计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190800069

一种面向门限结构的操作式可视多秘密分享方案

董　晨[1,2]　季姝廷[3]　张皓宇[3]　李　磊[3]
1 天津理工大学计算机科学与工程学院　天津 300384
2 天津市智能计算及软件新技术重点实验室　天津 300384
3 天津市大数据管理中心　天津 300221

摘　要　可视秘密分享将数字图像处理和秘密共享相结合,将秘密图像加密成多个共享份,在秘密恢复时将符合条件的共享份进行叠加,通过人眼直接解密秘密信息,具有解密复杂度低、信息容量大等优点。特别地,可视多秘密分享可用于分享多幅秘密图像,可应用于群体参与或控制领域。然而,目前操作式分享方案的研究受限于(2,2,n)存取结构,即n个参与者中的任意2个拿出持有的共享份进行恢复时,通过旋转和叠加操作最多能恢复2幅秘密图像。文中针对现有多秘密分享方法仅局限于两个参与者的问题,设计了一种新的秘密分享和共享份旋转操作规则,通过对秘密图像进行纵向区域划分,采用异或(XOR)运算基础矩阵对像素点逐区域进行加密,在此基础上设计了面向门限结构的操作式多秘密分享方案,并通过理论证明了方案的安全性和有效性。实验结果表明,与已有方案相比,所提方案通过在秘密分享时对秘密图像进行划分和标记纵向区域,实现了所有共享份地位对等,提高了可分享秘密的数量,最多可以同时将WT幅秘密图像分享到k个环形共享份中。该方案在满足安全条件的前提下,增强了相对差,改善了秘密图像的恢复效果。

关键词:可视秘密分享;多秘密;操作式方案;门限结构;异或
中图法分类号　TP309.7

Operational Visual Multi-secret Sharing Scheme for Threshold Structure

DONG Chen[1,2],JI Shu-ting[3],ZHANG Hao-yu[3] and LI Lei[3]
1 School of Computer Science and Engineering,Tianjin University of Technology,Tianjin Key Laboratory of Intelligence Computer and Novel Software Technology,Tianjin 300384,China
2 Key Laboratory of Intelligence Computer and Novel Software Technology,Tianjing 300384,China
3 Big Data Management Center of Tianjin,Tianjin 300221,China

Abstract　Visual secret sharing (VSS) combines digital image processing with secret sharing. It encodes the secret image into multiple shares. Then the secret information can be decoded by human eyes directly when the qualified shares are superimposed. It has the merits such as low decoding complexity and large information capacity. In particular, visual multi-secret sharing (VMSS) can be used to share multiple secret images and applied to the field of group participation and control. However, the current research on operational sharing schemes is limited by the (2,2,n) access structure, that is, when any 2 of the n participants take out their shares for recovery, 2 secret images at most can be recovered through rotation and superposition operations. Aiming at the problem that existing multi-secret sharing schemes are limited to 2 participants, a new secret sharing and sharing rotation operation rule is designed in this paper. By partitioning the secret image longitudinally and encrypting the pixels region by region with XOR basic matrix, an operational visual multi-secret sharing scheme (OVMSS) oriented to threshold structure is designed. Moreover, the security and validity of the scheme are proved theoretically. The experimental results show that, compared with the existing schemes, the proposed scheme achieves the equality of all shares by dividing secret images and marking the vertical regions in secret sharing, and improves the number of secrets that can be shared. WT secret images can be shared into k ring shares simultaneously at most. On the premise of meeting the safety conditions, the proposed scheme enhances the relative difference and improves the recovery quality of secret image.

Keywords　Visual secret sharing, Multiple secrets, Operational scheme, Threshold structure, XOR

到稿日期:2019-08-15　返修日期:2019-11-12　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家级大学生创新创业训练计划项目(201810060008)
This work was supported by the National Innovation and Entrepreneurship Training Program for College Students (201810060008).
通信作者:董晨(dongc@tjut.edu.cn)

1　引言

秘密共享是应用密码学领域的研究热点[1-4],它改变了传统的单人加密/解密、签名和认证模式,可防止伪造欺骗攻击,提升重要信息分存和传输的安全性。可视秘密分享(Visual Secret Sharing,VSS)是由 Naor 等[5]于 1994 年在欧洲密码学年会上提出的一种新兴图像秘密共享技术,它将数字图像处理和秘密共享相结合,通过逐像素点编码处理,将秘密图像加密成共享份,依据存取结构将共享份分为授权子集和禁止子集两部分,在秘密恢复时将符合条件的共享份进行叠加,通过人眼直接解密秘密信息,具有一次一密、解密复杂度低、信息容量大等优点,受到了学者们的广泛关注[6]。现有方案根据分享密图数量,可以分为单秘密可视分享和多秘密可视分享(Visual Multi-secret Sharing,VMSS)两类。进一步,依据授权子集与秘密图像之间的关系,常见的 VMSS 包括两类:存取式多秘密分享(Access-based VMSS,AVMSS)和操作式多秘密分享(Operation-Based VMSS,OVMSS)。文献[7]设计了一种适用于(n,n)门限结构的 AVMSS,要求所有参与者都在场时才能恢复秘密信息,因此应用场景受限。文献[8-10]设计了一种基于随机栅格的 AVMSS,适用于任意(k,n)门限结构,其共享份是大小与原图像相等的光栅,将它们叠加在一起,利用黑白区域的光通量不同来显示秘密信息。虽然共享份不存在像素扩展,但恢复图像存在信息损失,影响了视觉效果,且一个授权集合只能恢复一个秘密,而单个秘密可由多个授权集合恢复。相比之下,OVMSS 通过共享份的旋转或平移叠加操作,来实现通过一个授权子集恢复多个秘密。因此,存取式 AVMSS 分享的秘密图像有限,而操作式 OVMSS 可实现多秘密的分享。

然而,目前操作式分享方案的研究受限于$(2,2,n)$存取结构,即 n 个参与者中的任意 2 个拿出持有的共享份进行恢复时,通过旋转和叠加操作最多能恢复 2 幅秘密图像。Wu[11]和 Chen[12]首先提出一种(2,2,2)方案,通过 2 个共享份的旋转和叠加解密 2 幅图像;但其旋转或翻转操作存在角度限制,恢复图像存在外形比例失真的问题。为此,Hsu 等[13]将矩形共享份首尾相接拼成环状,解决了共享份旋转时的角度限制问题,提高了恢复效果,但只能分享 2 幅秘密图像。在此基础上,Fu 等[14]提出了地位对等的共享份设计思想,通过对共享份进行区域标记,结合(2,2)单秘密方案,提出了一种改进的 OVMSS,为增加参与者数量提供了可能。但上述方案均未突破 $n(n>2)$个共享份参与恢复的 OVMSS。

为解决秘密恢复时的共享份数量限制问题,本文设计了基础矩阵并定义了恢复过程中的图像旋转规则,提出了非遮盖式 OVMSS;基于异或(XOR)运算构造基础矩阵,设计了基于 XOR 的非遮盖操作式(k,n)可视多秘密分享,增加了参与者的数量,提高了恢复图像的清晰度。

2　基本概念

为解决秘密恢复时的共享份数量限制问题,本文设计了基础矩阵并定义了恢复过程中的图像旋转规则。

定义 1　若一个(k,n)-OVMSS 成立,OVMSS 需要满足以下两个条件:

1)(安全性)低于 k 个共享份进行恢复时,无法显示秘密图像的任何信息,形式化表示为:

$\forall X\in P,|X|<k$

满足 $H(V(X,M_0,\oplus))=H(V(X,M_1,\oplus))$

2)(对比性)任意 k 个共享份进行旋转和叠加操作,能够解密出对应的秘密信息,形式化表示为:

$\forall X\in P,|X|=k$

满足$\sum_{j=1}^{k}E[w(1,i,j)]\geqslant\sum_{j=1}^{k}E[w(0,i,j)]$

条件 1)表明,不符合条件的共享份组合以任意角度旋转都不能得到秘密信息。条件 2)表明,符合条件的共享份组合按照共享份旋转规则进行“异或”(⊕)叠加时,叠加图像中原黑像素对应子像素块的汉明重量期望值,高于原白像素对应子像素块的汉明重量期望值,人眼能直接识别出秘密信息。

可视秘密分享方案的两个评价参数[15]为像素扩展度 m 和相对差 α。

1)m 表示原图像中单个像素点在分享图像中对应子像素块包含的像素点个数,即恢复图像相比原图像在面积上扩展的倍数。m 越大表示面积失真越大,存储共享份的开销越大。

2)α 表示恢复图像中,原黑像素对应子像素块的汉明重量最小值 l 与原白像素对应子像素块汉明重量最大值 h 之差,与像素扩展度 m 之比,即 $\alpha=(l-h)/m$,其中 $\alpha\in[0,1]$。当 $\alpha=0$ 时,表示黑白像素的灰度值相等,完全不能辨别出原图像,即无法识别秘密信息;当 $\alpha=1$ 时,代表恢复图像中的黑白像素完美恢复,是最理想的情况。

定义 2　设有 h 幅秘密图像,尺寸大小为 $HT\times WT$ 个像素。秘密图像中的一个像素对应共享份中的一个子像素块,每个子像素块被划分成 h 个纵向区域,如图 1 所示。

第	第	第	第	第
1	2	…	h-1	h
区域	区域	区域	区域	区域

图 1　子像素块区域划分

Fig. 1　Subdivision of sub-pixel blocks

为便于方案设计,将所有秘密图像按列标记,如图 2 所示。

1	2	3	…	WT
1	2	3	…	WT
…	…	…	…	…
1	2	3	…	WT

图 2　秘密图像按列进行像素标记

Fig. 2　Secret image is pixel-marked by column

定义 3　令 $R(X_i,(i-1)(p-1))$为循环右移函数,用于将共享份 X_i 以子像素块为单位循环右移$(i-1)(p-1)$次$(1\leqslant i\leqslant n,1\leqslant p\leqslant h)$,$X_i$ 表示第 i 个共享份,S_p 表示第 p 幅秘密图像。

3　方案设计

本节设计了一种面向门限结构的非遮盖操作式可视多秘密分享方案,下文将分别介绍秘密分享和恢复流程。

3.1　秘密分享

基础矩阵的构造是秘密分享的核心步骤，算法 1 给出了非遮盖操作式 OVMSS 的基础矩阵构造思路，通过改进现有方法中旋转角度的限制，将其推广至(k,n)方案。算法 1 中，基础矩阵$(\boldsymbol{M}_0,\boldsymbol{M}_1)$的生成步骤如下。

算法 1　基础矩阵生成算法

输入：门限结构(k,n)，n≥k≥2

输出：基础矩阵$(\mathbf{M}_0,\mathbf{M}_1)$

Step1　对于所有偶数 p(0≤p≤k)，若 p>k－p，则 q＝n－k＋p，否则 q＝p，然后将所有含 q 个 1 的列向量加入 $\mathbf{M}_0$ 中。

Step2　对于所有奇数 p(0≤p≤k)，若 p>k－p，则 q＝n－k＋p，否则 q＝p，然后将所有含 q 个 1 的列向量加入 $\mathbf{M}_1$ 中。

Step3　当 $\mathbf{M}_0$ 和 $\mathbf{M}_1$ 中对应任意 k 行有多余列时，转至 Step 1－Step 2；将 $\mathbf{M}_1$ 中多余列经同样的方法添加至 $\mathbf{M}_0$，生成新的 $\mathbf{M}_0$；将 $\mathbf{M}_0$ 中多余列运用同样的方法添加至 $\mathbf{M}_1$，生成新的 $\mathbf{M}_1$。

Step4　若 $\mathbf{M}_0$ 和 $\mathbf{M}_1$ 中多余列相同时，该步骤结束，否则转至 Step 1。

Step5　生成和输出基础矩阵 $\mathbf{M}_0$ 和 $\mathbf{M}_1$，算法结束。

在秘密分享具体实施时，依据表 1 中共享份旋转规则对共享份旋转角度进行控制，并利用算法 1 生成的基础矩阵对各共享份中的像素点进行赋值。基本思路如下：首先针对每幅秘密图像，依次遍历所有像素点，对各像素点进行加密处理。设有 h 幅尺寸均为 $HT\times WT$ 的原始秘密图像，记为 S_1，$S_2,\cdots,S_h$，满足 $WT \bmod h\equiv 0$；生成 n 个共享份，记为 X_1，$X_2,\cdots,X_n$，其中任意 $k(k\in[2,n])$个共享份叠加可恢复秘密图像。然后，根据(k,n)基础矩阵构造方法得到大小为 $n\times l$ 的基础矩阵 $\boldsymbol{C}_0$ 和 $\boldsymbol{C}_1$。秘密图像中每个像素点对应共享份中的相应子像素块，因此每份共享份包括 $HT\times WT$ 个子像素块，每个子像素块的大小为 $l\times h$；最后，在进行分享时不同共享份要按一定规则进行右移变换，再利用基础矩阵 $\boldsymbol{C}_0$ 和 $\boldsymbol{C}_1$，经列变换和转置后按列分享到每个共享份中对应子像素块的对应标记列，从而完成秘密分享。

表 1　共享份旋转规则

Table 1　Rotation rules for shares

	S_1	S_2	…	S_p	…	S_h
X_1	0	0	…	0	…	0
X_2	0	1	…	$p-1$	…	$h-1$
X_3	0	2	…	$2(p-1)$	…	$2(h-1)$
X_4	0	3	…	$3(p-1)$	…	$3(h-1)$
…	…	…	…	…	…	…
X_i	0	$i-1$	…	$(i-1)(p-1)$	…	$(i-1)(h-1)$
…	…	…	…	…	…	…
X_n	0	$n-1$	…	$(n-1)(p-1)$	…	$(n-1)(h-1)$

基于上述思路，本文设计了(k,n)-OVMSS 的秘密分享流程，具体步骤如算法 2 所示。

算法 2　秘密图像分享算法

输入：秘密图像 $S_1,S_2,\cdots,S_h$

输出：共享份 $X_1,X_2,\cdots,X_n$

Step1　依据 k,n 门限值，结合算法 1 构造基础矩阵 $\mathbf{M}_0$ 和 $\mathbf{M}_1$；

Step2　按顺序依次选择秘密图像 S_p(1≤p≤h)，并对其进行分享；

Step3　按照定义 2 对秘密图像和未赋值共享份进行标记，并按照旋转规则(表 1)对共享份进行加密分享；

Step4　选择任意一个像素点，若为白(黑)色，则选基础矩阵 $\mathbf{M}_0$($\mathbf{M}_1$)；

Step5　对基础矩阵进行列变换，得 $\mathbf{C}_t=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1l} \\ a_{21} & a_{22} & \cdots & a_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nl} \end{bmatrix}$(t∈{0,1})，再将 $\mathbf{C}_t$ 转置，得 $\mathbf{C}_t^{\mathrm{T}}$；

Step6　将 $\mathbf{C}_t^{\mathrm{T}}$ 的第 j(j＝1,2,…,n)列填入第 j 个共享份对应子像素块的第 p 列；

Step7　若秘密图像未全部分享完，则返回 Step2，否则该步骤结束；

Step8　生成和输出共享份 $X_1,X_2,\cdots,X_n$，算法结束。

上述算法的关键步骤是 Step 3－Step 4，为利用环形共享份的处理，依据定义 2 在 Step 3 中对所有秘密图像的像素点进行纵向区域划分和标记，然后逐区域进行像素加密。

3.2　秘密恢复

秘密恢复时，从 n 幅共享份中任意选择 k 个 $X_q,X_{q+1},\cdots$，X_{q+k-1}($q\in\lceil 1,n+1-k\rceil$)。在解密图像 S_p 时，利用表 1 的旋转规则将这 k 幅共享份进行旋转操作，即共享份 X_i($i\in\lceil q,n+1-k\rceil$)向右旋转$(i-1)(p-1)$个子像素块，最后 XOR 叠加所有共享份恢复出秘密图像 S_p。

3.3　实例分析

下文以(3,4)门限结构下同时分享 3 幅秘密图像为例，说明秘密分享和恢复过程。S_1,S_2,S_3 是 3 幅秘密图像，如图 3 所示。

图 3　3 幅原始秘密图像

Fig. 3　Three original secret images

依据算法 2 的流程，依次对各秘密图像进行分享：X_1^1，X_2^1,X_3^1,X_4^1 是分享 S_1 后得到的过渡共享份，如图 4 所示，阴影部分表示还未赋值的部分；X_1^2,X_2^2,X_3^2,X_4^2 是分享 S_2 后的过渡共享份，如图 5 所示；X_1^3,X_2^3,X_3^3,X_4^3 是分享 S_3 后得到的最终共享份，如图 6 所示。

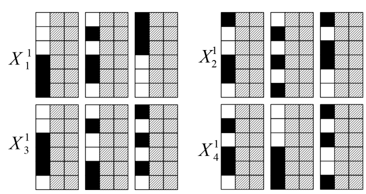

图 4　分享 S_1 后的过渡共享份

Fig. 4　Interim shares of sharing S_1

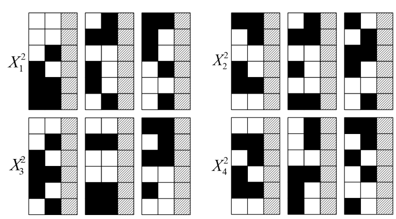

图 5　分享 S_2 后的过渡共享份

Fig. 5　Interim shares of sharing S_2

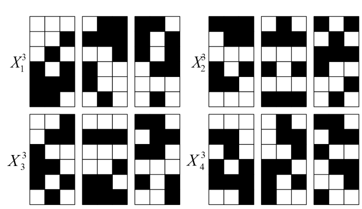

图 6　分享 S_3 后的过渡共享份

Fig. 6　Interim shares of sharing S_3

依据 3.2 节中的秘密恢复方法，选择其中 X_1^3,X_2^3,X_3^3 3 个共享份进行恢复操作，结果如图 7 所示，XOR 叠加 X_1^3,X_2^3,X_3^3 得到 S_1'，可恢复图 3 中的原始图像 S_1；XOR 叠加 X_1^3，$R(X_2^3,1)$，$R(X_3^3,2)$ 得到 S_2'，可恢复图 3 中的原始图像 S_2；XOR 叠加 X_1^3，$R(X_2^3,2)$，$R(X_3^3,4)$ 得到 S_3'，可恢复图 3 中的原始图像 S_3。以 S_1' 为例，由左至右各像素块的汉明重量依次为 9，7，9，因此相比左右两个像素块，中间像素块包含白像素最多，视觉系统会整体识别该区域为白色，与图 3 中的原始秘密图像 S_1 相符。

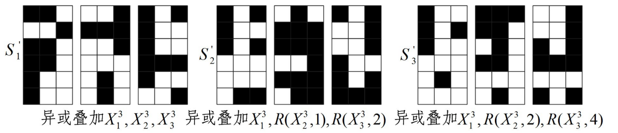

图 7　秘密恢复图像

Fig. 7　Secret recovery image

4　方案有效性证明

由定义 1 可知，可视秘密分享的有效性包含两方面：安全性和对比性。在本方案中，安全性表示不满足门限条件的共享份叠加后不会泄露秘密信息；对比性表明符合门限条件的共享份叠加后，由人眼可以直接识别秘密信息。

定理 1（安全性）　单份共享份不会泄露任何秘密信息。

证明：原秘密图像的单个黑白像素都分享为一黑一白两个子像素，且由算法 1 中的 Step 5 可知，各秘密像素对应的子像素排序都是随机生成的，结合信息熵理论可知，$H(S_i|A_1)=H(S_i|A_2)=\cdots=H(S_i|A_n)=H(S_i)$，其中 H 表示熵，表明通过单个共享份推测秘密图像等价于直接猜测秘密图像，因此单个共享份不会泄露秘密信息，得证。

定理 2（安全性）　少于 k 个人恢复时，无法得到秘密图像，即 $\forall X\in P, H(\boldsymbol{V}(X,\boldsymbol{M}_0,\oplus))=H(\boldsymbol{V}(X,\boldsymbol{M}_1,\oplus))$。

证明：共享集合 $K=\{i_1,i_2,\cdots,i_n\}$ 时，定义授权集合为 Q（$Q\subseteq K$ 且 $|Q|\geqslant k$），非授权集合为 P（且 $|P|<k$），对于任意参与者集合 $X\subseteq K=\{i_1,i_2,\cdots,i_p\}$，记 $\boldsymbol{V}(X,\boldsymbol{M},\oplus)$ 为矩阵 $\boldsymbol{M}$ 中 X 的分量所在行向量“XOR”运算得到的向量。即需要证明基础矩阵（$\boldsymbol{M}_0,\boldsymbol{M}_1$）满足 $H(\boldsymbol{V}(X,\boldsymbol{M}_0,\oplus))=H(\boldsymbol{V}(X,\boldsymbol{M}_1,\oplus))$，表明基础矩阵不泄露秘密信息，则证明该方案是安全的。由基础矩阵的构造可知，$\boldsymbol{M}_0$（$\boldsymbol{M}_1$）中任意 k 行包含所有的偶数（奇数）列及相同列。相同列使二者增加相同的汉明重量，不影响汉明重量的差异，因此只需考虑偶数列与奇数列。不妨以 $\boldsymbol{M}_0,\boldsymbol{M}_1$ 中任意 $q(q<k)$ 行为例，对于所有长度为 q 的奇数列向量，意味着 $\boldsymbol{M}_0,\boldsymbol{M}_1$ 中任意 $q(q<k)$ 行组成的矩阵为相同的矩阵（即可通过列交换相互转换）。这样，任意 $q(q<k)$ 行 XOR 运算所得到的汉明重量相等，即 $\forall X\in P, H(\boldsymbol{V}(X,\boldsymbol{M}_0,\oplus))=H(\boldsymbol{V}(X,\boldsymbol{M}_1,\oplus))$，得证。

定理 3（对比性）　共享份 X_1 与其他任意（$k-1$）个旋转后的共享份叠加后，可以恢复秘密图像 S_i，即 $\forall X\in P, |X|=k, \sum_{j=1}^{k}E[w(1,i,j)]\geqslant\sum_{j=1}^{k}E[w(0,i,j)]$。

证明：设 $w(0,i,j)$（$w(1,i,j)$）表示叠加共享份后，原白（黑）像素在秘密图像 S_i 中对应子像素块中区域 j 的汉明重量，其中 $E[w(0,i,j)]$（$E[w(1,i,j)]$）表示 $w(0,i,j)$（$w(1,i,j)$）的数学期望值，$E[w(0,i,j)]$（$E[w(1,i,j)]$）表示共享份 X_1 与剩余任意（$k-1$）个共享份旋转叠加后，原白（黑）像素在 S_i 中对应的子像素块的汉明重量的数学期望值，因此 $E[w(0,i,\Sigma)]=\sum_{j=1}^{k}E[w(0,i,j)]$，（$E[w(1,i,\Sigma)]=\sum_{j=1}^{k}E[w(1,i,j)]$），$1\leqslant i,j\leqslant h$。

依据算法 1 的基础矩阵生成流程可知，当参与者个数等于 k 时，基础矩阵 $\boldsymbol{M}_0$（$\boldsymbol{M}_1$）中任意 k 行包含所有的偶数（奇数）列及相同列，所有的偶数列异或后得到 2^{k-1} 个 0，所有的奇数列异或后得到 2^{k-1} 个 1，又因为其余列均相同，所以 $w(1,i,j)-w(0,i,j)=2^{k-1}$，故 $\sum_{j=1}^{k}E[w(1,i,j)]\geqslant\sum_{j=1}^{k}E[w(0,i,j)]$，得证。

综上，由定理 1 及定理 2 可知，本文方案满足定义 1 中的条件 1），符合安全性条件；由定理 3 可知，本文方案满足定义 1 中的条件 2），符合对比性条件，理论证明本文方案有效。

5　实验分析

以（3，4）-OVMSS 为例验证本文方案的有效性。图 8 给出了待分享的 3 个秘密图像，利用 2.1 节秘密分享算法生成 4 个共享份，任意选取其中 3 个，依据 2.2 节秘密恢复方法得到秘密图像，如图 8 所示。

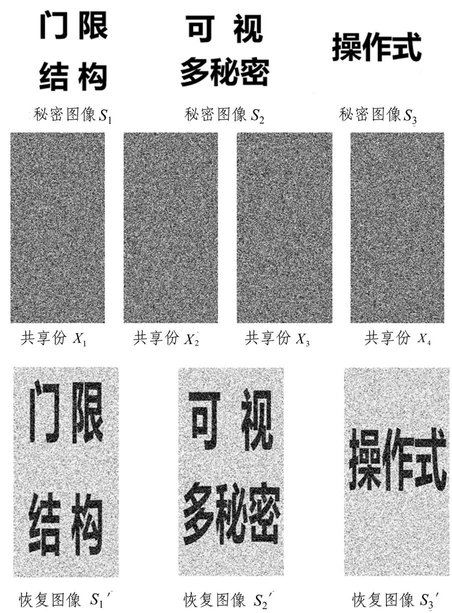

图 8　（3，4）-OVMSS 的实验结果

Fig. 8　Experimental results of (3,4)-OVMSS

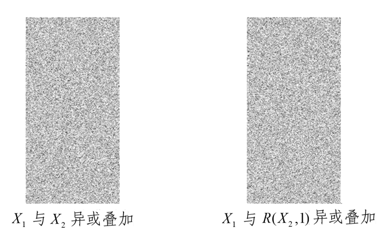

图 9　两个共享份的秘密恢复结果

Fig. 9　Secret recovery results of superimposing two shares

从图中可以看出，单个共享份 X_1,X_2,X_3,X_4 是杂乱无章的，不会显示任何秘密信息。对于共享份数量小于门限值的情况，由图 11 可以看出，当 2 个共享份进行恢复时，例如将

X_1 与 X_2 进行叠加，或者将 X_1 与 $R(X_2,1)$ 进行叠加，都无法显示秘密信息，验证了本文方案的安全性。当 3 个共享份进行恢复时，依据 2.2 节中的秘密恢复流程，$X_1^3 \oplus X_2^3 \oplus X_3^3$ 能恢复秘密图像 S_1'，$X_1^3 \oplus R(X_2^3,1) \oplus R(X_3^3,2)$ 能恢复 S_2'，$X_1^3 \oplus R(X_2^3,2) \oplus R(X_3^3,4)$ 能恢复 S_3'，验证了本文方案的对比性。

表 2 列出了本文方法与现有方法的综合比较。在存取结构方面，本文和文献[18]适用于任意 (k,n) 门限结构，而文献[14,16-17]仅适用于(2,2)结构。在共享份关系方面，相比文献[16-17]，本文和文献[14,18]产生的共享份在恢复过程中的地位是对等的，为增加参与者数量创造了条件。在分享秘密图像数量方面，本文可以恢复 $h(h \leqslant WT)$ 幅秘密图像，文献[14,17-18]和本文的分享数量明显多于文献[16]。在像素扩展方面，本文的像素扩展度为 mh，小于存取式方案[18]，由于文献[18]中的一个授权集合只能解密一幅图像，而本文中的一个授权集合可以恢复出多幅图像，因此像素扩展度较小，节省了存储开销。当 $k=2$，$n=2$ 时，本文像素扩展度为 $2h$，与文献[14]相等，因此文献[14]是本文的一个特例；文献[16-17]的像素扩展较高，增加了共享份图像的存储和传输开销。在恢复图像相对差方面，本文方案的相对差为 α/h，高于文献[14]中的方法，当 $k=2$，$n=2$ 时，本文方法的相对差为 $1/h$，高于文献[14,16-18]，因此恢复图像更清晰。由于本文基于 XOR 运算设计，本质上是群代数结构，原始图像中表示白像素的 0 存在逆元，提高了白像素的恢复概率，改善了秘密恢复效果。

表 2　本文方案与其他方案的性能比较

Table 2　Performance comparison among proposed scheme with others

类型	秘密图像数量	像素扩展度	相对差	共享份之间的关系	存取结构
文献[14]	h	$2h$	$1/(2h)$	对等	(2,2)
文献[16]	4	9	1/9	不对等	(2,2)
文献[17]	h	$3h$	$1/(3h)$	不对等	(2,2)
文献[18]	h	$\sum_{i=1}^{h} m_i$	$1/\sum_{i=1}^{h} m_i$	对等	(k,n)
本文	h	mh	α/h	对等	(k,n)

结束语　本文设计了一种面向门限结构的操作式可视多秘密分享方案，适用于任意 (k,n) 结构，与已有方案相比，通过在秘密分享时对秘密图像进行划分和标记纵向区域，实现了所有共享份地位对等，提高了可分享秘密的数量，最多可以同时将 WT 幅秘密图像分享到 k 个环形共享份中，该方案在满足安全条件的前提下，增强了相对差，改善了秘密图像的恢复效果。如何进一步实现秘密图像的完全恢复是未来的研究重点。

参考文献

[1] SHAO L P, LE Z F. Multiple Thresholds Progressive Secret Image Sharing Scheme Based on DCT[J]. Netinfo Security, 2018, 18(3): 54-62.

[2] XIONG J B MA R, ZHANG Y Y, et al. Image Information Hiding Method and Implementation for Social Network[J]. Netinfo Security, 2017, 17(3): 6-8.

[3] ZHANG Y S, WANG X M, QIU G G. Research on a New Dynamic Threshold Digital Signature Scheme[J]. Netinfo Security, 2016, 16(6): 62-67.

[4] LI Z H, XU T T, ZHANG N. The Construction of a Type of Ideal Access Structures[J]. Netinfo Security, 2016, 16(5): 15-22.

[5] NAOR M, SHAMIR A. Visual cryptography[C]// Advances in Cryptology-Eurocrypt'94. Lecture Notes in Computer Science, 1995, 950: 1-12.

[6] HU H, SHEN G, YU B, et al. XOR-based region incrementing visual cryptography scheme by random grids[J]. Chinese Journal of Computer Research and Development, 2016, 53(8): 1857-1866.

[7] KABIRIRAD S, ESLAMI Z. Improvement of (n,n)-multi-secret image sharing schemes based on Boolean operations[J]. Journal of Information Security and Applications, 2019, 47: 16-27.

[8] YAN X, XIN L, YANG C. An enhanced threshold visual secret sharing based on random grids[J]. Journal of Real-Time Image Processing, 2018, 14(1): 61-73.

[9] MEGHRAJANI Y, DESAI L, MAZUMDAR H. Secure and efficient arithmetic-based multi-secret image sharing scheme using universal share[J]. Journal of Information Security and Applications, 2019, 47: 267-274.

[10] JOY C, HUANG B, JUAN J. A new visual multi-secrets sharing scheme by random grids[J]. Cryptography, 2018, 2(3): 24.

[11] WU Z. Two new visual cryptography schemes: visual multi-secrets sharing scheme and colored visual secret sharing scheme [D]. Taiwan: National Dong Hwa University, 2001.

[12] CHEN L. A study on visual cryptography[D]. Taiwan: National Chiao Tung University, Master Thesis, 1998.

[13] HSU H, CHEN T, LIN Y. The ring shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing[C]// Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control. 2004: 996-1001.

[14] FU Z X, YU B. Ideal secure multi-secret visual cryptography scheme with ring shares[M]. Transactions on Data Hiding and Multimedia Security IX. Springer, Berlin, Heidelberg, 2014: 42-56.

[15] DROSTE S. New results on visual cryptography[C]// Advances in Cryptography-CRYPTO'96. 1996, LNCS 1109: 401-415.

[16] FU Z X, YU B. Research on rotation visual cryptography scheme[C]// Proceedings of the International Symposium on Information Engineering and Electronic Commerce. IEEE, 2016: 533-536.

[17] FENG J, WU B H, TSAIC C, et al. Visual secret sharing for multiple secrets[J]. Pattern Recognition, 2010(41): 3572-3581.

[18] SHEN G. Analysis and design of visual cryptography scheme [D]. Strategic Support Force Information Engineering University, 2017.

DONG Chen, born in 1976, master, is a member of China Computer Federation. Her main research interests include digital image processing, data mining and visual secret sharing.