解密区域完美恢复的区域递增式视觉密码方案构造

胡 浩* 郁 滨 沈 刚 张学思
(信息工程大学 郑州 450001)

摘 要：为了优化区域递增式视觉密码的恢复效果，该文通过为共享份添加身份标识，并结合随机数，构造了单个参与者持有多个共享份的异或单秘密视觉密码方案，在此基础上，设计了异或区域递增式视觉密码的秘密分享与恢复算法。对于解密区域利用异或单秘密方案进行分享，对于未解密区域，通过填充随机数实现秘密遮盖。实验结果表明，该方案可以实现解密区域图像的完美恢复，且有效减小了共享份的存储与传输开销。

关键词：视觉密码；图像秘密分享；区域递增；密级；异或运算；完美恢复
中图分类号： TP309.7 **文献标识码**： A **文章编号**：1009-5896(2016)10-2647-07
DOI: 10.11999/JEIT151448

Region Incrementing Visual Cryptography Scheme with Decrypt Regions Perfectly Recovered

HU Hao YU Bin SHEN Gang ZHANG Xuesi
(*Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: In order to optimize the recovery quality of Region Incrementing Visual Cryptography Scheme (RIVCS), by adding identities for shares and combing the random numbers, an XOR-based single-secret sharing Visual Cryptography Scheme (XVCS) with individual participant holding multi-share is designed. On basis of this, the secret sharing and recovering algorithms for XOR-based RIVCS (XRIVCS) are designed. For the decrypt regions, XVCS is used to share, and for the not decrypt regions, the random numbers are filled to keep the secret. The experimental results show that, the proposed scheme can realize the perfect recovery of decrypt regions, and decrease the storage and transmission cost effectively.

Key words: Visual cryptography; Image secret sharing; Region incrementing; Security levels; XOR operation; Perfect recovery

1 引言

多秘密视觉密码方案(Multi-secret Visual Cryptography Scheme, MVCS)主要用来分享多幅独立的秘密图像[1–4]，与 MVCS 不同，区域递增式视觉密码方案[5](Region Incrementing VCS, RIVCS)将一幅秘密图像划分为多个区域，不同区域具有不同的图像，区域恢复的数量与参与者人数有关，参与者人数越多，恢复区域的数目越多，在信息的分级管理、多密级访问控制领域有着广阔的应用前景。

文献[5]设计了存取结构为$(2,n)$的基于或运算(OR)的区域递增式视觉密码方案(OR-based RIVCS, ORIVCS)，将一幅秘密图像划分 $n-1$ 个区域，共享份以透明胶片作为载体，秘密恢复时叠加(相当于 OR 运算)任意 $2 \le t \le n$ 个共享份可以解密 $t-1$ 个区域的秘密信息，但参与者人数 n 仅局限于 3, 4, 5。文献[6]建立加密矩阵的线性规划模型，并构造了像素扩展度最优的$(2,n)$方案，但模型计算复杂度随着 n 的增加呈指数级增长。文献[7–9]通过拼接基于或运算的(t,n)单秘密方案(OR-based VCS, OVCS)$(k \le t \le n)$的加密矩阵，突破了$(2,n)$结构的限制，提出了像素扩展度优化的(k,n)-ORIVCS 加密矩阵的设计方法，但恢复图像的色彩存在反转失真问题。文献[10]实现了恢复图像的不同区域对比度相等，解决了现有方案与传统黑白二值视觉密码不兼容的问题，但像素扩展度仍需进一步优化。

上述方案主要依靠构造精简的加密矩阵来降低像素扩展度，各区域加密矩阵本质上是单秘密方案[11]加密矩阵的线性组合，因而随着 k 和 n 的增加，矩阵规模迅速增加，像素扩展度急剧增大，恢复图像的效果也随之降低。为了减小像素扩展度，文献[12]提出了基于随机栅格(Random Grid, RG)的视

收稿日期：2015-12-22；改回日期：2016-05-26；网络出版：2016-07-14
*通信作者：胡浩 wjjhh_908@163.com
基金项目：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)
Foundation Items: The National Natural Science Foundation of China (61070086), The Foundation of Science and Technology on Information Assurance Laboratory of China (KJ-13-107)

觉密码，共享份是大小与原图像相等的光栅，将它们叠加在一起，利用白黑区域的光通量不同来显示秘密图像，在此基础上，文献[13,14]给出了多种(k, n)-ORIVCS 的构造方法。随机栅格可以有效控制像素扩展，但该类方案的恢复图像中，原秘密图像黑白像素以一定的概率被正确恢复，因此恢复图像的信息熵存在损失。

通过梳理以上研究成果不难发现，现有方案着重于研究如何降低像素扩展度，对于如何提高恢复效果未能给出有效的解决方案，本质上此类构造方法主要局限于 OR 运算，由于 OR 运算$(1\otimes 1=1, 0\otimes 1=1)$的特点，致使黑像素(1)没有逆元，半群的代数结构导致原始白像素(0)无法被正确恢复。为了改善单秘密 OVCS 的恢复效果，文献[15]将异或运算(XOR)引入视觉密码，给出了基于异或运算的视觉密码方案(XOR-based VCS, XVCS)[16]的定义，并设计了(n, n)-XVCS，利用$(1\oplus 1=0)$，提高了白像素的恢复概率。

文献[17]利用XOR运算的{0,1}群中0作为单位元的性质，设计了一种 XRIVCS，当所有共享份叠加时，白像素的恢复概率为 1，但黑像素无法完美恢复。文献[18]分析了 OR 运算和 XOR 运算的特性，指出由于 XOR 运算存在奇偶特性(奇数个 1 的运算结果为 1，偶数个 1 的运算结果为 0)，即偶数个黑像素进行运算后恢复成白像素，导致原始黑像素的颜色产生反转，因而很难直接应用到目前 RIVCS 的构造方法中。

针对上述问题，本文通过给共享份添加身份标识，分享过程避开加密矩阵，直接结合随机数生成共享份，恢复过程依据身份标识出示对应共享份，构造了单个参与者持有多个共享份的单秘密 XVCS。在此基础上，结合不同授权子集完成 RIVCS 的共享份的赋值过程，对于任意授权子集对应解密区域利用 XVCS 进行分享，对于未解密区域，通过填充随机数实现遮盖，能够保持各区域分享的独立性，从而克服 XOR 运算产生的像素反转。实验结果表明，本文设计的基于异或运算的区域递增式视觉密码方案(XOR-based RIVCS, XRIVCS)能够实现解密区域图像的完美恢复，且进一步降低共享份的存储及传输开销。

2 基本概念

为方便描述，文中所用符号及含义见表 1。

定义 1[19] 记参与者集合$P=\{1,2,\cdots,n\}$，称能够恢复秘密图像的参与者集合为授权子集，记为Γ_Q，不能恢复秘密图像的参与者集合为禁止子集，记为Γ_F，满足$\Gamma_Q\subseteq 2^P$,$\Gamma_F\subseteq 2^P$，且$\Gamma_Q\bigcap\Gamma_F=\varnothing$。

表 1 主要符号及其含义

符号	含义	符号	含义
P	所有参与者集合	X	任意参与者集合
Γ_Q	授权子集集合	Γ_F	禁止子集集合
Γ_0	最小授权子集集合	Q	授权子集
F	禁止子集	K	最小授权子集
n	参与者总数	k	秘密恢复门限值
S	秘密图像	R_j	S 中的第 j 块区域
$\Re$	随机数序列	T_i^Q	第 i 个参与者的标识为 Q 的共享份
$\otimes$	OR 运算	$\oplus$	XOR 运算
$\cup$	图像拼接操作	$\|X\|$	集合 X 中的参与者数量
$R(X)$	秘密恢复函数	m	单个共享份的像素扩展度
h	单个参与者持有共享份的数量	TSE	单个参与者的共享份像素扩展度总和

记$\Gamma_0=\{X\in\Gamma_Q:\forall X'\subset X\Rightarrow X'\notin\Gamma_Q\}$，称$\Gamma_0$为最小授权集合。$(k,n)$门限结构是一类特殊的存取结构，满足$\Gamma_F=\{F\|F|<k\}$, $\Gamma_Q=\{Q\|Q|\geq k\}$, $\Gamma_0=\{K||K|=k\}$。

不同于以往方案[17]，本文提出的方案中单个参与者持有多个共享份，每个共享份有不同的标识，秘密恢复时，不同参与者依据恢复集合出示对应标识的共享份来完成秘密恢复，下面给出参与者持有多个共享份的 XRIVCS 的定义。

定义 2 设 n 表示参与者总数，k 表示秘密恢复门限值，满足$n\geq k\geq 2$，秘密图像 S 划分了 d 个区域 R_j，$1\leq j\leq d$，$d=n-k+1$，即 $S=R_1\cup R_2\cup\cdots\cup R_d$。$(k, n)$是参与者集合 P 上的门限结构，设T_i^Q表示参与者 i 持有的标识为 Q 的共享份，$1\leq i\leq n$,$Q\in\Gamma_Q$，记任意参与者集合$X=\{i_1,i_2,\cdots,i_x\}$，函数$R(X)=T_{i_1}^X\oplus T_{i_2}^X\oplus\cdots\oplus T_{i_x}^X$为秘密恢复函数，表示对 X 中参与者持有的标识为 X 的共享份进行 XOR 运算，若一个(k, n)-XRIVCS 成立，则满足以下 2 个条件：

(1)当$|X|<k$时，集合 X 中的参与者无论出示任何共享份也无法恢复秘密信息。

(2)当$|X|=j+k-1$时，集合 X 中的参与者 XOR 运算标识为 X 的共享份可以恢复区域$R_1\cup R_2\cup\cdots\cup R_j$的秘密信息。

其中，条件(1)是安全性条件，保证当参与者人数小于 k 个时，得不到秘密图像的任何信息。条件(2)是对比性条件，表明$j+k-1$个参与者最多可以恢复区域 R_j。若 $R(X)$ 中解密区域图像与原始图像完全一致，称该方案的解密区域是完美恢复的。

关于定义 2 的两点补充说明：

(1)考虑到严格的视觉密码方案，在秘密恢复前应该对共享份的真实性进行认证，因而在秘密恢复时，参与者可以提前知道恢复集合，能够依据恢复集合来判别出示某个共享份，因此参与者持有多个共享份的分享方式是合理的。

(2)本文方案成立的前提条件是每个参与者都是可信的，因此不单独考虑欺骗者存在的情形，这也是大部分视觉密码方案设计的前提，故单个参与者持有多个共享份的设计方法不会降低方案的安全性。

定义 3　设单个共享份的像素扩展度为 m，单个参与者持有共享份数量为 h，则单个参与者持有共享份的像素扩展度总和(Total Size Expansion, TSE)满足 $\mathrm{TSE}=m\times h$。

若秘密图像尺寸大小一定，则 TSE 和 m 可用来衡量方案的存储和传输开销，TSE 值越小，表明保存共享份所需的存储空间越小，m 值越小，表明秘密恢复时，占用通信带宽资源产生的传输开销越小。

3　方案设计

由于区域递增式视觉密码是在单秘密分享视觉密码的基础上构造的，因此，本节先给出一种单秘密(k,n)-XVCS 的共享份生成算法，在此基础上，设计 XRIVCS 的秘密分享与恢复流程。

3.1 XVCS 的共享份生成算法

定义空白共享份尺寸大小与秘密图像 S 相同，依次为每个最小授权子集 $K\in\Gamma_0$ 中的参与者分发标识为 K 的共享份，利用秘密图像和随机数共同完成空白共享份填充过程，算法步骤如下。

输入：k, n 值，秘密图像 $S(a\times b)$，$2\le k\le n$。

输出：共享份 T_i^K，$1\le i\le n$，$K\in\Gamma_0$。

步骤 1　从 Γ_0 中随机选取一个集合 $K=\{i_1, i_2,\cdots,i_k\}$，对 K 中参与者 i_t 的共享份 $T_{i_t}^K$ 进行赋值，$1\le t\le k$，具体赋值方法见图 1；

步骤 2　判断 Γ_0 中的元素是否全部遍历完毕，若是，该步骤结束，否则转到步骤 1；

步骤 3　输出步骤 1 和步骤 2 生成的所有共享份，分发给对应参与者，算法结束。

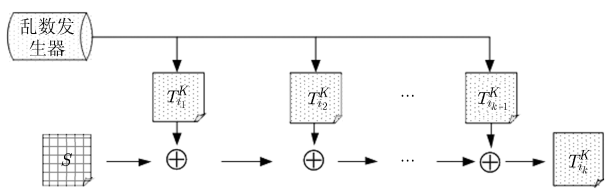

图 1 集合 K 中参与者的共享份赋值方法

共享份 $T_{i_t}^K$ 赋值的具体方法如图 1，$\Re_1,\Re_2,\cdots,\Re_{k-1}$ 表示由随机数序列$\{0,1\}^*$填充的大小为 $a\times b$ 的图像，则共享份赋值方法如下：$T_{i_t}^K=\Re_t(1\le t\le k-1)$，$T_{i_k}^K=S\oplus\Re_1\oplus\Re_2\oplus\cdots\oplus\Re_{k-1}$。

在上述算法中，有以下两点需要说明：

(1)当 XOR 运算的共享份数目达到 k 个时即可恢复秘密图像，当$|X|>k$ 时，文献[15]认为取 X 中的 k 个参与者即可恢复秘密图像，因此不需要直接计算 X 中所有的共享份。

(2)与文献[11]方案相比，本节 XVCS 中单个参与者持有多个共享份，当参与者数量达到恢复门限值时，依据恢复集合，出示相应标识的共享份来完成秘密恢复，而文献[11]中单个参与者只持有一个共享份。

3.2 XRIVCS 的秘密分享与恢复流程

在 3.1 节的基础上，本节给出 XRIVCS 的设计流程，基本思想是依次遍历区域 $R_1\cup R_2\cup\cdots\cup R_j$，$1\le j\le d$，结合该区域分享的存取结构 $\Gamma_0=\{X||X|=j+k-1\}$，利用单秘密 XVCS 进行加密，恢复时取相同标识的共享份进行异或运算，下面分别介绍秘密分享与恢复流程。

(1)秘密分享流程　秘密分享流程如图 2 所示，具体步骤如下。

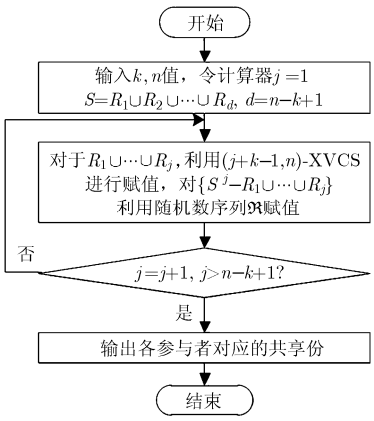

图 2　(k,n)-XRIVCS 的秘密分享流程

输入：k, n 值，秘密图像 $S=R_1\cup R_2\cup\cdots\cup R_d$，$2\le k\le n$，$d=n-k+1$。

输出：共享份 T_i^Q，$1\le i\le n$，$Q\in\Gamma_Q$。

步骤 1　输入秘密图像 S，令计数器 $j=1$；

步骤 2　初始化与 S 大小相等的空白共享份，对于区域 $R_1\cup R_2\cup\cdots\cup R_j$，$1\le j\le d$，利用 3.1 节提出的 $(j+k-1,n)$ - XVCS 的构造方法进行赋值，对于区域 $\left\{S-R_1\cup R_2\cup\cdots\cup R_j\right\}$，利用随机数序列 $\Re$ 赋值；

步骤 3 令 j=$j+1$，判断 j 是否大于 $n-k+1$，若是，该步骤结束，否则，转到步骤 2；

步骤 4 输出步骤 1–步骤 3 生成的所有共享份，分发给对应参与者，算法结束。

关于上述算法的补充说明：

步骤 2 是算法的核心，通过对解密区域和未解密区域单独进行加密，保持各部分分享的独立性，在实现区域递增式显示的前提下，可以解决像素叠加时由于异或运算产生的颜色反转问题。

(2)秘密恢复流程 对于授权集合 $Q=\{i_1,i_2,\cdots,i_q\}$，其中的参与者取标识为 Q 的共享份进行 XOR 运算，即 $R(Q)=T_{i_1}^{Q}\oplus T_{i_2}^{Q}\oplus\cdots\oplus T_{i_q}^{Q}$。

4 有效性证明

定理 1 当 $|X|<k$ 时，无法恢复出任何区域的秘密信息。

证明 设 $X=(i_1,i_2,\cdots,i_x)$，对于参与者 i_t 持有的共享份 $T_{i_t}^{Q}$，$Q\in\Gamma_Q$，$1\le t\le x<q$，由 3.1 节图 1 的共享份赋值过程可知，需要分下面两种情况进行考虑：

(1)若 $\left\{T_{i_1}^{Q},T_{i_2}^{Q},\cdots,T_{i_x}^{Q}\right\}\subset\left\{\Re_1,\Re_2,\cdots,\Re_{q-1}\right\}$，满足 $R(X)=T_{i_1}^{Q}\oplus T_{i_2}^{Q}\oplus\cdots\oplus T_{i_x}^{Q}=\Re_{i_1}\oplus\Re_{i_2}\oplus\cdots\oplus\Re_{i_x}=\Re$。

(2)若 $\left\{T_{i_1}^{Q},T_{i_2}^{Q},\cdots,T_{i_x}^{Q}\right\}\not\subset\left\{\Re_1,\Re_2,\cdots,\Re_{q-1}\right\}$，表明至少有一个共享份不在此集合中，不妨设 $T_{i_1}^{Q}=T_{q}^{Q}=S\oplus\Re_1\oplus\cdots\oplus\Re_{q-1}$，满足 $R(X)=T_{i_1}^{Q}\oplus T_{i_2}^{Q}\oplus\cdots\oplus T_{i_x}^{Q}=S\oplus\Re_1\oplus\cdots\oplus\Re_{q-1}\oplus\Re_{i_2}\oplus\cdots\oplus\Re_{i_x}=\Re$。

综上，由于情况(1)和情况(2)的结果具有随机性，$H(S|X)=H(S)$，其中 H 表示信息熵，表明无法恢复出原始图像 S，满足定义 2 的条件 1，因此集合 X 中的参与者无论出示任何共享份也无法恢复秘密信息。 证毕

定理 2 当 $|X|=j+k-1$ 时，X 中的参与者异或运算标识为 X 的共享份可以完美恢复区域 $R_1,R_2,\cdots,R_j$。

证明 由 3.2 节共享份生成算法可知，对于区域 $R_1\bigcup\cdots\bigcup R_j$，利用 $(j+k-1,n)$-XVCS 进行分享，依据 3.1 节秘密分享流程，对于任意 $X=(i_1,\cdots,i_{j+k-1})$，$T_{i_1}^{X}=\Re_1,\cdots,T_{i_{j+k-2}}^{X}=\Re_{j+k-2},T_{i_{j+k-1}}^{X}=\{R_1\bigcup\cdots\bigcup R_j\}\oplus\Re_1\oplus\cdots\oplus\Re_{j+k-2}$，满足 $R(X)=T_{i_1}^{X}\oplus\cdots\oplus T_{i_{j+k-1}}^{X}=\Re_1\oplus\cdots\oplus\Re_{j+k-2}\oplus\left\{R_1\bigcup\cdots\bigcup R_j\right\}\oplus\Re_1\oplus\cdots\oplus\Re_{j+k-2}\oplus\Re_{j+k-2}=R_1\bigcup\cdots\bigcup R_j$，由定义 2 的条件 2 可知，此时解密区域实现了完美恢复。 证毕

命题 1 (k,n)-XRIVCS 中单个参与者持有共享份数量 $h=\sum_{t=k}^{n}\begin{pmatrix}n-1\\t-1\end{pmatrix}$。

证明 由 3.2 节可知(k,n)-XRIVCS 通过(k,n) -XVCS, $(k+1,n)$-XVCS,$\cdots$,(n,n)-XVCS 构造，对于 (t,n)-XVCS$(k\le t\le n)$，不妨设最小授权子集 $K=\{i_1,i_2,\cdots,i_t\}$，参与者 i_1 持有的共享份数量为 h_t，由 3.1 节共享份生成算法可得 h_t 等于包含了参与者 i_1 的 K 的数量，即集合 $\{i_2,\cdots,i_t\}$ 的组合数，由于 $\{i_2,\cdots,i_t\}\subset\{i_2,\cdots,i_n\}$，故 $h_t=\begin{pmatrix}n-1\\t-1\end{pmatrix}$，因而参与者 i_1 持有的共享份总数 $h=\sum_{t=k}^{n}h_t=\sum_{t=k}^{n}\begin{pmatrix}n-1\\t-1\end{pmatrix}$。 证毕

5 实验与分析

5.1 方案有效性分析

本方案主要针对黑白二值图像，由于彩色和灰度图像中像素的色度阶数大于 2，因此不能直接应用于本方案。以(2,3)-XRIVCS 为例，对本文方案进行仿真实验，并与文献[6,10]的实验结果进行比较。实验图像 S 如图 3(a)所示，划分了 2 个大小不相等的区域，其中，R_1=“ABC”，R_2=“abc”。初始化与 S 大小相等的空白共享份，记 $T_i^{Q}[R_j]$ 为参与者 i 的标识为 Q 的共享份中区域 R_j 对应部分，按照 3.2 节秘密分享流程，可以得到图 3 所示的实验结果。

由图 3 所示实验结果分析可知：

(1)单个共享份(图 3(c, d, e))是杂乱无章的，无法得到任何区域的秘密信息；2 个相同标识的共享份进行异或运算后，区域 R_1 实现了完美恢复，而区域 R_2 是杂乱无章的(图 3(f))；3 个相同标识的共享份进行异或运算后，区域 R_1 和 R_2 都实现了完美恢复(图 3(g))，此时恢复图像与原图像 S 完全一致，与预期结果相同。

(2)在安全性方面，由于秘密图像中各区域划分大小不必相等，参与者无法预先知道秘密区域划分情况，因此无法根据恢复区域占共享份的大小比例来推测其他信息，确保了方案的安全性。

(3)在恢复效果方面，文献[6]对各区域利用不同矩阵单独进行分享，带来了恢复图像色彩反转失真的问题(图 3(h,i)中背景颜色比 ABC 和 abc 的颜色深)，且不同恢复区域对比度不相等，与典型黑白二值视觉密码方案不兼容[10]；文献[10]克服了色彩反转失真问题，且不同恢复区域的对比度相等，但恢复图像整体偏暗；本方案不同解密区域的对比度均为 1(图 3(f,g))，实现了解密区域图像的完美恢复，显然本方案的恢复效果最优。

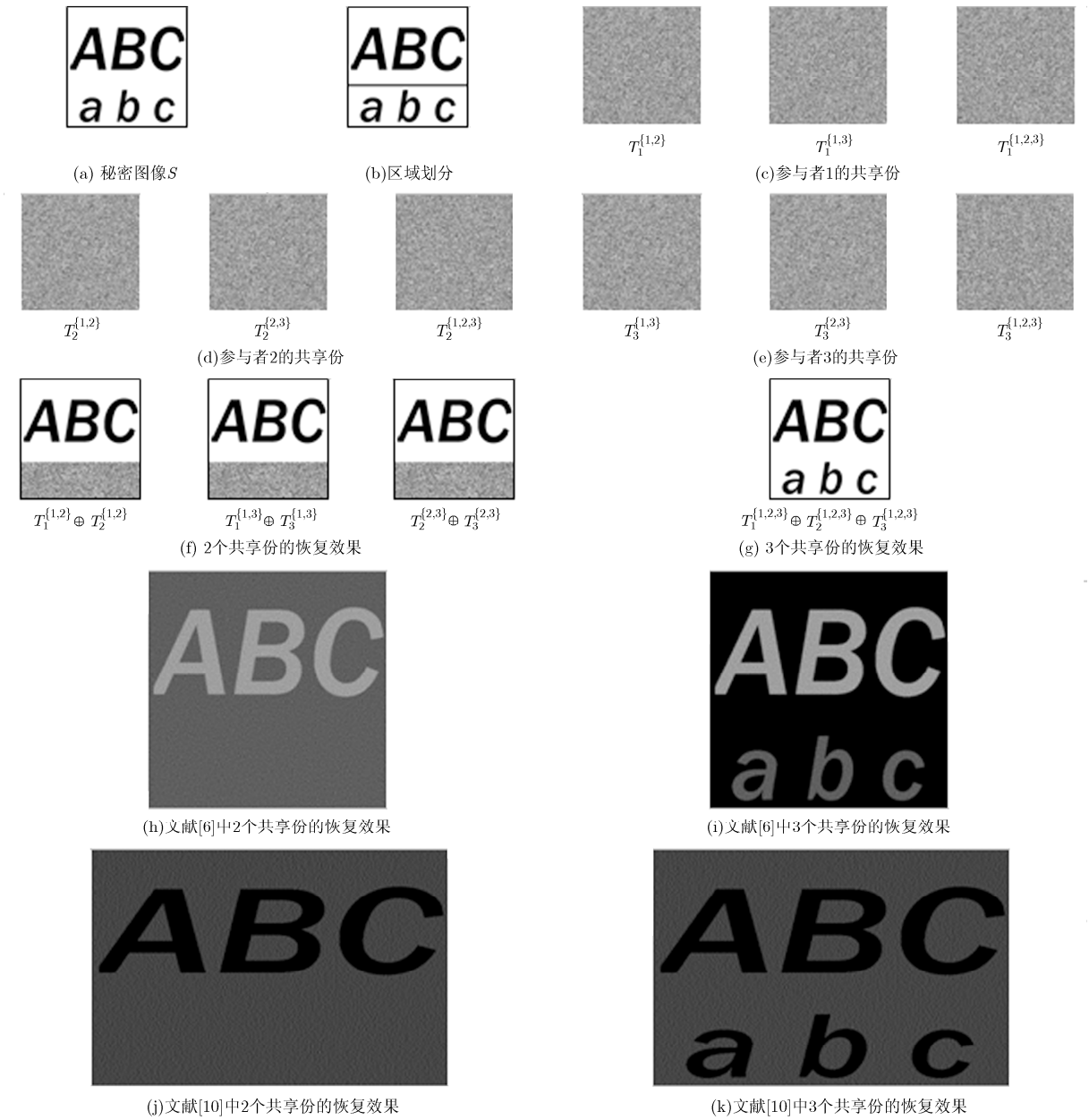

图 3　(2, 3)区域递增式视觉密码方案的实验结果

5.2 对比度分析

对比度可以用来衡量恢复图像的视觉效果，对比度越高，则恢复图像越清晰，反之，则越模糊。在考虑恢复图像不存在信息熵损失时，本文与文献[8]中基于 OR 运算的最优方案的对比度比较见表 2，从表中可以看出，对于不同 k,n 值，本方案中恢复区域的对比度均为 1，可以实现解密图像的完美恢复。文献[8]的对比度最大值为 1/2，且随着参与者人数的增多，恢复图像的对比度逐渐降低，直接影响了恢复图像的视觉效果。

5.3 像素扩展度分析

TSE 值可以用来衡量共享份的存储开销，在恢复图像不存在信息损失的前提下，本节给出本方案与文献[5–8]的 TSE 值比较结果。从表 3 可以看出，当 $k=2$，对于不同的 n 值，本方案的 TSE 值要明显小于文献[5–8]；当 $k>2$ 时，可以看出 k 值越大，本文方案的优化效果越明显，(3,5)方案中，本文的 TSE 值为 11，文献[8]为 20，保存共享份的存储开销是文献[8]的 55%, (4,5)方案中，本文的 TSE 值为 5，文献[8]为 20，存储开销是文献[8]的 25%，说明本方案的优化效率得到提高。

5.4 方案性能综合比较

本方案与其他区域递增式视觉密码方案综合比较见表 4。

(1)在设计方法方面，文献[6,8,10,17]基于加密矩阵设计，由于构造矩阵的约束条件复杂，随着参与

表 2 本文方案与文献[8]的对比度比较

(k,n)-RIVCS		区域	本文方案的对比度(文献[8]的对比度)			
			2 个共享份叠加	3 个共享份叠加	4 个共享份叠加	5 个共享份叠加
k=2	n=3	R_1	1(1/4)	1(1/2)	–	–
		R_2	–	1(1/4)	–	–
	n=4	R_1	1(1/5)	1(3/10)	1(2/5)	–
		R_2	–	1(1/10)	1(1/5)	–
		R_3	–	–	1(1/10)	–
	n=5	R_1	1(1/5)	1(3/10)	1(7/20)	1(7/20)
		R_2	–	1(1/20)	1(1/10)	1(3/20)
		R_3	–	–	1(1/20)	1(3/20)
		R_4	–	–	–	1(1/20)
k=3	n=4	R_1	–	1(1/10)	1(1/5)	–
		R_2	–	–	1(1/10)	–
	n=5	R_1	–	1(1/20)	1(1/10)	1(3/20)
		R_2	–	–	1(1/20)	1(3/20)
		R_3	–	–	–	1(1/20)
k=4	n=5	R_1	–	–	1(1/20)	1(3/20)
		R_2	–	–	–	1(1/20)

注：“–”表示该项不存在

表 3 本文方案与文献[5~8]的 TSE 值比较

(k,n)-RIVCS		文献[5]	文献[6]	文献[7]	文献[8]	本文方案
k=2	n=3	4	4	7	6	3
	n=4	10	10	18	14	7
	n=5	23	20	44	22	15
k=3	n=4	–	–	–	13	4
	n=5	–	–	–	20	11
k=4	n=5	–	–	–	20	5

注：“–”表示该项不存在

者人数的增加，矩阵规模迅速增大，导致像素扩展度急剧增加。文献[13,14]基于随机栅格实现了像素不扩展，但恢复图像的信息熵存在损失。本方案中不同区域的分享过程独立，基于授权集合，利用随机数设计，构造方法简单，不存在像素扩展，降低了共享份的存储开销，避免了构造和保存加密矩阵产生的额外开销。同时由于“异或”运算相当于 3 次“或”运算和 4 次“非”运算，因而相比或运算，异或运算并没有增加恢复操作的计算复杂度的阶数。

(2)在色彩失真方面，文献[8, 10, 14, 17]和本方案的恢复图像不存在色彩反转失真，因而可以正确显示原始图像颜色的真实信息。文献[10,14]和本方案中不同解密区域的对比度相等，与传统黑白视觉密码方案兼容。

(3)在完美恢复方面，文献[17]仅当所有共享份叠加时，能够实现白像素的完美恢复，而本方案进一步实现了所有解密区域图像的完美恢复。

(4)在传输开销方面，单个共享份的像素扩展度用来衡量方案的传输开销，文献[6,8,10,17]中单个共享份的像素扩展度随着参与者人数的增加而迅速增大，在秘密恢复过程中，共享份的传输开销大。文献[13,14]和本方案中单个共享份不存在像素扩展，在网络通信带宽受限的应用环境中，可以有效降低传输开销。

(5)在存储开销方面，共享份的像素扩展度之和用来衡量方案的存储开销，文献[6,8,10,17]的像素扩展度为单秘密方案的共享份像素扩展度之和(删除其中的冗余列)。文献[13,14]的存储开销最小，但损失了恢复图像的细节信息。本方案中单个参与者持多个共享份，共享份像素扩展度总和较小，在存储资源匮乏的应用环境中，能够有效降低共享份的存储开销，并确保恢复图像不存在信息损失。

6 结束语

本文对区域递增式视觉密码进行了研究，给出了一种解密区域完美恢复的实现方案，并对方案的

表 4 本文方案与其他区域递增式视觉密码方案的比较

	文献[6]	文献[8]	文献[10]	文献[13]	文献[14]	文献[17]	本文方案
设计方法	加密矩阵	加密矩阵	加密矩阵	随机栅格	随机栅格	加密矩阵	区域独立分享
恢复算法	OR 运算	OR 运算	OR 运算	OR 运算	OR 运算	XOR 运算	XOR 运算
色彩不失真	N	Y	Y	N	Y	Y	Y
兼容传统 VCS	N	N	Y	N	Y	N	Y
完美恢复	N	N	N	N	N	白像素	解密区域
m	>1	>1	>1	1	1	>1	1
TSE	$\le\sum_{i=2}^{n} m_{(i,n)}$	$\le\sum_{i=2}^{n} m_{(i,n)}$	$\le\sum_{i=2}^{n} m_{(i,n)}$	1	1	$\le\sum_{i=2}^{n} m_{(i,n)}$	$\sum_{i=k}^{n}\binom{n-1}{i-1}$

注：$m_{(i,n)}$为(i,n)-OVCS 的像素扩展度

有效性进行了理论证明和实验验证。通过为共享份添加身份标识，分享过程避开加密矩阵，直接利用随机数生成共享份，恢复过程依据身份标识出示对应共享份，构造了单个参与者持有多个共享份的单秘密视觉密码方案，在此基础上设计的区域递增式视觉密码方案，保持了各区域分享的独立性，解决了异或运算产生的像素反转问题，进一步降低了像素扩展度并提高了秘密图像的恢复效果，为区域递增式视觉密码的研究提供了一条新思路。

参 考 文 献

[1] 李鹏, 马培军, 苏小红, 等. 多重门限的图像秘密共享方法[J]. 电子学报, 2012, 40(3): 518–524. doi: 10.3969/j.issn.0372-2112.2012.03.018.
LI Ping, MA Peijun, SU Xiaohong, *et al*. Multi-threshold image secret sharing scheme[J]. *Acta Electronica Sinica*, 2012, 40(3): 518–524. doi: 10.3969/j.issn.0372-2112.2012.03.018.

[2] 付正欣, 沈刚, 郁滨, 等. 一种可完全恢复的门限多秘密视觉密码方案[J]. 软件学报, 2015, 26(7): 1757–1771. doi: 10.13328/j.cnki.jos.004611.
FU Zhengxin, SHEN Gang, YU Bin, *et al*. Threshold multi-secret visual cryptography scheme with perfect recovery[J]. *Journal of Software*, 2015, 26(7): 1757–1771. doi: 10.13328/j.cnki.jos.004611.

[3] BIN Y and GANG S. Multi-secret visual cryptography with deterministic contrast[J]. *Multimedia Tools and Applications*, 2014, 72(2): 1867–1886. doi: 10.1007/s11042-013-1479-8.

[4] SHYU S J and JIANG H W. General constructions for threshold multiple-secret visual cryptography schemes[J]. *IEEE Transactions on Information Forensics and Security*, 2013, 8(5): 733–743. doi: 10.1109/TIFS.2013.2250432.

[5] WANG R Z. Region incrementing visual cryptography[J]. *IEEE Signal Processing Letters*, 2009, 16(8): 659–662. doi: 10.1109/LSP.2009.2021334.

[6] SHYU S J and JIANG H W. Efficient construction for region incrementing visual cryptography[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2012, 22(5): 769–777. doi: 10.1109/TCSVT.2011.2180769.

[7] YANG C N, SHIH H W, CHU Y Y, *et al*. New region incrementing visual cryptography scheme[C]. Proceedings of the International Conference on Image Processing, Computer Vision, and Pattern Recognition in Conjunction with WORLDCOMP, Las Vegas, USA, 2011: 323–329.

[8] YANG C N, SHIH H W, WU C C, *et al*. k out of n region incrementing scheme in visual cryptography[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2012, 22(5): 799–810. doi: 10.1109/TCSVT.2011.2180952.

[9] YANG C N, LIN Y C, and WU C C. Region-in-region incrementing visual cryptography scheme[C]. Proceedings of 12th International Workshop on Digital-Forensics and Watermarking, Auckland, New Zealand, 2013: 449–463. doi: 10.1007/978-3-642-40099-5_37.

[10] 李吉亮, 李顺东, 王道顺. 区域递增视觉密码的构造[OL]. http://wenku.it168.com/huiyi/2349, 2014.
LI Jiliang, LI Shundong, and Wang Daoshun. Construction of region incrementing visual cryptography[OL]. http://wenku.it168.com/huiyi/2349, 2014.

[11] NAOR M and SHAMIR A. Visual cryptography[C]. Proceedings of the Advances in Cryptology-Eurocrypt'94, Berlin, 1995: 1–12. doi: 10.1007/BFb0053419.

[12] SHYU S. Image encryption by multiple random grids[J]. *Pattern Recognition*, 2009, 42(7): 1582–1596. doi:10.1016/j.patcog.2008.08.023.

[13] WANG R Z, LAN Y C, LEE Y K, *et al*. Incrementing visual cryptography using random grids[J]. *Optics Communications*, 2010, 283(21): 4242–4249. doi: 10.1016/j.optcom.2010.06.042.

[14] ZHONG G S and WANG J J. Region incrementing visual secret sharing scheme based on random grids [C]. Proceedings of IEEE International Symposium on Circuits and Systems, Los Alamitos, 2013: 2351–2354. doi: 10.1109/ISCAS.2013.6572350.

[15] 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. doi: 10.1007/s10623-004-3816-4.

[16] OU D, SUN W, and WU X T. Non-expansible XOR-based visual cryptography scheme with meaningful shares[J]. *Signal Processing*, 2015, 108: 604–621. doi: 10.1016/j.sigpro.2014.10.011.

[17] HAO H, GANG S, FU Z X, *et al*. General construction for XOR-based visual cryptography and its extended capability [J]. *Multimedia Tools and Applications*, 2016, 1–29. doi: 10.1007/s11042-016-3250-4.

[18] YANG C N and WANG D S. Property analysis of XOR based visual cryptography[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2014, 24(2): 189–197. doi: 10.1109/TCSVT.2013.2276708.

[19] ATENIESE G, BLUNDO C, SANTIS A D, *et al*. Visual cryptography for general access structures[J]. *Information and Computation*, 1996, 129(2): 86–106. doi: 10.1006/inco.1996.0076.

胡　浩：男，1989年生，博士生，研究方向为视觉密码和网络安全态势感知.

郁　滨：男，1964 年生，教授，博士生导师，主要研究方向为视觉密码和信息安全.

沈　刚：男，1986年生，博士生，研究方向为视觉密码.

张学思：女，1990 年生，助理工程师，主要研究方向为信息安全.