多重门限的图像秘密共享方案

李 鹏[1],马培军[1],苏小红[1],刘 峰[2]
(1.哈尔滨工业大学计算机科学与技术学院,黑龙江哈尔滨 150001;2.中科院信息工程研究所信息安全国家重点实验室,北京 100190)

摘 要: 针对传统的基于视觉密码的图像秘密共享方案存在像素扩张导致其只能共享小尺寸的秘密图像、信息隐藏效率较低的问题,提出一种能够提高信息隐藏容量的(t,k,n)多重门限图像秘密共享方案.该方案利用秘密图像信息控制视觉密码方案中共享矩阵的选取,从而实现秘密图像在视觉密码方案中的隐藏.在秘密图像恢复的第一阶段,任意t个参与者直接叠加其影子图像后可以视觉解密出低质量的秘密图像信息;在第二阶段,任意k个参与者可以从影子图像中提取出隐藏的信息,并通过计算恢复出精确的灰度秘密图像.相对于传统的视觉密码方案,本文方案在不影响视觉密码恢复图像的视觉质量前提下,可以隐藏更多的秘密图像信息,而像素扩张尺寸较小.

关键词: 信息隐藏;图像秘密共享;视觉密码;多重门限方案
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2012) 03-0518-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.03.018

Multi-Threshold Image Secret Sharing Scheme

LI Peng[1], MA Pei-jun[1], SU Xiao-hong[1], LIU Feng[2]
(1. *School of Computer Science and Technology, Harbin Institute of Technology, Harbin, Heilongjiang* 150001, *China*;
2. *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100190, *China*)

Abstract: From the point of view of information hiding, traditional visual cryptography scheme (VCS) is not an efficient method. It can only share a small sized secret image due to the large pixel expansion. A (t,k,n) multi-threshold image secret sharing scheme is proposed to increase the amount of hidden information. A grayscale secret image is hidden in a VCS to guide the choice of share matrices. In the first phase of the reconstruction process, any t participants can stack their shadow images to decode a vague secret image by human visual system. In the second phase, any k participants can extract additional information hidden in their shadow images, and reveal a precise grayscale secret image by computation. Compared with the traditional VCS, the proposed scheme can hide more information of the grayscale secret image, and has smaller size expansion without deteriorating the visual quality of the revealed image of VCS.

Key words: information hiding; image secret sharing; visual cryptography; multi-threshold scheme

1 引言

图像秘密共享(Image Secret Sharing,简称ISS)可以有效解决秘密图像信息的泄漏和篡改的问题,秘密图像信息的不经意损毁、丢失问题,以及秘密图像持有者权利过于集中的问题,提高了秘密图像保护的安全性.

一类特殊的ISS方案是Naor和Shamir[1]提出的(t,n)门限视觉密码方案(Visual Cryptography Scheme,简称VCS).秘密图像被分拆为n个影子图像,每个影子图像的尺寸是秘密图像的m倍,m为像素扩张系数.将其中任意t个影子图像打印在透明胶片上,然后叠加t个透明胶片可以从视觉上解密出秘密图像信息,无需任何计算设备的辅助和密码学知识.由于VCS存在像素扩张的问题,因此研究者提出了多种低像素扩张的VCS[2~5],其中包括无像素扩张的概率型VCS[4,5].对比度是用于评价VCS恢复图像的视觉质量的性能指标.很多文献提出了对比度优化的VCS构造方法[6~11].传统的VCS只能处理二值图像,对于灰度和彩色图像一般首先采用半色调技术转化为二值图像,然后再进行视觉密码共享[12~14].由于影子图像通常表现为噪声形式,容易引起攻击者的怀疑,并且不容易识别和管理.因此,有学者提出影子图像有意义的VCS以解决这一问题[15,16].传统的VCS需要多个参与者出示其影子图像合作解密,因此存在着参与者欺骗的可能性,即参与者

收稿日期:2011-05-25;修回日期:2011-07-29
基金项目:国家自然科学基金(No.60903210)

提供伪造的或篡改的影子图像进行解密,从而导致恢复出错误的秘密图像.研究者提出了防欺骗的 VCS[17],可以有效地检测参与者的欺骗行为.为了便于管理多个秘密图像的视觉共享,有学者提出了多秘密共享的视觉密码方案[18].

传统的 VCS 具有秘密图像快速解密的优点,但是只能恢复出模糊的秘密图像,无法直接解密出精确的秘密图像,尤其是灰度图像和彩色图像.同时传统的 VCS 还具有较大的像素扩张,一般只能处理小尺寸图像的秘密共享.从携带秘密信息的能力上来说,是一种效率较低的方案.另一类 ISS 方案是 Thien 和 Lin[19]提出的基于多项式的(t,n)-ISS 方案,即 PISSS(Polynomial-based Image Secret Sharing Scheme).该方案可以精确恢复灰度秘密图像,并且影子图像的尺寸缩小为秘密图像的 $1/t$.相对于 VCS,PISSS 解密过程需要复杂的计算.Lin 和 Lin[20]提出了一种结合了 VCS 和 PISSS 特性的二合一 ISS 方案,在解密过程中,既可以叠加任意 t 个影子图像视觉解密出模糊的秘密图像信息,也可以通过计算提取出影子图像中隐藏的信息,解密出更加精确的秘密图像.该方案的局限性在于 VCS 隐藏的信息量较少,通常需要将秘密图像进行较大的压缩,或者采用更大尺寸扩张的 VCS.为了降低影子图像的尺寸扩张,文献[21]利用灰度像素替代 VCS 中的黑色像素,提出了一种基于灰度的 VCS,即 GVCS (Gray-based Visual Cryptography Scheme).该方案具有文献[20]的方案相同的功能,并且大大减小了影子图像的尺寸扩张.但是,文献[21]的方案叠加影子图像后恢复的秘密图像的视觉质量较差,很难从视觉上获得秘密图像信息.另外文献[21]的容错能力很差,影子图像印制到透明胶片上之后,容易被磨损,而一旦有所磨损之后,则无法正确地提取其中的隐藏信息,从而无法恢复出精确的秘密图像信息.

为了在 VCS 中隐藏更多的秘密信息,并且不降低解密图像的视觉质量,本文提出了一种(t,k,n)的多重门限 ISS 方案,利用加密后的密文图像信息来控制 VCS 的共享矩阵选取,从而在 VCS 中隐藏额外的灰度秘密图像信息.在恢复过程的第一阶段,将任意 t 个影子图像叠加可以视觉解密出模糊的秘密图像信息;在第二阶段,从任意 k 个影子图像中提取出隐藏的信息,然后通过计算恢复出精确的秘密图像,其中 $t\leqslant k\leqslant n$.该方案可以用于多重门限的秘密图像共享;也可以利用第一阶段的恢复图像来验证影子图像的合法性,防止参与者欺骗.

2　二合一 ISS 方案

Lin 和 Lin 在文献[20]中提出的二合一 ISS 方案既可以通过叠加影子图像快速视觉解密出低质量的秘密图像,也可以通过计算解密出更加精确的秘密图像.该方案共享两个秘密图像:一个是用于(t,n)-PISSS 的灰度秘密图像 S,另一个是用于(t,n)-VCS 的秘密图像的半色调秘密图像 H.其主要思想是利用 PISSS 生成的共享份额控制 VCS 中不同类型共享矩阵的选取,从而将共享份额隐藏到 VCS 的影子图像中.在恢复时,既可选择叠加影子图像恢复模糊的秘密图像,也可以计算解密更加精确的秘密图像.令 $\boldsymbol{B}_0$ 和 $\boldsymbol{B}_1$ 分别表示 VCS 中共享白色像素和黑色像素的布尔基矩阵,其中"1"代表黑色像素,"0"代表白色像素.将 $\boldsymbol{B}_0$ 和 $\boldsymbol{B}_1$ 列置乱后得到的共享矩阵族分别表示为 $\boldsymbol{C}_0$ 和 $\boldsymbol{C}_1$.该方案将共享矩阵按照首行的不同排列对应成不同的类型,则共享矩阵族 $\boldsymbol{C}_0$ 和 $\boldsymbol{C}_1$ 中各包含有 C_{w+b}^{w}种不同的类型,其中 b 为共享矩阵首行中包含"1"的个数,w 为共享矩阵首行中包含"0"的个数.图 1 给出了一个由基矩阵首行的不同排列得到不同类型共享矩阵的例子.

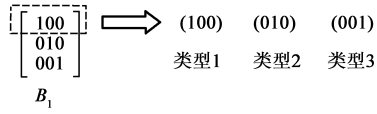


图1　由基矩阵B_1首行的不同排列对应到3种不同类型的共享矩阵

将不同类型的共享矩阵对应于一个不同的秘密信息,则共享单个秘密像素时共享矩阵可隐藏的信息量为:

$$I=\left\lfloor \log_2 \frac{(w+b)!}{w!\ b!} \right\rfloor \text{ bits} \tag{1}$$

令$|H|$表示 VCS 共享的半色调秘密图像 H 包含的像素个数,则整个 VCS 可以隐藏的信息量为:

$$Q=I\times|H| \text{ bits} \tag{2}$$

另一方面,文献[20]利用文献[17]的多项式共享方法将灰度秘密图像分解为 n 个份额,分别隐藏到对应的影子图像中.单个共享份额尺寸为灰度秘密图像的 $1/t$,并且单个影子图像只有 $1/n$ 的区域用于隐藏共享份额.因此,为了将共享份额信息完全隐藏到影子图像中,半色调图像的尺寸需满足如下条件:

$$|H|\geqslant[8n/(t\cdot I)]\cdot|S| \tag{3}$$

即半色调图像的尺寸为灰度秘密图像尺寸的 $8n/(t\cdot I)$ 倍.文献[20]的方案需要放大半色调图像的尺寸,因而使得影子图像具有更大的尺寸.大尺寸的影子图像会给存储和传输带来更大的负担.

3　多重门限的图像秘密共享方案

文献[20]将共享矩阵按第一行的不同排列划分成不同类型,所得到的类型数目较少,因此单个共享矩阵能隐藏的信息量较低.为了在 VCS 中隐藏更多的信息,

本文选取共享矩阵族 $\boldsymbol{C}_0$ 和 $\boldsymbol{C}_1$ 中的所有两两不同的矩阵作为不同的类型来隐藏秘密信息.该方法可以得到更多的共享矩阵类型数目,从而可以隐藏更多的秘密信息.例如,对于图 1 中(2,3)-VCS 的基矩阵 $\boldsymbol{B}_1$,对其列置乱后可以得到 6 个不同类型的共享矩阵;而采用文献[20]的方法,只能得到 3 个不同类型的共享矩阵.显然,更多数目的共享矩阵类型可以用来隐藏更多的秘密信息.图 2 给出了由基矩阵 $\boldsymbol{B}_1$ 列置乱后得到的不同类型的共享矩阵.

$$B_1=\begin{bmatrix}100\\010\\001\end{bmatrix}\Rightarrow \underset{\text{类型1}}{\begin{bmatrix}100\\010\\001\end{bmatrix}}\ \underset{\text{类型2}}{\begin{bmatrix}100\\001\\010\end{bmatrix}}\ \underset{\text{类型3}}{\begin{bmatrix}010\\100\\001\end{bmatrix}}\ \underset{\text{类型4}}{\begin{bmatrix}010\\001\\100\end{bmatrix}}\ \underset{\text{类型5}}{\begin{bmatrix}001\\100\\010\end{bmatrix}}\ \underset{\text{类型6}}{\begin{bmatrix}001\\010\\100\end{bmatrix}}$$

图2 由基矩阵B_1列置乱后得到的6种不同类型共享矩阵

另外,本文利用图像加密算法加密原灰度秘密图像,将得到的密文图像作为 VCS 的伪随机输入来控制共享矩阵的选取,从而将额外的灰度秘密图像信息隐藏在 VCS 中.相对于文献[20]和文献[21]的方案,本文的方案无需对原灰度秘密图像进行多项式共享的过程.

3.1 基本框架

本文提出的(t,k,n)-ISS 方案共享两个秘密图像:一个是灰度秘密图像 S,另一个是该灰度图像的半色调图像 H.首先将灰度秘密图像加密得到密文图像 S^1,然后利用(t,n)-VCS 共享半色调图像 H,共享过程由密文图像数据 S^1 作为伪随机数列来控制选取不同类型的共享矩阵.在恢复过程中,叠加任意 t 个影子图像可以视觉解密低质量的秘密图像信息;从任意 k 个影子图像中提取出密文图像数据,经解密过程可以计算恢复精确的灰度秘密图像.

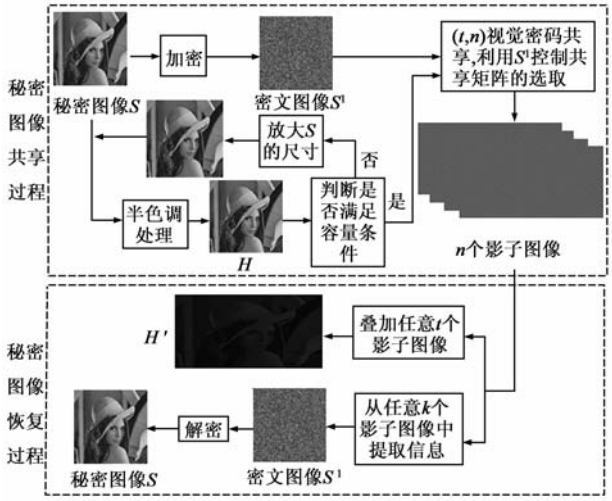


图3 多重门限图像秘密共享方案的框架

图 3 给出了多重门限 ISS 方案的框架.该方案主要包括两个过程:秘密图像共享过程和秘密图像恢复过程.

3.1.1 秘密图像共享过程

为了更好地利用秘密图像数据来模拟伪随机序列,需要加密秘密图像 S 得到密文图像 S^1.加密算法可以采用一般的对称加密算法,如 AES 加密.对于加密后数据的伪随机特性,文献[22]给出了详细的测试.加密密钥 K 通过 Shamir[23]的(k,n)多项式门限共享生成 n 个子密钥并分配给对应的参与者,使得其中任意 k 个参与者可以联合恢复密钥 K,任意少于 k 个参与者联合不能恢复密钥.

另一方面,为了利用视觉密码方案共享灰度秘密图像,需要将秘密图像 S 进行半色调处理转换成半色调图像 H.然后利用(t,n)-VCS 共享半色调图像 H.为了将密文图像数据隐藏到 VCS 中,需要建立秘密信息与共享矩阵不同类型之间的映射表.最后利用密文图像 S^1 的信息查找映射表得到对应类型的共享矩阵来生成影子图像,从而实现密文图像信息在 VCS 中的隐藏.

考虑到密文图像数据量有可能大于 VCS 最大可隐藏信息容量的情况,此时需要增大半色调图像 H 的尺寸.首先放大秘密图像 S,然后再利用半色调技术得到更大尺寸的半色调图像 H.需要注意的是,半色调图像满足容量条件时,即当密文图像数据量小于 VCS 最大可隐藏信息容量时,无需增大半色调图像 H 的尺寸.算法 1 给出了秘密图像共享过程的具体步骤.

算法 1 秘密图像共享过程

输入:秘密图像 S,密钥 K;

输出:n 个影子图像和 n 个子密钥;

第 1 步:利用密钥 K 加密秘密图像 S 得到密文图像 S^1;

第 2 步:利用 Shamir 的(k,n)多项式共享方案共享密钥 K,生成 n 个子密钥并分配给 n 个参与者;

第 3 步:对秘密图像 S 半色调处理得到半色调图像 H;

第 4 步:判断半色调图像 H 是否满足 VCS 的最大隐藏容量大于密文图像.若满足,则转到第 5 步;否则,放大秘密图像 S 的尺寸,转到第 3 步;

第 5 步:利用(t,n)-VCS 共享半色调图像 H 得到 n 个影子图像,其中共享矩阵的选取由密文图像信息控制.

3.1.2 秘密图像恢复过程

(t,k,n)-ISS 方案的秘密图像恢复过程分为两个阶段.第一阶段是通过叠加任意 t 个影子图像,利用视

觉密码的原理解密出低质量的秘密图像 H'.由于视觉密码具有像素扩张和对比度下降的缺点,因此解密后图像 H' 在视觉质量比半色调图像 H 要差很多,但是仍可以看出原秘密图像的大体轮廓信息.第二阶段为精确恢复阶段.首先获得 k 个影子图像.针对影子图像中的每个像素块,由 k 个像素块可以得到共享矩阵中对应的 k 行,然后利用这 k 行信息唯一确定共享矩阵的类型,再通过查找秘密信息与共享矩阵不同类型之间的映射表,恢复出密文图像 S^1 的数据;最后通过计算解密 S^1 得到精确的灰度秘密图像 S.算法 2 给出了秘密图像恢复过程的具体步骤.

算法 2　秘密图像恢复过程

输入:k 个影子图像和 k 个子密钥;

输出:秘密图像 H' 和秘密图像 S;

第 1 步:直接叠加任意 t 个影子图像,可以视觉解密模糊的秘密图像 H';

第 2 步:由 k 个影子图像中相同位置的像素块重构出唯一的共享矩阵,进而解密出对应的密文图像信息;

第 3 步:利用 Lagrange 插值原理,由 k 个子密钥重构出密钥 K;

第 4 步:利用密钥 K 解密密文图像得到秘密图像 S.

3.2　VCS 中共享矩阵隐藏数据量分析

在 VCS 中,共享矩阵族 $\boldsymbol{C}_0$(或 $\boldsymbol{C}_1$)由 $n\times m$ 的基矩阵 $\boldsymbol{B}_0$(或 $\boldsymbol{B}_1$)进行列置乱得到.因此,$\boldsymbol{C}_i(i=0,1)$包含对 $\boldsymbol{B}_i$ 列置乱得到的 $m!$ 个矩阵.由于 $\boldsymbol{B}_i$ 可能包含相同的列,因此 $\boldsymbol{C}_i$ 中可能存在完全相同的共享矩阵.为了实现秘密信息和共享矩阵类型的一一对应,本文将 $\boldsymbol{C}_i$ 中两两不同的共享矩阵当作不同的类型.令基矩阵 $\boldsymbol{B}_i$ 中所包含两两不同的列为 $b_1,b_2,\cdots,b_c$,并且每一列在 $\boldsymbol{B}_i$ 中重复出现的次数为 $f_1,f_2,\cdots,f_c$,则对应的共享矩阵族 $\boldsymbol{C}_i$ 包含的不同类型矩阵个数为:

$$|\boldsymbol{C}_i| = m!\ \Big/\Big(\prod_{i=1}^{c} f_i!\Big) \tag{4}$$

由于信息的最小单位是比特,因此单个共享矩阵可隐藏的信息量最大为$\lfloor\log_2|\boldsymbol{C}_i|\rfloor$比特.令视觉密码共享的二值秘密图像(即半色调图像 H)一共包含 a_0 个白色像素和 a_1 个黑色像素,则 VCS 可以隐藏的总比特数 Q 为:

$$Q = a_0\lfloor\log_2|\boldsymbol{C}_0|\rfloor + a_1\lfloor\log_2|\boldsymbol{C}_1|\rfloor \tag{5}$$

为了将密文图像数据 S^1 完全隐藏到 VCS 中,需要满足

$$Q \geqslant 8|S^1| \tag{6}$$

其中 $|S^1|$ 表示密文图像 S^1 所包含的灰度像素个数.由于从 S 到 S^1 为对称加密过程,图像的数据量不会改变,即

$$|S| = |S^1| \tag{7}$$

因此,当秘密图像 S 所包含的数据容量大于 Q 时,需要扩展半色调图像的尺寸.即当 $8|S|>Q$ 时,需要放大秘密图像尺寸,然后经半色调处理得到更大尺寸的半色调图像 H,直到满足不等式(6)为止.

本文主要考虑秘密图像无损恢复的情况,对于秘密图像有损恢复的情况,可以通过压缩秘密图像大小的方式,使得不等式(6)成立.令 R 表示压缩比率,其定义为

$$R = (S\text{ 的比特数})/(S\text{ 压缩后的比特数}) \tag{8}$$

则压缩比率 R 需满足如下条件

$$a_0\lfloor\log_2|\boldsymbol{C}_0|\rfloor + a_1\lfloor\log_2|\boldsymbol{C}_1|\rfloor \geqslant 8|S|/R \tag{9}$$

化简后得:

$$R \geqslant 8|S|/(a_0\lfloor\log_2|\boldsymbol{C}_0|\rfloor + a_1\lfloor\log_2|\boldsymbol{C}_1|\rfloor) \tag{10}$$

需要注意的是,当不等号右边的值小于等于 1 时,表明 VCS 可隐藏的数据量大于等于待隐藏的秘密图像数据量,因此无需执行压缩过程.

3.3　共享矩阵的唯一确定

在秘密图像恢复过程的第二阶段,需要从任意 k 个影子图像中提取出隐藏的密文图像信息.也就是说,需要利用 k 个影子图像中每个对应位置像素块重构出 VCS 中唯一类型的共享矩阵,从而提取出对应的秘密信息.由 (t,n)-VCS 的定义可知,任意 $t-1$ 或更少的影子图像不能确定秘密图像的像素信息,也就不能确定所选取的共享矩阵.因此 k 的取值必须大于等于 t.

对于 $k=n$ 的情况,若恢复过程中得到了 n 个影子图像,显然可以通过这 n 个影子图像中相同位置的像素块唯一确定一个 n 行的共享矩阵,进而解密出所隐藏在共享矩阵中的密文图像数据.因此,对于一个 (t,n)-VCS 可以很容易的构造出多重门限的 (t,n,n) 图像秘密共享方案.

下面给出当 $t\leqslant k<n$ 时,利用共享矩阵的任意 k 行唯一确定共享矩阵的方法.本文采用 Droste[3] 提出的 (t,n)-VCS 构造方法来构造视觉密码的基矩阵.令 T_0 和 T_1 分别表示基矩阵 $\boldsymbol{B}_0$ 和 $\boldsymbol{B}_1$ 中列向量的海明重量所组成的集合.通过分析 Droste[3] 提出的 (t,n)-VCS 构造方法可知,基矩阵 $\boldsymbol{B}_0$ 和 $\boldsymbol{B}_1$ 中所包含的列向量的海明重量组成的集合分别为

$T_0=\{a\,|\,0\leqslant a\leqslant\lfloor t/2\rfloor, a \bmod 2=0\}\cup\{a+n-t\,|\,\lfloor t/2\rfloor < a\leqslant t, a \bmod 2=0\}$,和 $T_1=\{a\,|\,0\leqslant a\leqslant\lfloor t/2\rfloor, a \bmod 2=1\}\cup\{a+n-t\,|\,\lfloor t/2\rfloor < a\leqslant t, a \bmod 2=1\}$.由于共享矩阵是由基矩阵进行列置乱后得到,其列向量的海明重量集合与基矩阵列向量的海明重量集合相同.因此,利用共享矩阵的任意 $n-1$ 行信息,可以唯一确定出第

n 行的信息.算法 3 给出了利用 $n-1$ 行信息唯一确定第 n 行的具体步骤.

算法 3 由共享矩阵的任意 $n-1$ 行唯一确定出共享矩阵

输入:$\boldsymbol{C}_i(i=0,1)$中任意共享矩阵 $\boldsymbol{D}$ 的任意 $n-1$ 行;

输出:共享矩阵 $\boldsymbol{D}$;

第 1 步:由于 $t \leqslant k=n-1$,叠加任意 t 行可以解密出秘密像素信息;

第 2 步:令 $\boldsymbol{D}$ 的 $n-1$ 行组成的子矩阵为 $\boldsymbol{E}$,对 $\boldsymbol{E}$ 的每一列 p_i,计算出 p_i 的海明重量为 w;

(1)当秘密像素是白色像素时,如果 $w \in T_0$,则该列最后一行的元素为 0;否则为 1;

(2)当秘密像素是黑色像素时,如果 $w \in T_1$,则该列最后一行的元素为 0;否则为 1;

第 3 步:循环执行第 2 步,直到 $\boldsymbol{E}$ 的每一列都处理完后,得到 $\boldsymbol{D}$ 的最后一行的所有元素.再结合已知的 $n-1$ 行重构出共享矩阵 $\boldsymbol{D}$.

因此,当 $k \geqslant \max\{t, n-1\}$,利用本文的方法可以有效地实现$(t,k,n)$-ISS 方案.

4 实验结果与分析

为了验证本文的方案,本文选取 256×256 像素的灰度图像 Lena 作为秘密图像.首先针对 $t=k<n$ 的情况,选取$(3,3,4)$-ISS 方案验证本文算法.由 Droste 方案[3]构造出$(3,4)$-VCS 的基矩阵:

$$\boldsymbol{B}_0=\begin{bmatrix}0&1&1&1&0&0\\0&1&1&0&1&0\\0&1&0&1&1&0\\0&0&1&1&1&0\end{bmatrix},\boldsymbol{B}_1=\begin{bmatrix}1&0&0&0&1&1\\0&1&0&0&1&1\\0&0&1&0&1&1\\0&0&0&1&1&1\end{bmatrix}$$

由 3.2 节隐藏信息量分析可知,共享单个秘密像素可以隐藏的信息量为$\lfloor \log_2 | \boldsymbol{C}_0 | \rfloor = \lfloor \log_2 | \boldsymbol{C}_1 | \rfloor = \lfloor \log_2 | 360 | \rfloor = 8$ 比特.由于单个灰度像素恰好包含 8 比特信息,因此秘密图像的半色调图像与原秘密图像具有相同的尺寸.图 4(a)给出了秘密图像,其尺寸大小为 256×256 像素.由于$(3,4)$-VCS 的像素扩展为 6,所以生成的 4 个影子图像尺寸均为原秘密图像的 6 倍,即 512×768 像素.图 4(b)显示了其中的一个影子图像.在秘密图像恢复过程中,首先叠加任意三个影子图像后,可以视觉解密模糊的秘密图像信息,如图 4(c)所示.在恢复过程的第二个阶段,可以从 3 个影子图像中提取出隐藏的密文图像数据,然后计算解密得到原秘密图像.

采用文献[20]的方案,单个秘密像素可以隐藏的信息量为$\lfloor \log_2 [6!/(3! \times 3!)] \rfloor = 4$ 比特,因此需要将半色调图像尺寸放大为原秘密图像的 8/3 倍.又因为 VCS 的像素扩张系数 $m=6$,因此得到的影子图像尺寸为原秘密图像尺寸的 16 倍,即 1024×1024 像素.图 4(d)给出了叠加影子图像后的恢复图像.相对于本文的方案,文献[20]的影子图像尺寸为本文方案的 8/3 倍.

(a) 秘密图像 (b) 利用本文的方法生成一个影子图像

(c)由本文的方法得到的解密图像 (d) 由文献[20]的方法得到的解密图像

图4 (3,3,4)-ISS方案的实验结果

针对 $t<k=n$ 的情况,除了对加密密钥 K 的共享外,(t,n,n)-ISS 方案的构造方法和$(t,n\text{-}1,n)$-ISS 方案完全相同.$(3,3,4)$-ISS 方案中,密钥 K 以$(3,4)$门限方案共享生成 4 个子密钥并分配给各参与者,任意 3 个参与者可以联合恢复密钥 K.而$(3,4,4)$-ISS 方案中,密钥 K 以$(4,4)$门限共享生成 4 个子密钥,只有 4 个子密钥联合才能恢复密钥 K.因此,在$(3,4,4)$-ISS 方案中,即使 3 个参与者联合利用影子图像可以恢复得到密文图像数据,但是无法得到加密密钥 K,因此也无法恢复出原秘密图像.

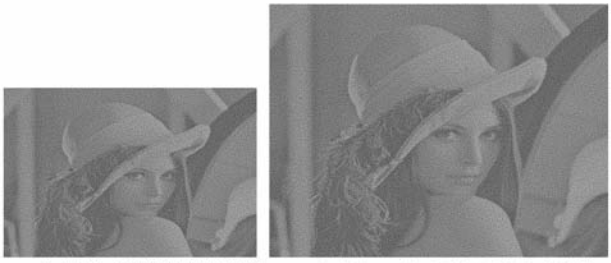
(a) 由本文方法得到的恢复图像 (512×1024像素)

(b) 由文献[20]的方法得到的恢复图像(1024×1024像素)

图5 (3,3,3)-ISS方案的实验结果

本文同时给出针对 $t=k=n$ 时,选取$(3,3,3)$-ISS 方案的实验结果(如图 5 所示),以及 $t<k<n$ 时,选取$(2,3,4)$-ISS 方案的实验结果(如图 6 所示).实验结果表明,利用本文方案得到的影子图像尺寸均小于文献[20]的结果.由于本文方案和文献[20]方案使用相同

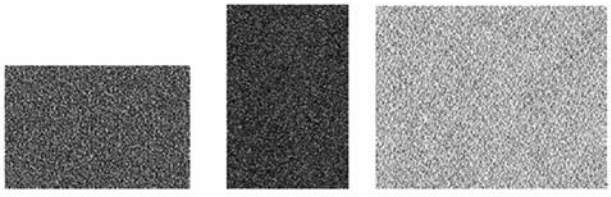
VCS 基矩阵,因此视觉解密的图像具有相同的对比度,即叠加影子图像恢复的秘密图像具有相同的视觉质量.但是,本文方案的影子图像尺寸要远小于文献[20]的结果.事实上,更小尺寸的影子图像可以降低存储和传输过程中的开销.



(*a*) 由本文方法得到的恢复图像(680×1024像素)　(*b*) 由文献[20]的方法得到的恢复图像(1024×1366像素)

图6　(2,3,4)-ISS方案的实验结果

文献[21]同样可以实现与本文相似的多重门限图像秘密共享的功能,本文也给出在上述实验相同的条件下利用文献[21]的方案得到的实验结果.如图 7 所示,由于文献[21]中的 GVCS 采用灰度像素替代 VCS 中的黑色像素,使得每个影子图像能够隐藏更多的信息,从而得到更小尺寸扩张的影子图像.但是,该方案降低了叠加影子图像后得到的恢复图像的视觉质量.由图 7 的实验结果可知,从叠加影子图像后得到的恢复图像中,很难从视觉上获得原秘密图像内容信息.因此,文献[21]的方案视觉解密秘密图像的能力较差.另外,由于文献[21]得到的影子图像为灰度图像,物理保存难度更大,将影子图像打印在透明胶片上后,稍有磨损则无法恢复精确的秘密图像信息.



(*a*) 由(3,3,4)-ISS方案得到的恢复图像(171×256像素)　(*b*) 由(3,3,3)-ISS方案得到的恢复图像(256×171像素)　(*c*) 由(2,3,4)-ISS方案得到的恢复图像(256×342像素)

图7　文献[21]的实验结果

本文的方案与文献[20]、文献[21]的方案均可实现 (t,k,n)-ISS 的功能.三个方案既具有叠加任意 t 个影子图像后视觉解密模糊秘密图像的功能,又可以利用任意 k 个影子图像计算解密出精确的原秘密图像.由于视觉质量和尺寸扩张是视觉密码的两个重要指标,表 1 给出了三个方案在共享原理、影子图像尺寸大小和视觉解密图像的视觉质量上的比较.与文献[20]中的方案相比,本文方案的影子图像具有更小的尺寸扩张,更有利于减轻存储和传输过程中的负担.尽管文献[21]的方案可以得到更小尺寸的影子图像,但该方案叠加影子图像后得到的解密图像视觉质量较差,很难从视觉上获取原秘密图像信息.另外,文献[21]的容错能力差,将影子图像打印在透明胶片上后,稍有磨损则无法恢复精确的秘密图像信息.

表 1　本文的方案与文献[20]、文献[21]的性能比较

	共享方案的原理	影子图像尺寸	叠加影子图像解密的视觉质量
文献[20]的方案	加密 + PISSS + VCS	大	好
文献[21]的方案	加密 + PISSS + GVCS	小	差
本文的方案	加密 + VCS	中	好

5　结论

本文提出的 (t,k,n) 多重门限图像秘密共享方案,可以在不影响 VCS 解密图像视觉质量的前提下,隐藏更多的秘密图像信息,提高了 VCS 的信息隐藏效率.在密图恢复过程中,任意 t 个参与者可以叠加其影子图像解密出低质量的秘密图像,任意 k 个参与者可以合作计算解密出精确的秘密图像.该方案可以实现多重权限的图像秘密共享,也可用于防止参与者的欺骗.同时,本文的方案还可以共享两个不同的秘密图像,根据不同的门限恢复出不同的秘密图像.当 $k \geqslant \max\{t, n-1\}$,本文给出了 (t,k,n)-ISS 方案的构造方法.下一步研究方向是,当 $t < k < n-1$ 时,给出 (t,k,n)-ISS 方案的构造方法.

参考文献

[1] NAOR M, SHAMIR A. Visual cryptography[A]. Advances in Cryptology-Eurocrypt'94 (LNCS 950)[C]. Berlin: Springer-Verlag, 1995. 1 – 12.

[2] BLUNDO C, CIMATO S, et al. Visual cryptography schemes with optimal pixel expansion[J]. Theoretical Computer Science, 2006, 369(1): 169 – 182.

[3] DROSTE S. New results on visual cryptography[A]. Advances in Cryptology-Crypto'96 (LNCS 1109)[C]. Berlin: Springer-Verlag, 1996. 401 – 415.

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

[5] ITO R, KUWAKADO H, et al. Image size invariant visual cryptography[J]. IEICE Transactions on Fundamentals, 1999, E82-A(10): 2172 – 2177.

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

[7] BLUNDO C, ARCO P D', et al. Contrast optimal threshold visual cryptography schemes[J]. SIAM Journal on Discrete

Mathematics,2003,16(2):224 – 261.
[8] KRAUSE M, SIMON H U. Determining the optimal contrast for secret sharing schemes in visual cryptography[J]. Combinatorics, Probability and Computing,2003,12(3):285 – 299.
[9] CIMATO S, SANTIS A D, et al. Ideal contrast visual cryptography schemes with reversing[J]. Information Processing Letters,2005,93(4):199 – 206.
[10] 黄东平,王道顺,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.
HUANG Dong-ping, WANG Dao-shun, et al. A novel (k,n) threshold scheme for visual secret sharing[J]. Acta Electronica Sinica,2006,34(3):503 – 507.(in Chinese)
[11] 张海波,王小非,等.利用反转实现理想对比度的密图分存[J].电子学报,2010,38(2):465 – 468.
ZHANG Hai-bo, WANG Xiao-fei, et al. Ideal contrast secret image sharing using reversing[J]. Acta Electronica Sinica, 2010,38(2):465 – 468.(in Chinese)
[12] LIN C C, TSAI W H. Visual cryptography for gray-level images by dithering techniques[J]. Pattern Recognition Letters, 2003,24(1-3):349 – 358.
[13] HOU Y C. Visual cryptography for color images[J]. Pattern Recognition,2003,36(7):1619 – 1629.
[14] YANG C N, CHEN T S. Colored visual cryptography scheme based on additive color mixing[J]. Pattern Recognition,2008, 41(10):3114 – 3129.
[15] LIU F, WU C K. Embedded extended visual cryptography schemes[J]. IEEE Transactions on Information Forensics & Security,2011,6(2):307 – 322.
[16] WANG D S, YI F, et al. On general construction for extended visual cryptography schemes[J]. Pattern Recognition,2009,42 (11):3071 – 3082.
[17] LIU F, WU C K, et al. Cheating immune visual cryptography scheme[J]. IET Information Security,2011,5(1):51 – 59.
[18] 付正欣,郁滨,等.一种新的多秘密分享视觉密码[J].电子学报,2011,39(3):714 – 718.
FU Z X, YU B, et al. A new multi-secret sharing visual cryptography[J]. Acta Electronica Sinica,2011,39(3):714 – 718.(in Chinese)
[19] THIEN C C, LIN J C. Secret image sharing[J]. Computer& Graphics,2002,26(5):765 – 770.
[20] LIN S J, LIN J C. VCPSS: A two-in-one two-decoding-options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches[J]. Pattern Recognition,2007,40(12):3652 – 3666.
[21] YANG C N, CIOU C B. Image secret sharing method with two-decoding-options: lossless recovery and previewing capability[J]. Image and Vision Computing,2010,28(12):1600 – 1610.
[22] SOTO J, BASSHAM L. Randomness Testing of the Advanced Encryption Standard Finalist Candidates[DB/OL]. http://csrc.nist.gov/publications/nistir/ir6483.pdf,2000.
[23] SHAMIR A. How to share a secret[J]. Communications of the ACM,1979,22(11):612 – 613.

作者简介

李 鹏 男,1982 年 6 月出生于四川省仁寿县.博士研究生.主要研究方向为图像秘密共享、视觉密码、图像处理.
E-mail:lphit@163.com

马培军 男,1963 年生.现为哈尔滨工业大学教授、博士生导师.主要从事空间计算、信息融合、色彩匹配、图像处理及智能控制等计算机应用技术研究.
E-mail:ma@hit.edu.cn

苏小红 女,1966 年生.现为哈尔滨工业大学教授、博士生导师.中国计算机学会高级会员.主要研究方向:软件缺陷检测、图像处理与识别、信息融合、智能计算等.
E-mail:sxh@hit.edu.cn

刘 峰 男,1980 年 9 月生于山东济南.博士.中国科学院信息工程研究所信息安全国家重点实验室副研究员.主要研究方向包括视觉密码学和安全协议形式化分析.
E-mail:fengliu.cas@gmail.com