展，2006，16(1)：95-100

[13] Chen L H, Wu C C. A study on visual cryptography [D]. Taiwan: National Chiao Tung University, 1998

[14] Feng Jen-bang, Wub H-C, Tsaic C-S, et al. Visual secret sharing for multiple secrets [J]. Pattern Recognition, 2008, 41(12): 3572-3581

[15] Wang D S, Yi F, Li X B. On general construction for extended visual cryptography schemes [J]. Pattern Recognition, 2009