利用反转实现理想对比度的密图分存

张海波,王小非,徐海樵,黄友澎
(武汉数字工程研究所,湖北武汉 430074)

摘 要: 可视秘密共享的一个主要不足是重构后图像的对比度损失严重.提出了利用反转实现理想对比度的密图分存方案.编码轮数为 m/h(上取整)(m 和 h 分别是白像素加密所用基阵全部列和全白列的数量),采取像素块编码方式,每步都将 m 个连续相同的像素进行一次性加密编码,不产生像素扩展.对方案的正确性和安全性进行了证明,并与类似方案进行了对比分析和实验.该方案编码效率较高,系统容量较小.

关键词: 可视秘密共享; 反转; 理想对比度; 黑像素完善的可视秘密共享
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2010) 02-0465-04

Ideal Contrast Secret Image Sharing Using Reversing

ZHANG Hai-bo, WANG Xiao-fei, XU Hai-qiao, HUANG You-peng
(*Wuhan Digital Engineering Institute*, *Wuhan*, *Hubei* 430074, *China*)

Abstract: In visual secret sharing (VSS) schemes, the contrast of reconstructed image is much lost. A novel VSS scheme with reversing is presented. It can achieve really ideal contrast within (the ceiling integer of) m/h encoding runs, where m and h are respectively the number of all columns and the number of whole-white columns in the basis matrix for white pixels encoding. It encodes a secret image block by block and no pixel expansion occurs. A block consists of consecutive m pixels with same type, which means that m pixels together join into each encoding step. The proof of its correctness and security, the experimental results, analyses and comparisons are also shown. High encoding efficiency and low system capacity are its main advantages.

Key words: visual secret sharing (VSS); reversing; ideal contrast; perfect black visual secret sharing (PBVSS)

1 引言

1994 年,Naor 与 Shamir[1]共同提出了第 1 个可视秘密共享(visual secret sharing, VSS)方案.该方案将一幅秘密黑白图像分存到 n 个份额(透明的黑白图像)中,其中任意等于或多于 k($k \leqslant n$)个份额叠加在一起可恢复出人眼可辨识的原始图案,少于 k 个份额(叠加)不可能透露关于原始秘密的任何信息.

VSS 方案一般用两个基阵 $\boldsymbol{M}_0$ 和 $\boldsymbol{M}_1$($n \times m$ 维布尔矩阵)分别将秘密白像素和黑像素加密成或白或黑、具有一定灰度的像素块(块长为 m).若秘密黑像素能够完全重构为全黑的像素块,则称为黑像素完善的 VSS (perfect black VSS, PBVSS)方案;否则称为黑像素不完善的 VSS(non-perfect black VSS, NPBVSS)方案.

虽然目前涌现出了许多扩展型或新型 VSS 方案,但仍存在一个不容回避的问题:重构(重叠)后图像的对比度损失严重[2~5].近来,一个有效解决该问题的方法——借助反转操作并适当增加编码轮数——已初露端倪,并正在形成一个研究热点[6~8].

2 相关工作

2004 年,Viet 与 Kurosawa[6]设计了第 1 个该方面的方案,但仅能获得近似理想的对比度.为了达到理想对比度,该方案需要进行无限轮编码.但编码轮数越多,产生的份额就越多,系统存贮和传输等开销也越大,因而此类方案的设计重在降低编码轮数.后来,Cimato 等[7]提出的方案将编码轮数降为 m(基阵 $\boldsymbol{M}_0$ 或 $\boldsymbol{M}_1$ 的列向量数).Yang 等[8]又引入移位操作作为补充,进一步将编码轮数降为($m - h + 1$),其中 $m > h > 0$,h 为基阵 $\boldsymbol{M}_0$ 中全白列的个数.而且,文献[7,8]给出的方案均实现了理想对比度.

在密图分发阶段,上述方案均是基于传统 PBVSS 方案,只是每轮编码方式不同.Viet-Kurosawa 方案[6]将基础方案根据需要独立地执行一定的轮数;Cimato 等方案[7]将基阵的每 1 列用于其中 1 轮的编码;Yang 等方

收稿日期:2008-12-02;修回日期:2009-05-20
基金项目:国防"十一五"重点预研项目(No.51306020201)

案[8]将传统 VSS 方案作为首轮编码,然后将最新 1 轮产生的份额中对应于每个秘密像素的由 m 个子像素组成的块执行块内循环右移 1 位操作,从而形成新 1 轮的份额.

在密图重构阶段,上述方案的处理都是一样的.对于每轮编码,k 或更多个份额叠加,可重构出一幅对比度较差的图像 T_i.然后执行"反转-叠加-反转"过程,即将各个 T_i 反转,再将反转后的 T_i 叠加,并再次反转,完成密图重构.设编码轮数为 r,则最终还原图像可记为 $\overline{\overline{T}_1+\overline{T}_2+\cdots+\overline{T}_r}$,其对比度显著改善[6~8].此时,可将原始秘密白和黑像素最终重构后的趋白程度分别记为 P_0 和 P_1.易知,若方案具有理想对比度,则有 $P_0=1$ 和 $P_1=0$.

归纳起来,上述方案存在以下不足:

(1)Viet-Kurosawa 方案[6]和 Yang 等方案[8]存在像素扩展,各份额大小是原始密图的 m 倍,导致还原后密图变形,且需要更多的存贮和传输开销.

(2)一次仅加密 1 个像素,效率较低.由于此类方案需多轮编码,效率问题值得关注.

(3)编码轮数有待进一步降低,以利于实际应用.

基于此,本文提出一个新的基于 PBVSS 和反转操作的密图分存方案,仅$\lceil m/h\rceil$轮编码就可实现理想对比度,且不产生像素扩展,一次能同时编码 m 个像素.

3 本文方案

3.1 秘图分发

加密编码的对象是由 m 个连续的具有相同类型的像素组成的像素块.设当前待编码块在密图中的位置为 $l_1,l_2,\cdots,l_m$,则其间可能存在间隔,易知这些间隔位置上的像素具有相反类型,它们将参加下一个块的编码.

先解决白像素块(即 $l_1,l_2,\cdots,l_m$ 全为白像素)的加密编码.这里引入集合 $\boldsymbol{A}$ 表示基阵 $\boldsymbol{M}_0$ 中所有列的序号,即 $\boldsymbol{A}=\{1,2,\cdots,m\}$.

首轮编码时,先将基阵 $\boldsymbol{M}_0$ 随机列重排,并记重排后基阵为 $\boldsymbol{M}_0^1$.然后将 $\boldsymbol{M}_0^1$ 中第 i 行的 m 个子像素填入第 i 个份额中的 $l_1,l_2,\cdots,l_m$ 位置.第 1 轮编码完成.此时,令集合 $\boldsymbol{B}$ 表示 $\boldsymbol{M}_0^1$ 中 h 个全"0"列的序号,即 $\boldsymbol{B}=\{i_1,i_2,\cdots,i_h\}$,其中 $1\leqslant i_1,i_2,\cdots,i_h\leqslant m$.则集合 $\boldsymbol{H}=\boldsymbol{A}-\boldsymbol{B}$中的元素是 $\boldsymbol{M}_0^1$ 中那些含有至少 1 个"1"的列的序号.此时有:$|\boldsymbol{A}|=m$,$|\boldsymbol{B}|=h$ 和 $|\boldsymbol{H}|=m-h$.重复以下步骤,直至 $\boldsymbol{H}=\varnothing$.

从集合 $\boldsymbol{H}$ 中任取 h 个元素 $j_1,j_2,\cdots,j_h$,在 $\boldsymbol{M}_0^1$ 中,将 $j_1,j_2,\cdots,j_h$ 列分别与集合 $\boldsymbol{B}=\{i_1,i_2,\cdots,i_h\}$ 标示的各列进行一对一互换.如,将第 i_1 列与第 j_1 列互换,第 i_2 列与第 j_2 列互换,…,第 i_h 列与第 j_h 列互换.记互换后形成的新基阵为 $\boldsymbol{M}_0^u$,其中 $2\leqslant u\leqslant\lceil m/h\rceil$.再将 $\boldsymbol{M}_0^u$ 中第 i 行的 m 个子像素填入第 i 个份额中的 $l_1,l_2,\cdots,l_m$ 位置.然后,从集合 $\boldsymbol{H}$ 中删除元素 $j_1,j_2,\cdots,j_h$.第 u 轮编码完成.

值得注意的是,最后 1 轮编码时有可能出现集合 $\boldsymbol{H}$ 中元素个数 $x<h$ 的情形,此时只需将集合 $\boldsymbol{B}=\{i_1,i_2,\cdots,i_h\}$ 标示的前 x 个列与 $j_1,j_2,\cdots,j_x$ 列互换.

若 $l_1,l_2,\cdots,l_m$ 为黑像素块,则在每轮编码中,均将基阵 $\boldsymbol{M}_1$ 随机列重排,并将重排后基阵的第 i 行的 m 个子像素填入第 i 个份额中的 $l_1,l_2,\cdots,l_m$ 位置.共进行$\lceil m/h\rceil$轮编码.

重复上述像素块编码过程直至整张密图分发完成.最后,每个参与者只拥有$\lceil m/h\rceil$个份额.另外,有可能出现密图最后所剩像素个数 $y<m$ 的情形.解决办法是,先仍将它们当作一个完整的块进行处理,填入时只取当前生成好的基阵中的前 y 列.

3.2 秘图重构

重构过程与其它具备反转功能的方案一样,经过"反转-叠加-反转"过程后,最终重构图像为 $\overline{\overline{T}_1+\overline{T}_2+\cdots+\overline{T_{\lceil m/h\rceil}}}$,并具备理想对比度,即 $P_0=1$ 和 $P_1=0$.

3.3 方案的正确性与安全性

定理 1 本文方案能够在$\lceil m/h\rceil$轮编码内达到理想对比度,即 $P_0=1$ 和 $P_1=0$.

证明 首先,本文方案是基于 PBVSS 方案,故对于任一个秘密黑像素,它在每轮叠加还原图像 T_i 中必定是黑像素.所有 T_i 经过"反转-叠加-反转"过程后,该像素在最终重构图像中也必定是黑像素.故有 $P_1=0$.

其次,黑像素的编码轮数是$\lceil m/h\rceil$.白像素编码时,每轮都从集合 $\boldsymbol{H}$ 中取出 h 个元素,直到最后 1 轮 $\boldsymbol{H}$ 中所剩元素个数不超过 h.由于开始编码时有 $\boldsymbol{H}=\boldsymbol{A}$,$|\boldsymbol{A}|=m$,编码完成时又有 $\boldsymbol{H}=\varnothing$,故所需编码轮数等于$\lceil m/h\rceil$.

再看白像素的加密编码.可将 m 个连续的白像素看作一个整体的"像素".从方案的编码过程易知,对于该"像素"中的每 1 个子像素,在至少 1 个还原图像 T_i 中的同样位置有 1 个白色子像素与之对应.另一方面,由 De Morgan 定律,有 $\overline{\overline{T}_1+\overline{T}_2+\cdots+\overline{T_{\lceil m/h\rceil}}}=T_1\times T_2\times\cdots\times T_{\lceil m/h\rceil}$,表明经过"反转-叠加-反转"过程后,每 1 个子像素在最终重构图像中也必定是白色.故有 $P_0=1$.

综上所述,本文方案能够在$\lceil m/h\rceil$轮编码内达到 $P_0=1$ 和 $P_1=0$,即获得理想对比度.

(证毕)

定理 2 本文方案的安全性与传统 Naor-Shamir 方案等价.

证明　VSS 方案的安全性与所选基阵的构造及加密编码方式有关[1].易知本文方案的安全性主要取决于加密编码方式.在传统 Naor-Shamir 方案[1]中,当编码白(或黑)像素时,先将对应的基阵 $\boldsymbol{M}_0$(或 $\boldsymbol{M}_1$)随机列重排.在本文方案中,对于黑像素,每轮编码前也同样是将基阵 $\boldsymbol{M}_1$ 随机列重排.因而,黑像素编码的安全性与传统 Naor-Shamir 方案等价.

再看白像素的加密编码.在第 1 轮编码前也是将基阵 $\boldsymbol{M}_0$ 随机列重排(记重排后的基阵为 $\boldsymbol{M}_0^1$),这意味着白像素的第 1 轮编码同样足够安全,且与传统 Naor-Shamir 方案等价.进一步地,从方案的密图分发过程易知,后续各轮编码所用基阵 $\boldsymbol{M}_0^u(2\leqslant u\leqslant\lceil m/h\rceil)$均是将 $\boldsymbol{M}_0^1$ 中的若干列进行交换得到的,而列交换也是一种列重排操作,可见 $\boldsymbol{M}_0^u$ 的安全性与 $\boldsymbol{M}_0^1$ 等价,也即后续各轮编码的安全性与第 1 轮等价,故白像素各轮编码的安全性也与传统 Naor-Shamir 方案等价.

(证毕)

4　实验与分析

取如式(1)所示的用于(4,4)-PBVSS 的基阵,易知 $m=6, h=3$.取如图 1 所示密图.

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

图 2 是本文方案与其它方案的对比实验结果.易知,本文方案与 Cimato 等[7]方案没有像素扩展,其它方案的扩展倍数均为 6,还原后图像发生了变形;除了 Viet-Kurosawa[6] 方案,其它各方案均能在 6 轮编码内达到理想对比度,而本文方案达到同样目的仅需 2 轮编码.

图1　原始密图(125×125)

本文方案除了适用于(n, n)和(k, n)门限访问结构,也可适用于通用访问结构[9],这取决于具体实现过程中基于 PBVSS 的基阵的选取[10].另一方面,只要正确地选用合适的色彩模型并引入半调化技术[10,11],本文方案也可应用于灰度和彩色图像并改善这类图像重构后的对比度.

进一步地,以(k, n)门限访问结构为例,表 1 列出了对上述各方案的分析结果.

在基于反转操作的 VSS 方案中,由于单轮加密编码的复杂性主要体现在基阵列重排和填入操作,各方案区别不明显,故表 1 重点讨论了重构阶段(包括叠加和反转操作)的复杂性,易知重构复杂度与编码轮数成正比.同时可知,编码轮数也与份额总数、系统容量、传输带宽成正比.进一步表明降低编码轮数在此类方案中的重要作用.以(k, n)门限访问结构为例,若编码轮数减少 d,则带来的直接好处是:份额总数减少 $d*n$;叠加操作至少减少 $d*k$,最多减少 $d*n$;反转操作减少 d;系统存贮容量及传输带宽至少减少 $d*k$ 或 $d*m*k$(存在像素扩展),最多减少 $d*n$ 或 $d*m*n$(存在像素扩展).

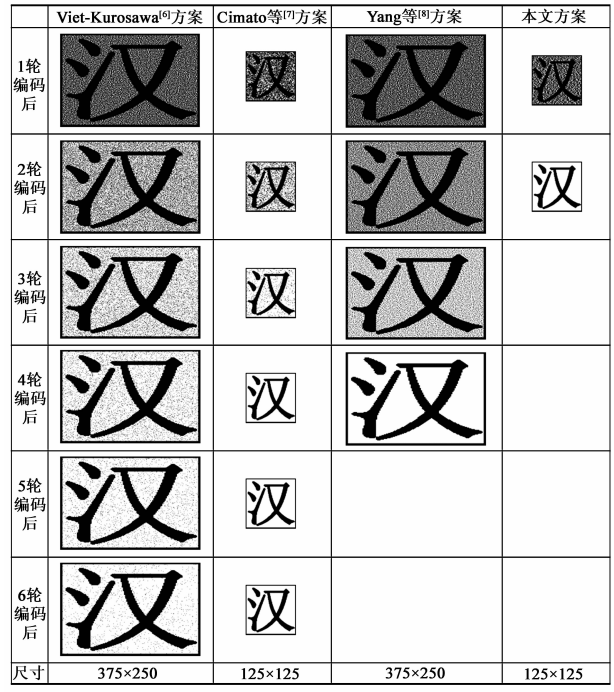

图2　基于PBVSS和反转操作的不同方案实验结果

此外,像素扩展既影响系统存贮容量和传输带宽,也直接影响各份额及重构图像的视觉效果,表明像素不扩展编码也是此类方案需努力的一个方向.

综上所述,在同样达到理想对比度的情况下,本文方案具有最少的编码轮数、份额总数、系统容量、传输带宽、重构复杂度,具有较高的编码效率,因而本文方案的优势和现实意义明显.

5　结束语

目前的研究工作一般都是用黑像素表示有用的秘密信息.研究具有理想对比度的 VSS 方案后,可突破这一限制,有用信息可用白像素或黑白混合色来表示.故该项研究现实意义明显.本文基于 PBVSS 和反转操作提出的新方案仅在$\lceil m/h\rceil$轮编码内即可达到理想对比度,没有像素扩展,采取像素块编码方式提高了编码效率,可适用于任意访问结构,也可应用于灰度和彩色图像.进一步的研究方向是如何将本文方法应用于 NPB-VSS 方案,使其获得理想对比度.

表 1 基于(k,n)-PBVSS 和反转操作的不同方案对比分析

		Viet-Kurosawa[6]方案	Cimato 等[7]方案	Yang 等[8]方案	本文方案
编码轮数		r	m	$m-h+1$	$\lceil m/h \rceil$
对比度		近似理想($r\to\infty$时理想)	理想	理想	理想
像素扩展倍数		m	1	m	1
重构复杂度	叠加操作($w\in[k,n]$)	$r*w-1$	$m*w-1$	$(m-h+1)*w-1$	$\lceil m/h \rceil *w-1$
	反转操作	$r+1$	$m+1$	$m-h+2$	$\lceil m/h \rceil +1$
份额总数		$r*n$	$m*n$	$(m-h+1)*n$	$\lceil m/h \rceil *n$
系统存贮容量(相对于原始密图的倍数)		$r*m*n$	$m*n$	$(m-h+1)*m*n$	$\lceil m/h \rceil *n$
系统传输带宽(相对于原始密图的倍数)		$r*m*n$	$m*n$	$(m-h+1)*m*n$	$\lceil m/h \rceil *n$
编码方式		单像素编码	单像素编码	单像素编码	像素块编码
编码效率		低	低	低	高

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] Ateniese G, Blundo C, De Santis A, Stinson D R. Extended capabilities for visual cryptography[J]. Theoretical Computer Science, 2001, 250(1 – 2): 143 – 161.

[3] Blundo C, De Santis A, Stinson D R. On the contrast in visual cryptography schemes[J]. Journal of Cryptology, 1999, 12(4): 261 – 289.

[4] Kuhlmann C, Simon H U. Construction of visual secret sharing schemes with almost optimal contrast[A]. Proceedings of the 11th Annual ACM-SIAM Symposium on Discrete Algorithms[C]. Philadelphia: Society for Industrial and Applied Mathematics, 2000. 263 – 272.

[5] Eisen P A, Stinson D R. Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels[J]. Designs, Codes and Cryptography, 2002, 25(1): 15 – 61.

[6] Viet D Q, Kurosawa K. Almost ideal contrast visual cryptography with reversing[A]. Proceeding of Topics in Cryptology-CT-RSA2004 (LNCS 2964)[C]. Berlin: Springer-Verlag, 2004. 353 – 365.

[7] Cimato S, De Santis A, Ferrara A L, Masucci B. Ideal contrast visual cryptography schemes with reversing[J]. Information Processing Letters, 2005, 93(4): 199 – 206.

[8] Yang C N, Wang C C, Chen T S. Real perfect contrast visual secret sharing schemes with reversing[A]. Lecture Note in Computer Science 3989[C]. Berlin: Springer-Verlag, 2006. 433 – 447.

[9] Yi F, Wang D S, Luo P, Huang L S, Dai Y Q. Multi secret image color visual cryptography schemes for general access structures[J]. Progress in Natural Science, 2006, 16(4): 431 – 436.

[10] 张海波,王小非,黄友澎,罗威.基于自适应多像素编码的可视密图分存[J].西南交通大学学报,2009,44(3):448 – 454.
Zhang H B, Wang X F, Huang Y P, Luo W. Secret image sharing based on self-adaptive multi-pixel encoding[J]. Journal of Southwest Jiaotong University, 2009, 44(3): 448 – 454. (in Chinese)

[11] Mese M, Vaidyanathan P P. Recent advances in digital halftoning and inverse halftoning methods[J]. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2002, 49(6): 790 – 805.

作者简介:

张海波 男,1972 年出生,博士,高工,FCC 高级会员.研究方向为信息安全、秘密共享与信息论.
E-mail: zhanghb412@yahoo.com.cn

王小非 男,1957 年出生,博士,研究员,博士生导师,研究方向为信息安全、网络和并行计算.