中图法分类号: TN918 **文献标志码**: A **文章编号**: 1006-8961(2011)03-0364-06

论文索引信息:宋涛, 王道顺, 李顺东, 罗向阳. 具有优化对照度的灰度图像的可视分存方案[J]. 中国图象图形学报,2011, 16(3):364-369

具有优化对照度的灰度图像的可视分存方案

宋涛[1)], 王道顺[1)], 李顺东[2)], 罗向阳[1),3)]

[1)](清华大学计算机系信息国家实验室, 北京 100084) [2)](陕西师范大学计算机科学学院,西安 710062)

[3)](解放军信息工程大学信息工程学院, 郑州 450002)

摘 要: 在可视分存方案(VCS)中,其解密过程通过人的视觉系统完成。对照度是 VCS 中重要的研究主题。现有复制设备提供了反色复制的基本功能,黑白图像的全黑反色方案(PBVCS)通过叠加一定数目的分存图像可以精确重构密图,从而为解决 VCS 重构图像质量问题提供了一种新的途径。给出了灰度图像的反色方案不能直接使用已有的全黑反色 PBVCS 来构造的原因和存在的问题,进而给出一般灰度图像的反色(k,n)-VCS,该方案的有效性被证明,使用我们的灰度反色 VCS,对分存图执行有限次反色和叠加操作可正确重构密图。

关键词: 可视分存; 对照度; 反色方案; 秘密共享

Visual cryptography scheme for gray-scale images with optimal contrast

Song Tao[1)], Wang Daoshun[1)], Li Shundong[2)], Luo Xiangyang[1),3)]

[1)](*Tsinghua National Laboratory for Information Science and Technology (TNlist), Department of Computer Science and Technology, Tsinghua University, Beijing* 100084 *China*) [2)](*School of Computer Science, Shaanxi Normal University, Xi'an* 710062 *China*)

[3)](*Information Science and Technology Institute, Zhengzhou* 450002 *China*)

Abstract: Visual cryptography scheme (VCS) is an encryption technique that utilizes human visual system in the recovering of the secret image and it does not require any complex calculation. Contrast has been a major issue of VCS schemes. Most copy machines have reversing function, in which can change a black image into a white one and vice versa. By means of the reversing operation, perfect black binary VCS with reversing can obtain ideal contrast. In this paper we conclude that we do not use existing VCS with reversing to construct an ideal contrast VCS for gray-scale images, then we show how to construct an ideal gray-scale VCS with reversing. In our scheme each participant is required to store a certain number of shares, and the number is same as that of binary VCS with reversing. Furthermore, the scheme guarantees that reconstructed image is correct since we perform certain runs operations.

Keywords: visual cryptography; contrast; scheme with reversing; secret sharing scheme

0 引 言

在一个黑白图像的(k,n)-VCS(可视分存方案)[1]中,原始密图被分存为 n 幅分存图,每幅分存图印刷在一张透明片上,直接叠加任意 k 张透明片都可以可视地重构原始密图。如果少于 k 张透明片,则无法恢复关于密图的任何信息。VCS 将原始

收稿日期:2009-10-26;**修回日期**:2010-01-06

基金项目:国家自然科学基金项目(60873249,60673065, 60902102);国家高技术研究发展计划(863)项目(2008AA01Z419, 2009AA011906)。

第一作者简介:宋涛(1979—),男。2010 年于清华大学计算机系获硕士学位,主要研究方向:信息安全。E-mail:hb. songtao@ gmail. com。

通讯作者:王道顺,E-mail:wangdaoshun@ gmail. com。

图像中的每个像素编码成 m 个像素,因此重构的图像是原始图像的 m 倍大小。像素膨胀 m 和对照度 α 是 VCS 中重要的两个参数。在一个黑白图像的 (k,n)-VCS 中的像素膨胀 m 和对照度 α 的关系是 $\alpha \propto \frac{1}{m}$ [1-3]。因此提高重构图像的质量(对照度 α)难度很大。在现在大多复制设备中,提供了反色复制功能,可以将黑色变成白色或者反过来将白色变成黑色,Viet 和 Kurosawa [4] 注意到这样一个现象并第一次直接使用一个全黑的黑白图像 VCS(PBVCS)去构造一个反色 PBVCS。随后,文献[5-8]研究了该方法并分别给出了方案去改进文献[4] 的对照度 α 和像素膨胀 m。兼容性、对照度、每个参与者拥有的分存图数、重构的复杂性、像素膨胀是衡量一个反色 VCS 重要指标,从这几个因素综合来看,文献[6,8]的方案是一个最佳选择。g 级灰度图像 (k,n)-VCS(GVCS)[9-10],像素膨胀 $m'=(g-1)m$,相邻两个灰度之间的对照度 $\alpha_{i+1,i}=1/((g-1)m)$ $(i=1,\cdots,(g-1))$,这个值非常小,在 m 和 g 的值比较大的时候,人的视觉系统无法区分相邻的灰度级。在这种情况下,我们使用反色技术去构造灰度图像的 GVCS 反色方案,进而提高对照度 $\alpha_{i+1,i}$。值得注意的是,若直接采用已有黑白图像反色 VCS 的构造方法去实现灰度图像的反色 GVCS,在 2.2 节经过相关的分析后,得到了其不能保持相邻灰度级之间的对照度的原因。

1　简介黑白 VCS 和灰度图像 GVCS

简要介绍文献[1-3]的可视分存方案(VCS)和灰度图像的可视分存方案(GVCS)[9-10]。

1.1　简介 (k,n)-VCS [1-3]

在一个黑白图像的 (k,n)-VCS,秘密图像包括一系列黑色和白色的像素,每个像素被分为 n 个分存图中的 m 个黑色和白色的子像素。子像素的集合可以使用一个 $n\times m$ 的布尔矩阵 $\boldsymbol{S}=[s_{ij}]$ 表示,其中元素 s_{ij} 表示第 i 个分存中的第 j 个子像素。白色子像素用 0 表示,黑色子像素用 1 表示。$s_{ij}=1$ 当且仅当第 i 个分存中的第 j 个子像素为黑色。叠加第 $i_1,\cdots,i_r$ 个分存得到的组合分存的灰度级与 $\boldsymbol{S}$ 中 $i_1,\cdots,i_r$ 行的布尔或的汉明重(即 1 的个数)$H(\boldsymbol{V})$ 成正比,$H(\boldsymbol{V})$ 表示 $\boldsymbol{V}$ 中 1 的个数。Verheul 和 Van Tilborg[2] 扩展了 Naor 和 Shamir 的方案[1] 中的定义,让 $z(\boldsymbol{V})$ 表示向量 $\boldsymbol{V}$ 中“0”坐标的数目,$H(\boldsymbol{V})+z(\boldsymbol{V})=m$,当 $H(\boldsymbol{V})\leqslant l$ 表示一个黑像素,$H(\boldsymbol{V})\geqslant h(h>l)$ 表示一个白像素,这里 l,h 分别表示白像素的数目。在文献[1-2]中,重构图像的质量通过对照度 α 来度量,即 $\alpha=(h-l)/m$。

1.2　简介灰度图像 GVCS

直接使用黑白 VCS [1-3] 中独立给出的通用方法实现灰度图像的 VCS,下面列出了其定义。

定义 1[9-10]　让 $\boldsymbol{\Gamma}_{\text{Grey}}=\{i_0,\cdots,i_{g-1}\}$ 是一个 $g\geqslant 2$ 级灰度的灰度调色板集合。一个 (k,n)- VCS 中包含 g 个 $n\times m$ 布尔矩阵集族 $\{\boldsymbol{C}_0,\cdots,\boldsymbol{C}_{g-1}\}$ 的,这里 $\boldsymbol{C}_q$ 是灰度为 i_q 的集合,$0\leqslant q\leqslant(g-1)$。若存在对照度为 $\alpha_1,\cdots,\alpha_{g-1}$,这里 α_q 表示第 q 灰度和 $q+1$ 灰度之间的对照度。满足

1)对任意的 $\boldsymbol{S}^q\in\boldsymbol{C}_q$ 和 $\boldsymbol{S}^{q+1}\in\boldsymbol{C}_{q+1}$,在 $\boldsymbol{S}^q$ 中,从 n 行中任意选择 k 行 m 维向量 $\boldsymbol{V}^q$ 的布尔或的汉明重 $H(\boldsymbol{V}^q)$ 和在 $\boldsymbol{S}^{q+1}$ 中,从 n 行中任意选择 k 行 m 维向量 $\boldsymbol{V}^{q+1}$ 布尔或的汉明重 $H(\boldsymbol{V}^{q+1})$ 满足 $H(\boldsymbol{V}^{q+1})-H(\boldsymbol{V}^q)\geqslant\alpha_{q+1,q}\cdot m$。

2)在 $\{1,\cdots,n\}$ 集中任意 t 个组成的子集 $\{i_1,\cdots,i_t\}$,这里 $t<k$,从 $n\times m$ 的矩阵集 $\boldsymbol{C}_q$ 中任选 t 行构成的子矩阵集是无法区分的。

第 1 个条件是确保相邻两个灰度级之间存在一个对照度 $\alpha_{q+1,q}$,第 2 个条件是确保方案的安全性,少于 k 个分存组合在一起得不到秘密图像的任何信息。

下面给出一个例子来说明灰度图像 GVCS 的构造方法。

例 1　一个 3 级灰度(2,3)-GVCS,在黑白(2,3)-VCS中,基本矩阵是

$$\boldsymbol{B}_0=\begin{bmatrix}110\\110\\110\end{bmatrix},\boldsymbol{B}_1=\begin{bmatrix}110\\011\\101\end{bmatrix}$$

构造一个 3 级灰度(2,3)- GVCS 基本矩阵为 $\boldsymbol{C}^{(0)}=\boldsymbol{B}_0\cdot\boldsymbol{B}_0,\boldsymbol{C}^{(1)}=\boldsymbol{B}_0\cdot\boldsymbol{B}_1,\boldsymbol{C}^{(2)}=\boldsymbol{B}_1\cdot\boldsymbol{B}_1$,即

$$\boldsymbol{C}^{(0)}=\left[\begin{array}{c|c}110&110\\110&110\\110&110\end{array}\right],\boldsymbol{C}^{(1)}=\left[\begin{array}{c|c}110&110\\110&011\\110&101\end{array}\right],$$

$$\boldsymbol{C}^{(3)}=\left[\begin{array}{c|c}110&110\\011&011\\101&101\end{array}\right]$$

像素膨胀为 $m'=6$,根据对照度定义

$$\alpha_0 = \frac{H(\boldsymbol{C}^{(1)}) - H(\boldsymbol{C}^{(0)})}{m'}, \alpha_1 = \frac{H(\boldsymbol{C}^{(2)}) - H(\boldsymbol{C}^{(1)})}{m'}$$

即 $\alpha_0 = \frac{5-4}{6} = \frac{1}{6}, \alpha_1 = \frac{6-5}{6} = \frac{1}{6}, \alpha_0 = \alpha_1$。

g 级灰度像素点的所有基本矩阵为 $\boldsymbol{C}^{(0)}$, $\boldsymbol{C}^{(1)}, \cdots, \boldsymbol{C}^{(g-1)}$,矩阵 $\boldsymbol{C}^{(q)}$ 由 $(g-1)$ 个矩阵通过矩阵并运算得到,$q=0,1,\cdots,(g-1)$,并且这 $(g-1)$ 个矩阵中有 $(g-1-q)$ 个 $\boldsymbol{B}_0$ 和 q 个 $\boldsymbol{B}_1$。

$$\boldsymbol{C}^{(q)} = \overbrace{\boldsymbol{B}_0 \cdot \cdots \cdot \boldsymbol{B}_0}^{g-1-q} \cdot \overbrace{\boldsymbol{B}_1 \cdot \cdots \cdot \boldsymbol{B}_1}^{q} \quad (1)$$

2 由全黑 VCS 方案构造灰度反色 GVCS

在介绍灰度反色 VCS 之前,有必要简要介绍一下黑白全黑反色 VCS。在黑白全黑反色 VCS(PBVCS)中,从兼容性、精确重构和重构复杂度这 3 个因素来综合权衡,Yang 等人[6,8] 的 PBVCS 最优。

2.1 简介 Yang 等人(k,n)-PBVCS

Yang 的方案[6,8] 中引入循环右移动操作来实现,并有如下定理。

定理 2 Yang 等人[6,8] 的 PBVCS 是一个反色(k,n)-PBVCS,像素膨胀 m,$H(P=0)=0$,$H(P=1)=m$,$\alpha = \frac{H(P=1)-H(P=0)}{m} = \frac{m}{m} = 1$。这里 $P=0,1$ 分别表示重构图像中的元素是白色和黑色像素。

2.2 由反色 PBVCS 直接扩展到灰度反色 GVCS 面临的问题

从 1.2 节可以看出,黑白 VCS 可以直接扩展到灰度图像的 VCS。下面通过一个例子来说明将 Yang 等人的 PBVCS 直接扩展成灰度反色 GVCS 后存在的问题,当然这个问题在其他反色 PBVCS 的扩展后一样存在,其分析方法是类似的。

例 2(继续例 1) 在一个 3 级灰度(2,3)-GVCS,其基本矩阵集为 $\boldsymbol{C}^{(0)}$,$\boldsymbol{C}^{(1)}$,$\boldsymbol{C}^{(2)}$,直接使用 Yang 等人 PBVCS 反色方案来处理(2,3)-GVCS。首先确定轮数,矩阵 $\boldsymbol{C}^{(0)}$ 轮数 $m'-2h+1=5$,矩阵 $\boldsymbol{C}^{(1)}$ 轮数 $m'-h+1=6$,矩阵 $\boldsymbol{C}^{(2)}$ 轮数 $m'+1=7$。最小轮数 $r=\min\{$轮数($\boldsymbol{C}^{(0)}$),轮数($\boldsymbol{C}^{(1)}$),轮数($\boldsymbol{C}^{(2)}$)$\}=\min\{5,6,7\}=5$。下面我们进行分发和重构处理。表 1 是管理者进行的密钥的分发处理,表 2—4 分别是参加者 1 和 2,1 和 3,2 和 3 进行的重构过程。

表 1 分发过程(管理者)

Tab.1 Distribution phase of dealer

灰度级	参与者	第 1 轮	第 2 轮	第 3 轮	第 4 轮	第 5 轮
1	1	(110110)	(011011)	(101101)	(110110)	(011011)
	2	(110110)	(011011)	(101101)	(110110)	(011011)
	3	(110110)	(011011)	(101101)	(110110)	(011011)
2	1	(110110)	(011011)	(101101)	(110110)	(110110)
	2	(110011)	(111001)	(111100)	(011110)	(001111)
	3	(110101)	(111010)	(011101)	(101110)	(010111)
3	1	(110110)	(011011)	(101101)	(110110)	(110110)
	2	(011011)	(101101)	(110110)	(011011)	(101101)
	3	(101101)	(110110)	(011011)	(101101)	(110110)

表 2 重构过程(参与者 1 和 2)

Tab.2 Reconstruction phase of participants 1 and 2

密图像素	第 1 轮	第 2 轮	第 3 轮	第 4 轮	第 5 轮	$\overline{U}$
1	(110110)	(011011)	(101101)	(110110)	(011011)	(000000)
2	(110111)	(111011)	(111101)	(111110)	(011111)	(010000)
3	(111111)	(111111)	(111111)	(111111)	(111111)	(111111)

表 3 重构过程(参与者 1 和 3)

Tab.3 Reconstruction phase of participants 1 and 3

密图像素	第 1 轮	第 2 轮	第 3 轮	第 4 轮	第 5 轮	$\overline{U}$
1	(110110)	(011011)	(101101)	(110110)	(011011)	(000000)
2	(110111)	(111011)	(111101)	(111110)	(0111111)	(010000)
3	(111111)	(111111)	(111111)	(111111)	(111111)	(111111)

表 4 重构过程(参与者 2 和 3)

Tab.4 Reconstruction phase of participants 2 and 3

密图像素	第 1 轮	第 2 轮	第 3 轮	第 4 轮	第 5 轮	$\overline{U}$
1	(110110)	(011011)	(101101)	(110110)	(011011)	(000000)
2	(110111)	(111011)	(111101)	(111110)	(0111111)	(010000)
3	(111111)	(111111)	(111111)	(111111)	(111111)	(111111)

计算对照度

$$\alpha_0' = \frac{H_2(\overline{U}) - H_1(\overline{U})}{m'}, \alpha_1' = \frac{H_3(\overline{U}) - H_2(\overline{U})}{m'}$$

得到 $\alpha_0' = \frac{1-0}{6} = \frac{1}{6}, \alpha_1' = \frac{6-1}{6} = \frac{5}{6}, \alpha_0' \neq \alpha_1'$

这样直接采用 Yang 等人方案去实现反色(2,3)-GVCS 得到对照度 $\alpha_0' \neq \alpha_1'$,与例 1(2,3)-GVCS 中 $\alpha_0 = \alpha_1$ 相比,这个方案不能保持相邻灰度之间的

差异,为此我们需要对上述方案做一些有益的调整,目标是执行 GVCS 反色方案后,能保持相邻灰度之间的差异。在 2.3 中将给出相应的证明。

2.3　灰度图像的反色可视分存方案(GVCS)

根据 2.2 节分析并借鉴 Yang[6,8] 的 PBVCS 方法,本节实现灰度图像的反色 GVCS。

符号定义如下:灰度分存图用 $\boldsymbol{s}=[s_{ijk}]$ 表示,s_{ijk} 表示在一个 $W\times H$ 原始灰度图像的像素 s_{ij} 通过 $m'=(g-1)\cdot m$ 个黑色和白色像素来替换,$s_{ij}=(s_{ij_1},s_{ij_2},\cdots,s_{ij_{(g-1)m}})$,这里 $i\in[1,W]$,$j\in[1,H]$,$k\in[1,m']$。

1) 循环右移限制

用 $\Gamma(\cdot)$ 表示从 $1\sim(g-1)m$ 个像素的循环右移操作,$\Gamma([s_{ijk}])=[\gamma'(s_{ijk})]$,其中操作 $\gamma'(\cdot)$ 是指一个位的限制块(子矩阵)内循环右移函数,并不是全局循环右移,即

$$\gamma'(s_{ij_1},s_{ij_2},\cdots,s_{ij_{(g-1)m}})=(\gamma(s_{ij_1},s_{ij_2},\cdots,s_{ij_m}),\cdots,\gamma(s_{ij_{(g-2)m+1}},s_{ij_{(g-2)m+2}},\cdots,s_{ij_{(g-1)m}}))=((s_{ij_m},s_{ij_1},\cdots,s_{ij_{m-1}}),\cdots,(s_{ij_{(g-1)m}},s_{ij_{(g-2)m+1}},\cdots,s_{ij_{(g-2)m+m-1}}))$$

这里 $\gamma(\cdot)$ 同文献[6,8]定义。

2) 基本矩阵的构造以及列变换进行限制

在一个 g 级灰度 (k,n)-GVCS 中,其基本矩阵集为 $\boldsymbol{C}^{(0)},\boldsymbol{C}^{(1)},\cdots,\boldsymbol{C}^{(g-1)}$(见式(1)),$\boldsymbol{C}^{(q)}=\overbrace{\boldsymbol{B}_0\cdot\cdots\cdot\boldsymbol{B}_0}^{g-1-q}\cdot\overbrace{\boldsymbol{B}_1\cdot\cdots\cdot\boldsymbol{B}_1}^{q},0\leqslant q\leqslant(g-1)$。我们给出一个新的符号 $\overleftrightarrow{\boldsymbol{C}}^{(q)}$ 表示矩阵 $\boldsymbol{C}^{(q)}$ 的列变换矩阵,定义如下

$$\overleftrightarrow{\boldsymbol{C}}^{(q)}=\overbrace{\overleftrightarrow{\boldsymbol{B}}_0\cdot\cdots\cdot\overleftrightarrow{\boldsymbol{B}}_0}^{g-1-q}\cdot\overbrace{\overleftrightarrow{\boldsymbol{B}}_1\cdot\cdots\cdot\overleftrightarrow{\boldsymbol{B}}_1}^{q}\tag{2}$$

从式(2)中看出,$\overleftrightarrow{\boldsymbol{C}}^{(q)}$ 是通过独立的对它的基本组成矩阵 $\boldsymbol{B}_0$ 或 $\boldsymbol{B}_1$ 进行矩阵列变换(符号 $\overleftrightarrow{\boldsymbol{B}}_0(\overleftrightarrow{\boldsymbol{B}}_1)$ 表示矩阵 $\boldsymbol{B}_0(\boldsymbol{B}_1)$ 的列变换)。下面给出方案的算法,分别为分发算法和重构处理。

分发过程(管理者):

1) 对灰度秘密图像执行一个灰度 (k,n)-GVCS,然后生成 n 个分存图 $s_1^1,\cdots,s_n^1$,完成第一轮操作,这里上标 1 表示第 1 轮操作,$r=1$。

2) 使用函数 $s_j^r=\Gamma(s_j^{r-1})$,执行第 i 轮操作,这里 $r\in[2,(m-h+1)]$ 得到相应的分存图。这里分存图被标有标识,便于参与者管理。

3) 分发 $(m-h+1)$ 个分存 $s_j^1,\cdots,s_j^{m-h+1}$ 给第 j 个参与者,这里 $j\in[1,n]$。

4) 每个参与者拥有带有标识的 $(m-h+1)$ 个分存图,其像素膨胀为 $(g-1)m$。

重构过程(参与者)

任意 k 参与者 $P_{j_1},\cdots,P_{j_k}$ 按照下列步骤去重构秘密图像 $\boldsymbol{P}$。

1) 对带有标识的 k 个分存图直接叠加(布尔 OR 运算),并执行 $(m-h+1)$ 轮,$T_r=s_{j_1}^r+s_{j_2}^r+\cdots+s_{j_k}^r$,$\{j_1,j_2,\cdots,j_k\}\subseteq\{1,\cdots,k\}$,$r=1,\cdots,(m-h+1)$。

2) 分别对 T_r 执行反操作(布尔反运算)得到相应的 $\overline{T}_r$,$r=1,\cdots,(m-h+1)$。

3) 对 $\overline{T}_1,\cdots,\overline{T}_{(m-h+1)}$ 直接叠加得到 $U=\overline{T}_1+\cdots+\overline{T}_{(m-h+1)}$。

4) 对 U 执行布尔反操作(布尔反运算)得到 $\boldsymbol{P}$,即 $P=\overline{U}=\overline{\overline{T}_1+\cdots+\overline{T}(m-h+1)}$。

5) $\boldsymbol{P}$ 即为重构的秘密图像,是原始图像的 $(g-1)m$ 倍大小。

定理 2　上述构造的算法是一个 g 级 (k,n)-GVCS 的反色方案,相邻灰度级之间的对照度均为 $1/(g-1)$。

证明:

在分发过程中,其处理方式跟 g 级灰度的 (k,n)-GVCS 相似的,每个参与者拥有多个分存图,而这些分存图是同一分存图经过不同轮数 r 循环右移的结果,它并没有拥有其他参与者的分存图的任何信息,这样任意 $k-1$ 个参与者得不到原始图像的任何信息,安全性得到保证。

根据式(1)可知

$$\boldsymbol{C}^{(q)}=\overbrace{\boldsymbol{B}_0\cdot\cdots\cdot\boldsymbol{B}_0}^{g-1-q}\cdot\overbrace{\boldsymbol{B}_1\cdot\cdots\cdot\boldsymbol{B}_1}^{q},0\leqslant q\leqslant(g-1)$$

根据式(2)

$$\overleftrightarrow{\boldsymbol{C}}^{(q)}=\overbrace{\overleftrightarrow{\boldsymbol{B}}_0\cdot\cdots\cdot\overleftrightarrow{\boldsymbol{B}}_0}^{g-1-q}\cdot\overbrace{\overleftrightarrow{\boldsymbol{B}}_1\cdot\cdots\cdot\overleftrightarrow{\boldsymbol{B}}_1}^{q}$$

在分发过程中,对 $\overleftrightarrow{\boldsymbol{C}}^{(q)}$ 操作即对其中的每个子矩阵 $\boldsymbol{B}_0,\boldsymbol{B}_1$ 独立的执行相应同步的循环右移操作。而 B_0 包含 $m-h$ 个黑像素和 h 个白像素,在 0 和 $m-h$ 之间,需要循环的轮数为 $r=m-h+1$。在重构过程中取反和叠加将产生全部黑像素(见重构过程中的 2)和 3)步骤),最后在取反(见 4)步骤)得到全白颜色,同理对包含 m 个黑像素 $\boldsymbol{B}_1$ 一样得到全黑的黑像素。从式(1)可知,q 级灰度矩阵 $\boldsymbol{C}^{(q)}$ 包

含$(q-1)$个全黑矩阵,因此重构图像 $\boldsymbol{P}$ 的 q 级灰度时,$H_q(\boldsymbol{P})=m\cdot(q-1)$。结合定理 1 的结论得

$$\alpha_{q+1,q}=\frac{H_{q+1}(\boldsymbol{P})-H_q(\boldsymbol{P})}{(g-1)m}=\frac{m\cdot(q+1-1)-m\cdot(q-1)}{(g-1)m}=\frac{1}{g-1}$$

2.4 实验结果及讨论

通过一个例子来说明 2.3 节的方案如图 1,2 所示。

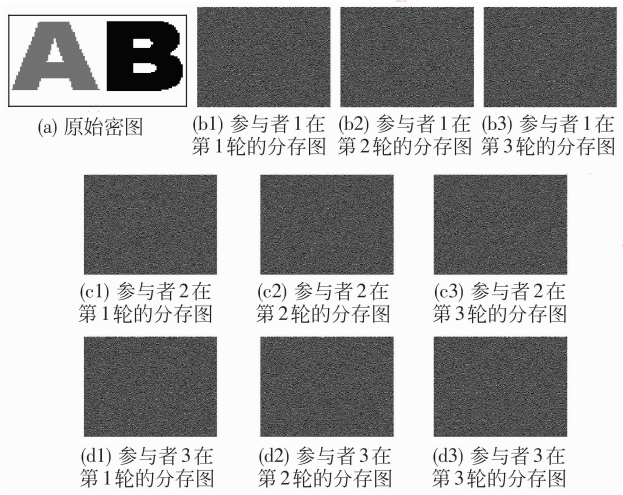

图 1 原始密图和参与者的分存图

Fig. 1 Original image and shares of participant

图 2 参与者的重构结果

Fig. 2 Reconstructed image of participant

例 3(继续例 1) 3 级灰度(2,3)-GVCS,基本矩阵 $\boldsymbol{C}^{(0)},\boldsymbol{C}^{(1)},\boldsymbol{C}^{(2)}$。

矩阵列变换:

$$\overleftrightarrow{\boldsymbol{C}^{(0)}}=\left[\begin{array}{c|c}\overleftrightarrow{110}&\overleftrightarrow{110}\\110&110\\110&110\end{array}\right],\overleftrightarrow{\boldsymbol{C}^{(1)}}=\left[\begin{array}{c|c}\overleftrightarrow{110}&\overleftrightarrow{110}\\110&011\\110&101\end{array}\right],$$

$$\overleftrightarrow{\boldsymbol{C}^{(2)}}=\left[\begin{array}{c|c}\overleftrightarrow{110}&\overleftrightarrow{110}\\011&011\\101&101\end{array}\right]$$

对照度:$\alpha_0=\frac{H_2(P)-H_1(P)}{m'},\alpha_1=\frac{H_3(P)-H_2(P)}{m'}$,

即 $\alpha_0=\frac{3-0}{6}=\frac{1}{2},\alpha_1=\frac{6-3}{6}=\frac{1}{2},\alpha_0=\alpha_1=\frac{1}{g-1}$

表 5 列出我们的灰度反色方案和直接利用文献[6,8]的方案实现灰度反色方案的比较表。

表 5 本文灰度反色方案与直接利用文献[6,8]实现反色 GVCS 的比较表

Tab. 5 Comparison of between GVCSR using directly schemes in [6, 8] and our GVCS

	文献[6,8]的方案	本文灰度反色方案
重构的兼容性	是	是
是否保持相邻灰度之间的对照度	否	是
轮数(r)	$(g-1)\cdot(m-h+1)$	$m-h+1$
像素膨胀 m'	$(g-1)\cdot m$	$(g-1)\cdot m$
参与者拥有的分存数目	$(g-1)\cdot(m-h+1)$	$(m-h+1)$
重构图像运算次数	$(g-1)\cdot((m-h+1)k-1)$ OR $s+(m-h+2)$ NOT s)	$((m-h+1)k-1)$ OR $s+(m-h+2)$ NOT s

从上表可以看出,本文给出的方案在重构的图像的质量、执行的轮数、参与者拥有的分存数和重构图像运算的次数均好于直接利用文献[6,8]的方案来实现反色的 GVCS。

3 结 论

基于黑白反色技术,论证了不能直接使用已有的全黑反色 PBVCS 来构造灰度图像的反色方案,重新定义了一个新的矩阵列置换方法,给出了一般灰度图像的反色(k,n)- VCS,当 k 个或更多的参与者,对拥有的分存图执行有限次反色和叠加操作就可正确重构密图。

参考文献(References)

[1] Naor M, Shamir A. Visual cryptography [C]//Advances in

Cryptology-EUROCRYPT'94, Lecture Notes in Computer Science. Berlin: Springer,1995,950: 1-12.

[2] Verheul E R, Van Tilborg H C A. Constructions and properties of k-out-of-n visual secret sharing schemes[J]. Designs, Codes and Cryptography, 1997, 11(2):179-196.

[3] Blundo C, De Bonis A, De Santis A. Improved schemes for visual cryptography [J]. Designs, Codes and Cryptograph, 2001, 24(3): 255 -278.

[4] Viet D Q, Kurosawa K. Almost ideal contrast visual cryptography with reversing[C]//Proceedings of the Topics in Cryptology-CT-RSA 2004. The Cryptographers' Track at the RSA Conference 2004. Berlin: Springer, 2004: 353-365.

[5] Cimato S, De Santis A, Ferrara A L, et al. Ideal contrast visual cryptography schemes with reversing[J]. Information Processing Letters, 2005, 93(4):199-206.

[6] Yang C N, Wang C C, Chen T S. Real perfect contrast visual secret schemes with reversing[C]//LNCS 3989, ACNS 2006, Singapore: ACNS, 2006:433-447.

[7] Chi Ming H, Wen Guey T. Compatible ideal contrast visual cryptography schemes with reversing[C]//Proceedings of the 8th Information Security Conference (ISC 05), LNCS 3650, Berlin: Springer, 2005:300-313.

[8] Yang C N, Wang C C, Chen T S. Visual cryptography schemes with reversing[J]. The Computer Journal, 2008,51(6):710-722.

[9] Muecke I. Greyscale and Colour Visual Cryptography [D]. Dalhouse: Uinversity-Daltech, 1999.

[10] Blundo C, De Santis A, Naor M. Visual cryptography for grey level images[J]. Information Processing Letters Archive, 2000, 75(6):255-259.