Journal of Computer Applications
计算机应用,2012,32(3):669-678
ISSN 1001-9081
CODEN JYIIDU
2012-03-01
http://www.joca.cn

文章编号:1001-9081(2012)03-0669-10
doi:10.3724/SP.J.1087.2012.00669

视图的秘密分享及其代数编码方法

王晓京,方佳嘉*,蔡红亮,王一丁
(中国科学院 成都计算机应用研究所,成都 610041)
(*通信作者电子邮箱 fjcigar@163.com)

摘　要:视图的秘密分享是图像信息安全领域独具吸引力的研究问题。寻求秘密视图完全的(Perfect)和理想的(Ideal)门限秘密分享方案(也称图像门限分享的完备方案),则是其中富有挑战性的未决课题。文中引入灰度值域 $GF(2^m)$ 上像素矩阵秘密分享的新观点和相应的代数几何编码方法,实现了数字图像 (t,n) 门限秘密分享的一种完备方案。该方案能够将一幅或多幅秘密图像编码为 n 幅各具随机视觉内容,同时又共具 (t,n) 门限结构的影子图像(或称份额图像)。证明了这种秘密分享方案的 (t,n) 门限结构不仅是完全的而且也是理想的,并给出了提高像素灰度值域 $GF(2^m)$ 上图像秘密分享算法效率的"m 位像素值的分拆与并行"方法。分析表明,该图像秘密分享方法可以应用于高安全等级的秘密图像的网络多路径传输、保密图像信息的分散式存储控制、高维图形码(Bar-code in k dimension)和弹出码(Popcode)等新一代信息载体技术的识读控制等各方面。

关键词:图像分享;(t,n) 门限;像素灰度值域 $GF(2^m)$;代数几何编码;m 位像素值的分拆与并行
中图分类号:TP309.7　　**文献标志码**:A

Secret image sharing and its algebraic coding method

WANG Xiao-jing, FANG Jia-jia*, CAI Hong-liang, WANG Yi-ding
(*Chengdu Institute of Computer Applications, Chinese Academy of Sciences, Chengdu Sichuan 610041, China*)

Abstract: Image sharing is an attractive research subject in computer image information security field. Seeking for Perfect and Ideal image threshold secret sharing scheme (i.e. the complete image sharing scheme) is one of the unresolved challenging problems. By introducing into the methods of pixel matrix secret sharing over pixel value field $GF(2^m)$ and algebraic-geometry coding, a complete scheme of image sharing with a (t, n) threshold structure was achieved in this paper. The scheme could encode secret images into n shadow images in such a way that all the shadow images were in a Perfect and Ideal (t, n) threshold structure, while each shadow image had its own visual content assigned at random. This approach to image sharing was able to be applied to the new information carrier technology, e.g. network multipathed transmission of secret image in high security level, distributed storage control of secret image, bar-code in k dimension and Popcode. This paper also presented a method to cut down a great deal of computational time for image sharing based on a pixel field $GF(2^m)$, called "partition and paralleling of m-bit pixel".

Key words: image sharing; (t, n) threshold; pixel value field $GF(2^m)$; algebraic-geometry coding; partition and paralleling of m-bit pixel

0　引言

给定正整数 $t \leqslant n$,如何将一幅秘密图像映射成 n 幅影子图像(即 n 个具有视觉意义的份额图像),使得从其中任何 t 个以上份额都可恢复秘密图像,而少于 t 个份额则无法恢复原秘密图像,属于视图的 (t,n) 门限秘密分享研究范围。视图秘密分享的目的是通过影子图像及其准入结构来保护秘密图像信息,影子图像的外在伪装视觉内容可以避免敌手的猜疑和攻击,而影子图像的准入结构是为了保证图像分享在密码学意义上的安全性,(t,n) 门限结构则是一种备受青睐的准入结构。

图像分享的理念源于秘密分享理论。1979 年,Shamir 和 Blakley[1-2] 针对密钥等纯数据的安全保管问题,分别独立地提出了自己的 (t,n) 门限结构的数据分享方法。在秘密分享理论的发展中,一种秘密分享方案是否是完备的(Complete),即秘密分享的 (t,n) 门限结构是否同为完全的(Perfect)和理想的(Ideal),在信息安全上具有至关重要的基本重要性[3-4](完全的和理想的等概念详见本文第 1 章和第 2 章中的进一步说明)。Blakley 的方案建立在空间平面交线(点)的简明几何观点上,但它不属于完备的方案。Shamir 的 (t,n) 门限方案则基于素域 $F_p = \{0, 1, 2, \cdots, p-1\}$ 上的插值多项式原理[1],其门限结构被证明既是完全的也是理想的[3-4],从而是一个完备的数据分享方案。由于数字图像是由像素值构成的,故图像分享可以视为秘密分享的一个专门领域。因此,和一般秘密分享一样,图像秘密分享方案是否是完备的(或准入结构是否既是完全的又是理想的)是安全性的主要考虑因素。然而,如果将秘密分享方法直接应用于图像分享上,得到的影子图像将是没有视觉意义的累赘数据集合(本文也称其

收稿日期:2011-09-13;**修回日期**:2011-11-29。
基金项目:国家 863 计划项目(2008AA01Z402);中国科学院知识创新工程项目(2004CB18003)。
作者简介:王晓京(1953-),男,安徽滁州人,研究员,博士,主要研究方向:编码与信息安全;　方佳嘉(1985-),男,福建漳州人,博士研究生,主要研究方向:编码与信息安全;　蔡红亮(1983-),男,山西临汾人,博士研究生,主要研究方向:编码与信息安全;　王一丁(1983-),男,四川成都人,博士,主要研究方向:编码与信息安全。

为无视觉意义的份额),这很容易招致怀疑并被重点攻击、不利于保管。此外,在当代数字信息的许多应用场合中,保证恢复的秘密图像像素值的完整性和精确性也是十分必要的,因此适合准确描述图像分享的像素值域也需要建立起来。鉴于这些原因,发展针对图像分享这个专门领域的秘密分享方法是必要的,具有特殊重要的意义。

长期以来,人们尝试了各种方法去构造图像分享方案,力图让其影子图像各具独立的外在视觉意义、而其准入结构又是完全的和理想的。然而找到这样的完备方案并非易事[5-32]。早前图像分享的工作中,各种主要方案都是通过视觉秘密分享(Visual Secret Sharing, VSS)方法[7]来实现的。这种方法获得的影子图像的视觉效果一般都较差,恢复的秘密图像在像素数据上损失较大[7-24],与原秘密图像有明显差别。而且由于视觉密码方法固有的像素扩张问题[7-24],造成凡具有可视影子图像的 VSS 方案其准入结构都不是理想的。在随后发展的数字图像秘密分享理论中[6]26-28,33,人们把图像的门限秘密分享看成像素数据的秘密分享,依然沿用了早期数据秘密分享[1]所习惯的素域 $F_p = \{0,1,2,\cdots,p-1\}$ 上的插值多项式的方法来构造 (t,n) 门限结构。此类方法先将秘密图像映射为若干没有视觉意义的份额数据,再将份额数据伪装在其他图像中,解决了影子图像的视觉意义问题和视觉质量问题。但这类方法构造的 (t,n) 门限结构迄今都不是理想的,因此这类方法尚欠缺密码学意义上的足够安全性。此外,由于数字图像的像素值在计算机等设备上是按照 m 位的比特值来表示的,故像素值域本质上是 $GF(2^m)$ 而不是素域 F_p。而现有的数字图像分享方法仍然沿用 F_p 表示像素值域——它意味着图像的某些像素值不得不被"截短"或"填长",这就必然造成像素数据的损失或冗余[6]。综上,迄今为止已有的各种图像分享方案[5-33]仍存在着明显的不足,尚不能很好地同时满足人们对安全性的期望和对视觉效果的追求,寻找针对图像分享的完备方案仍然是一个未解决的挑战性问题。

本文聚焦于解决当前图像分享领域中存在的上述根本问题,特别是其中理想的安全性问题。本文的新思路是:

1)不仅仅把图像分享看作像素数据的秘密分享,而且把图像秘密分享看作像素矩阵的秘密分享,由此可以构造像素矩阵的安全 (t,n) 门限结构。

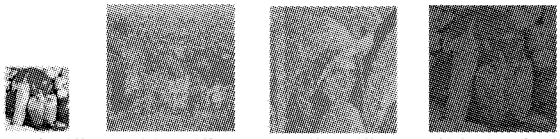
2)由于秘密分享与编码理论的特殊相关性[34-36],对构造像素矩阵的 (t,n) 门限结构来说,采用最大距离可分码(Maximum-Distance-Separable, MDS)性质的编码公式[37]比采用传统的拉格朗日插值多项式更为方便,形式上也更具一般性。

3)通过像素灰度值域 $GF(2^m)$ 上的代数几何编码[37-39],很自然地实现了数字图像 (t,n) 门限秘密分享的一种完备方案:它的门限结构不仅是完全的而且是理想的,它的 n 个影子图像的外在视觉内容都是随机指定的,且影子图像的视觉质量与秘密图像几乎相同。

1 相关研究

秘密分享的理论提出后,Naor 等[7]于 1994 年提出了针对像素图的 VSS 方法,当时也称为视觉密码(Visual Cryptography Scheme, VCS),这是图像秘密分享的开创性工作。VSS 的提出引起了多个领域学者们的广泛兴趣和研究参与,此后相继出现了许多关于黑白像素图像[19]和简单色彩图像[10]20-22的 VSS 方案。这类方案的一个典型例子是:在几张透明胶片上分别打印黑白像素点构成不同的影子图像(可以是没有视觉内容的点阵),其中某些胶片组合重叠在一起时人类视觉能辨认出预定的秘密图像,而其他组合则不会显露秘密图像。计算机屏幕也可以展示 VSS 的效果:用鼠标拖动某些数字图片重合一起时人眼可以看出预定的秘密图像,而其他图片的叠合则没有这种效果。VSS 的基本特征是以人类视觉方法为主来实现像素图在视觉效果上的分拆与合成,不必采用复杂的密码算法,也不要求数据恢复的完整性,而 (t,n) 门限结构的 VSS 则是人们一直追求的目标。但是,VSS 方案的影子图像和恢复图像普遍具有像素扩张膨胀的问题[10]19-22。为消除像素扩张,Kuwakado 等[8]21,23-24后来补充了概率型视觉密码方法。付出的代价则是:恢复的秘密图像更加模糊不清,其影子图像一般也都是没有任何视觉意义的像素点阵。由于 VSS 主要依靠人的视觉感官而不是主要依靠逻辑计算来设计影子图像的像素,随着秘密图像的精细化及其恢复重构的精度提高,VSS 的设计越来越困难,造成其固有的弱点:这类方案都无法保证像素数据的完整性和图像恢复的精确性,这使得其影子图像的视觉品质(清晰度和分辨率等)普遍比较粗糙[8]11,15,23-24,40,许多 VSS 方案也仅适用于非常简单的图像[7]12-15,24,由此恢复的秘密图像也只能粗略地与原始秘密图像相似[8]23,24,40,而且 VSS 的有效的 (t,n) 门限通常只局限于参数的特殊情形,例如,许多文献只给出了 $t=2$ 或 $t=n$[21]40 的方案实例。因此,针对更复杂的视觉内容和更高的恢复精度,如何扩大门限参数 t 和 n 的自由度范围并保持图像像素不扩张,仍是发展视觉密码技术的一大难题。特别地,基于 VSS 的像素构造方法,目前还很难生成同时具有理想性质的门限结构和清晰视觉内容的影子图像。

图 1 中给出了 VSS 的一个(2, 2)门限方案实例[40]:该方案的图像视觉效果在 VSS 中属较好的一类。但该方案只有 $t=n=2$ 的特殊情况下是可行的。



(a) 秘密图像 (b) 影子图像1 (c) 影子图像2 (d) 恢复的秘密图像

图 1 视觉秘密分享

2002 年,Thien 等[6]基于拉格朗日(Lagrange)插值多项式方法在计算机上实现了一种图像数据层的 (t,n) 门限秘密分享方案。该方案是完全的,并且可以处理高精度的彩色数字图像数据的任意 (t,n) 门限秘密分享,恢复的秘密图像数据也是完整的。该方案将一幅秘密图像视为像素数据的一个集合,然后把它映射为具有 (t,n) 门限结构的 n 个数据份额,其标志性的特点是把份额数据量缩小到了大约为原始秘密图像数据量的 $1/t$,从而该方案的每个缩小份额都没有自己独立的视觉意义。但这样的缩小份额便于存储、传输以及隐藏(到其他宿主图像中)。在一系列研究中[26-30],许多后继工作按照 Thien 和 Lin 的方案思路沿着以下方向不断改进:通过无损或有损压缩的图像信源编码技术进一步缩小份额的数据量[26-28];将缩小份额隐藏在大尺寸[26-27]或小尺寸[33]的宿主图像中,从而赋予这些份额外在的视觉内容,成为秘密图像的

影子图像。作为数字图像分享的这类新方法,这些方案通过付出一定的计算复杂性代价,最终克服了 VSS 的大部分固有缺陷。尽管如此,这些方案仍然存在着两方面的根本问题:

1)由于每个缩小份额所属的像素信息空间远比秘密像素空间要小,缩小份额导致了其门限结构不是理想的[1]3-4,基于这种门限结构的方案的安全性总归还是脆弱的(详见第 2 章和第 4 章)。尽管缩小的份额可以隐藏在另外一些宿主图像中[26-30]41,但是一个具有理想门限结构的图像分享方案比一个依靠信息隐藏[42-44]替代措施的图像分享方案在安全性上明显要强壮和可靠得多。Alvarez 等[32]利用离散动力系统原理的可逆胞控自动机方法构造了一种图像秘密分享的理想方案。但该方案仅仅限制于平凡的门限参数时才是可行的,即它仅仅是一个 (n, n) 方案,而且该方案的影子图像只能是不具有外在视觉意义的乱码点阵。

2)数字图像的像素灰度值在现行显示设备上通常用 m 个比特位显示(例如8 比特表示像素灰度值范围为0 ~ 255)。因此,图像分享的像素值运算法则应该建立在正好有 2^m 个不同元素的有限域,例如 $GF(2^m)$。而现有的数字图像分享方案的运算绝大部分是建立在素域 $F_p = \{0, 1, 2, \cdots, p-1\}$ 上的(注意,当 $p > 2$ 时两个有限域 F_p 和 $GF(2^m)$ 不同构)。由于部分像素值在 $F_p = \{0, 1, 2, \cdots, p-1\}$ 上表示时不得不被人为地"截短"或"填长"[26-30],基于素域 F_p 的计算不利于保证恢复图像的数据完整性和精确性。为此,Wang 等[31]提出用伽罗华域 $GF(2^m)$ 代替素域 F_p 的想法,但其实际的运算操作过程仍沿用了 mod (2^m) 的算术运算方式[31],由于当 $m > 1$ 时 2^m 恒不为素数,因此 mod (2^m) 的运算方式完全可能导致计算错误[45]。

现有的图像分享研究工作表明,不论是视觉秘密分享 VSS 的方法还是"传统秘密分享 + 图像隐藏"的简单结合方法,都不足以产生既有高质量伪装视觉内容的影子图像又有完全的和理想的门限结构的图像分享完备方案。

2　主要概念和预备知识

一幅数字图像的 L 个像素值按照其在图像中的排列位置可以自然地表示为一个像素值矩阵,或者形象地表示为三维空间的一张曲面,其中 X-Y 平面坐标指示了像素在图像中出现的位置,Z 坐标指示了像素的值域(如图 2 所示)。

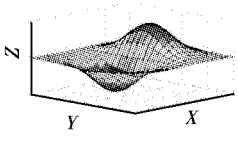


图 2　数字图像像素值构成的曲面

本文用术语图像品质泛指像素密度(Resolution)、像素值范围(Definition)和峰值信噪比(Peak Signal-to-Noise Ratio, PSNR)[44]46,特别是指峰值信噪比。由于任何彩色图像均可用三重灰度像素阵列表示,为讨论简便起见,以下只论及灰度像素图像。设 $1 \leqslant s < t \leqslant n$($s$, t, n 均为正整数)。不失一般性,令 (t,n) 为门限参数,m 为像素灰度值在实际数字显示设备中表示的比特位数,$GF(2^m)$ 为一有限域。显而易见,像素值灰度域与有限域 $GF(2^m)$ 是同构的[37]45。例如,当 $m = 8$ 时,有256 个像素灰度值,不同的灰度值与有限域 $GF(2^m)$ 中的不同元素是一一对应的;反之,有限域中的元素与灰度值也是一一对应。本文所述的所有像素灰度值均从有限域 $GF(2^m)$ 中获得。有限域 $GF(2^m)$ 的加法和乘法运算参见文献[45]。

为描述和衡量一个具有 (t,n) 门限结构的图像分享方案,以下 3 个重要的概念是基本的和必要的。

1) 完全的(Perfect) 方案。对于给定的 s 幅秘密图像 $\boldsymbol{V}_1$, $\boldsymbol{V}_2, \cdots, \boldsymbol{V}_s$,该方案能够生成 n 个份额 $\boldsymbol{G}_i (i = 1, 2, \cdots, n)$,使得其中任意 t 个份额能完整恢复(或精确重构)s 个秘密图像的所有像素数据,而任何 $t-1$ 个或更少的份额都无法揭示出秘密图像的任何像素数据信息。

换言之,完全的方案是指每幅秘密图像 $\boldsymbol{V}_j (j = 1, 2, \cdots, s)$ 都是诸份额的一个函数:$\boldsymbol{V}_j = F_j(\boldsymbol{X}_1, \boldsymbol{X}_2, \cdots, \boldsymbol{X}_t)$,其中 $\boldsymbol{X}_i (i = 1, 2, \cdots, t)$ 为 t 个份额变量。如果将已知的任何 t 个份额的像素数据代入变量 $\boldsymbol{X}_i$,则秘密图像 $\boldsymbol{V}_j$ 的像素数据能够通过计算函数 F_j 来完整获得,而如果已知份额少于 $t-1$ 个,则不可能从函数 F_j 获取任何秘密信息。

2) 理想的(Ideal) 方案。对于给定的秘密图像,该方案能够生成 n 个份额或影子图像 $\boldsymbol{G}_i$,每个影子图像中与门限结构实质关联的像素值集合的信息空间大小等于秘密像素集合的信息空间的大小。用文献[3-4]中提及的信息率 ρ 语言来表达,即:

$$\rho = \frac{\text{lb}(\text{秘密像素信息空间大小})}{\text{lb}(\text{每个实质性份额的像素信息空间大小})} = 1$$

由此容易得到更简明的判断准则:如果一个图像分享的方案是理想的,则它的每个影子图像的像素数量都应该等于 s 个秘密图像的像素数量;反之则不然,除非影子图像中的像素全都与门限结构关联(缺少其中任何一个像素,都不能构成完整的门限方案)。

尽管理想的概念很少在图像分享领域中提及,但它与图像分享的安全性是密切相关的。事实上,一个完全的但非理想的分享方案是不安全的。例如,如果某一个影子图像(比如说 $\boldsymbol{G}_{k_i}$) 的像素信息空间小于秘密图像的信息空间,则敌手即使只获得不足 t 个影子图像(假设 $t-1$ 个份额 $\boldsymbol{G}_{k_i} (i = 1, 2, \cdots, t-1)$,包括 $\boldsymbol{G}_{k_i}$),敌手就可以通过函数 F 在一个比秘密像素空间小的空间上搜索秘密图像信息(即,通过函数 $F(\boldsymbol{G}_{k_1}, \boldsymbol{G}_{k_2}, \cdots, \boldsymbol{G}_{k_{t-1}}, \boldsymbol{X})$,其中 $\boldsymbol{G}_{k_1}, \boldsymbol{G}_{k_2}, \cdots, \boldsymbol{G}_{k_{t-1}}$ 已知,$\boldsymbol{X}$ 未知,但 $\boldsymbol{X}$ 的信息空间可能比秘密图像信息空间要小)。另一方面,如果每个影子图像的像素信息空间大于秘密图像的像素信息空间,则被认为是不必要的浪费。

3)优化的(Optimal)方案。给定具有视觉内容和任意图像品质的秘密图像,该方案能够生成这样的影子图像,其视觉内容是各自随机指定的,因此不会留下秘密图像的任何视觉踪迹,而且影子图像与原秘密图像在图像质量上的差异不易被人眼分辨;从影子图像恢复出来的秘密图像与原秘密图像具有相同的视觉内容,但恢复的像素数据无须和原秘密数据完全相同。

如果一种图像分享方案同时具备以上 3 条性质,我们就称其为图像秘密分享的完备方案(Complete Scheme)。

本文方法中用到两种特殊的矩阵及其重要的性质,表述如下:

定义 1　在 $GF(2^m)$ 上的校验矩阵和生成矩阵。

令 $n \leqslant q-1 \leqslant 2^{m-1}$，$GF(q)$ 是 $GF(2^m)$ 的一个子域，g 是 $GF(q)$ 的一个素元，因此，$a_1 = g^1$，$a_2 = g^2$，…，$a^n = g^n$ 是 $GF(q)$ 中 n 个不同的非零元素。构造一个 $n \times (n-t)$ 的矩阵（本文称它为校验矩阵）如下：

$$\boldsymbol{H}_{n\times(n-t)} = \begin{bmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-t-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-t-1} \\ 1 & a_3 & a_3^2 & \cdots & a_3^{n-t-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-t-1} \end{bmatrix}$$

构造另外一个 $n \times (n-t)$ 的矩阵（本文称它为生成矩阵）如下：

$$\boldsymbol{D}_{n\times t} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ d_{t+1,1} & d_{t+1,2} & d_{t+1,3} & \cdots & d_{t+1,t} \\ d_{t+2,1} & d_{t+2,2} & d_{t+2,3} & \cdots & d_{t+2,t} \\ \vdots & \vdots & \vdots & & \vdots \\ d_{n,1} & d_{n,2} & d_{n,3} & \cdots & d_{n,t} \end{bmatrix}$$

其中：$d_{i,j} \in GF(2^m)$，$\boldsymbol{D}_{n\times t}$ 的任一列向量均与 $\boldsymbol{H}_{n\times(n-t)}$ 的所有列向量正交，且 $\boldsymbol{D}_{n\times t}$ 的前 t 行向量是一个单位子矩阵。

命题 1　给定 $n \times (n-t)$ 的校验矩阵 $\boldsymbol{H}_{n\times(n-t)}$，必存在一个 $n \times t$ 的生成矩阵 $\boldsymbol{D}_{n\times t}$。

证明　$\boldsymbol{H}_{n\times(n-t)}$ 的秩为 $n-t$，这归因于 $\boldsymbol{H}_{n\times(n-t)}$ 的范德蒙行列式结构。这样，$\boldsymbol{H}_{n\times(n-t)}$ 的 $n-t$ 个列向量是线性无关的，且这些列向量能生成 $GF(q)$ 上 n 维线性空间的一个 $n-t$ 维子空间 $\boldsymbol{R}_{n-t}$。因此，就存在 $\boldsymbol{R}_{n-t}$ 的一个正交补子空间 $\boldsymbol{R}_t$，它是一个 t 维线性子空间，满足 $GF(q)$ 上线性子空间的关系：$\boldsymbol{R}_{n-t} \perp \boldsymbol{R}_t$。显然这个正交关系 $\boldsymbol{R}_{n-t} \perp \boldsymbol{R}_t$ 延伸到扩域 $GF(2^m)$ 上讲也是成立的。现在，取 $\boldsymbol{R}_t$ 中的 t 个基向量 $\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \cdots, \boldsymbol{\beta}_t$，把这些基向量作成矩阵 $\boldsymbol{B}_{n\times t}$ 的 t 个列向量 $\boldsymbol{B}_{n\times t} = (\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \cdots, \boldsymbol{\beta}_t)$，则 $\boldsymbol{B}_{n\times t}$ 的任一列向量与 $\boldsymbol{H}_{n\times(n-t)}$ 的每一列向量都是正交的。接着，对 $\boldsymbol{B}_{n\times t}$ 执行列的初等线性变换，直到把 $\boldsymbol{B}_{n\times t}$ 变成这样的矩阵 $\boldsymbol{D}_{n\times t}$，它的前 t 行是一单位子矩阵。由于列的初等线性变换保持 $\boldsymbol{D}_{n\times t}$ 的列向量仍然在子空间 $\boldsymbol{R}_t$ 中，因此 $\boldsymbol{D}_{n\times t}$ 的每一列向量仍然正交于 $\boldsymbol{H}_{n\times(n-t)}$ 的每一列向量（作为 $GF(2^m)$ 上的向量正交）。　证毕。

显然，校验矩阵 $\boldsymbol{H}_{n\times(n-t)}$ 的构造是容易的，根据证明过程，相应的生成矩阵 $\boldsymbol{D}_{n\times t}$ 的构造也总是可行的。

用编码理论的语言来说[37]45，线性方程组 $\boldsymbol{H}^{\mathrm{T}}_{n\times(n-t)} \cdot \boldsymbol{\beta} = \boldsymbol{\theta}$ 的解空间构成一个 (n, t) 线性 MDS 码，即广义里所（Reed-Solomon，RS）码，它是一种特殊的代数几何码（详见文献[37-39]）。从而，$\boldsymbol{\beta} = \boldsymbol{D}_{n\times t} \cdot \boldsymbol{\alpha}$ 称为编码，$\boldsymbol{\beta}$ 称为码字，从 $\boldsymbol{H}^{\mathrm{T}}_{n\times(n-t)} \cdot \boldsymbol{\beta} = \boldsymbol{\theta}$ 求解出 $\boldsymbol{\beta}$ 的过程称为译码。由于秘密分享与编码理论的特殊相关性[34-35]38，对图像分享而言，编码模型可以被认为是一种比插值多项式更一般化的数学模型。显然，线性码的译码过程在本质上与 Blakley 的秘密分享方案[2]中求解多个相交超平面交点的过程等价，而更为专门的广义 RS 码（或代数几何码）的译码过程在本质上则与 Shamir 的秘密分享方案[1]中的确定插值多项式的过程等价。关于 $GF(2^m)$ 域上的编码，见文献[36-38,47]。

3　基于代数几何码的方案

为实现一个完备的图像分享方案，本文最基本的观点就是将图像分享视为像素矩阵的秘密分享，用代数几何（Algebraic Geometry，AG）编码[39]方法取代人们惯用的插值多项式方法，据此实现对像素矩阵中的每一秘密像素值的秘密分享。由此，在秘密像素矩阵的每个像素坐标位置上均可用编码的方法得到该秘密像素值的 n 个份额数据，这 n 个份额数据可以被视为某 n 个其他矩阵在同一坐标位置上对应的 n 个像素值（见图 3）。从具有 MDS 性质[37]45 的 (n, t) 代数几何编码的观点看，在这 n 个像素值（或份额数据）中恒有 t 个像素值是自由的，这 t 个自由的像素值决定了其他 $n-t$ 个像素值。换言之，给定 s 幅秘密图像，我们能据此生成 n 个具有同一 (t, n) 门限结构的像素值阵列（即影子图像），其中至少 t 个像素值阵列可以是具有视觉意义的影子图像，而其他 $n-t$ 个像素值阵列可能是无外在视觉意义的份额数据集。之后，我们用所谓“二次可视分享手续”，进一步使得 n 个像素值阵列均成为共具同一 (t, n) 门限结构而又各具自身外在视觉意义的影子图像。

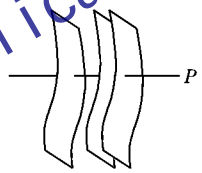


图 3　将图像分享视为像素值阵列分享

本章中的符号 m，$GF(2^m)$，s，t，n，(t, n) 的定义与第 2 章相同。再令 L 表示每幅秘密图像中的像素总数量，P 表示一幅图像的像素阵列中当前像素的坐标位置。显然，2^m 指示了像素值范围（Definition），L 与像素解析度（Resolution）直接相关。

首先，按照第 2 章的定义构造一个生成矩阵 $\boldsymbol{D}_{(n+s)\times t}$ 和一个校验矩阵 $\boldsymbol{H}_{(n+s)\times(n+s-t)}$，其中 $n+s \leqslant q-1 \leqslant 2^{m-1}$，$GF(q)$ 是 $GF(2^m)$ 的子域。注意本节矩阵的行数是 $n+s$（代替第 2 章所述的 n）。

3.1　份额（影子图像）的生成

对于给定 s 幅秘密图像 $\boldsymbol{V}_1$，$\boldsymbol{V}_2$，…，$\boldsymbol{V}_s$，随机补充另外的 $t-s$ 幅图像（每幅图像的视觉内容均为随机选定，每幅图像拥有 L 个像素，每个像素值域均为 $GF(2^m)$），于是共得到 t 幅图像（像素值矩阵）$\boldsymbol{V}_1$，$\boldsymbol{V}_2$，…，$\boldsymbol{V}_s$，…，$\boldsymbol{V}_t$。按照既定的顺序，找到像素值矩阵的当前像素坐标 P，从每个阵列的坐标 P 位置上获取像素值 $a_i \in GF(2^m)$，从而得到坐标 P 上的像素值序列 a_1，a_2，…，a_s，…，a_t，表示为向量 $\boldsymbol{\alpha} = (a_1, a_2, \cdots, a_s, \cdots, a_t)^{\mathrm{T}}$，其中 a_1，a_2，…，a_s 是秘密图像像素值。利用 $\boldsymbol{\alpha}$ 通过生成矩阵 $\boldsymbol{D}_{(n+s)\times t}$ 来构造份额，并通过校验矩阵 $\boldsymbol{H}_{(n+s)\times(n+s-t)}$ 由份额恢复 $\boldsymbol{\alpha}$，具体如下：

从方程 $\boldsymbol{\beta} = \boldsymbol{D}_{(n+s)\times t} \cdot \boldsymbol{\alpha}$ 获得向量 $\boldsymbol{\beta}$，其中矩阵 $\boldsymbol{D}_{(n+s)\times t}$ 和向量 $\boldsymbol{\alpha}$ 的乘法运算是基于 $GF(q)$ 的扩域 $GF(2^m)$ 中。由于 $\boldsymbol{D}_{(n+s)\times t}$ 的上半部分是一个单位矩阵，向量 $\boldsymbol{\beta}$ 的前 t 个元素和 $\boldsymbol{\alpha}$ 的相同，即 $\boldsymbol{\beta} = (a_1, a_2, \cdots, a_s, \cdots, a_t, b_{t+1}, \cdots, b_{t+((n+s)-t)})^{\mathrm{T}}$。弃

掉 s 个秘密图像像素值 $a_1,a_2,\cdots,a_s$,将剩下的像素值 b_{t+1}, $b_{t+2},\cdots,b_{t+((n+s)-t)}$ 分别分配到另外的某 $n+s-t$ 个像素矩阵在坐标 P 的位置上。重复这个步骤,直到 P 遍历过所有 L 个位置,由此我们能够获得 $n+s-t$ 个像素值矩阵 $\boldsymbol{G}_{t+1},\boldsymbol{G}_{t+2},\cdots,\boldsymbol{G}_{t+((n+s)-t)}$。加上前面已经补充的 $t-s$ 幅图像 $\boldsymbol{V}_{s+1},\cdots,\boldsymbol{V}_t$,至此我们可得到 n 个像素值矩阵(即秘密图像的 n 个份额或影子)。上述生成份额像素矩阵的步骤亦即矩阵形式的 AG 编码过程。

如前所述,这里的 $t-s$ 个像素矩阵 $\boldsymbol{V}_{s+1},\cdots,\boldsymbol{V}_t$ 具有各自随机的视觉内容(即随机影子图像),而其他 $n+(t-s)$ 个像素矩阵 $\boldsymbol{G}_{t+1},\cdots,\boldsymbol{G}_{t+((n+s)-t)}$ 被 s 幅秘密图像和 $t-s$ 幅影子图像唯一决定,因此 $\boldsymbol{G}_{t+1},\cdots,\boldsymbol{G}_{t+((n+s)-t)}$ 通常是难以具有独立视觉意义的(在第 4 章将通过一种称为“二次可视分享手续”的方法来改进这个结果,这样便可获得 n 个各具随机外在视觉内容的影子图像 $\boldsymbol{G}_1'$, $\boldsymbol{G}_2'$,$\cdots$,$\boldsymbol{G}_n'$。

3.2　秘密图像的恢复

令 $\boldsymbol{G}_{i_1},\boldsymbol{G}_{i_2},\cdots,\boldsymbol{G}_{i_t}$ 表示任意已知的 t 个份额像素矩阵(影子图像)。$b_{\{j,P\}}$ 为第 j 个已知矩阵 $\boldsymbol{G}_j$ 在坐标位置 P 处的像素数据,$j=i_1,i_2,\cdots,i_t$, $P\in\{1,2,\cdots,L\}$。恢复 s 幅秘密图像在坐标位置 P 处相应的 s 个像素值的过程如下:

为叙述方便,令 $\boldsymbol{\beta}=(b_{\{1,P\}},b_{\{2,P\}},\cdots,b_{\{n+s,P\}})^{\mathrm{T}}$,其中 $b_{\{i_1,P\}},b_{\{i_2,P\}},\cdots,b_{\{i_t,P\}}$ 为已知像素值,其他 $n+s-t$ 个 $b_{\{j,P\}}$ 为未知像素值。由份额像素矩阵的生成过程,可知 $\boldsymbol{\beta}=\boldsymbol{D}_{(n+s)\times t}\cdot\boldsymbol{\alpha}$。根据第 2 章给出的生成矩阵和校验矩阵的性质,可知校验矩阵 $\boldsymbol{H}_{(n+s)\times(n+s-t)}$ 的每一列向量与生成矩阵 $\boldsymbol{D}_{(n+s)\times t}$ 列向量张成的线性子空间是正交的,即:方程 $\boldsymbol{H}^{\mathrm{T}}_{(n+s)\times(n+s-t)}\cdot\boldsymbol{\beta}=\boldsymbol{\theta}$ 成立。其中矩阵与向量的乘法运算都在 $GF(q)$ 的扩域 $GF(2^m)$ 中进行。从方程 $\boldsymbol{H}^{\mathrm{T}}_{(n+s)\times(n+s-t)}\cdot\boldsymbol{\beta}=\boldsymbol{\theta}$ 可以得到如下线性方程组:

$$\begin{cases} b_{1,P}+b_{2,P}+\cdots+b_{n+s,P}=0 \\ a_1b_{1,P}+a_2b_{2,P}+\cdots+a_{n+s}b_{n+s,P}=0 \\ a_1^2b_{1,P}+a_2^2b_{2,P}+\cdots+a_{n+s}^2b_{n+s,P}=0 \\ \cdots \\ a_1^{n+s-t-1}b_{1,P}+a_2^{n+s-t-1}b_{2,P}+\cdots+a_{n+s}^{n+s-t-1}b_{n+s,P}=0 \end{cases}$$

其中:$b_{\{i_1,P\}},b_{\{i_2,P\}},\cdots,b_{\{i_t,P\}}$ 已知。

将含已知数的项都移到方程右端并保留含未知数的项在方程左端,恰好得到含 $(n+s-t)$ 个未知数且有具 $(n+s-t)$ 个方程的线性方程组:

$$\boldsymbol{A}^{\mathrm{T}}_{(n+s-t)\times(n+s-t)}\cdot\boldsymbol{\gamma}=\boldsymbol{\eta}$$

其中:$\boldsymbol{\gamma}=(b_{\{k_1,P\}},b_{\{k_2,P\}},\cdots,b_{\{k_{n+s-t},P\}})^{\mathrm{T}}$ 为 $GF(2^m)$ 上的未知向量,$\boldsymbol{\eta}=(c_1,c_2,\cdots,c_{n+s-t})^{\mathrm{T}}$ 为 $GF(2^m)$ 上的已知向量,而矩阵 $\boldsymbol{A}^{\mathrm{T}}_{(n+s-t)\times(n+s-t)}$ 是一个 $(n+s-t)\times(n+s-t)$ 的范德蒙方阵:

$$\boldsymbol{A}^{\mathrm{T}}_{(n+s-t)\times(n+s-t)}=\begin{bmatrix} 1 & a_{k_1} & \cdots & a_{k_1}^{n+s-t-1} \\ 1 & a_{k_2} & \cdots & a_{k_2}^{n+s-t-1} \\ \vdots & \vdots & & \vdots \\ 1 & a_{k_{n+s-t}} & \cdots & a_{k_{n+s-t}}^{n+s-t-1} \end{bmatrix}$$

各个 a_{k_j} 互异且 $a_{k_j}\in GF(q)$,$a_{k_j}\neq 0$。因此,方程组 $\boldsymbol{A}^{\mathrm{T}}_{(n+s-t)\times(n+s-t)}\cdot\boldsymbol{\gamma}=\boldsymbol{\eta}$ 在 $GF(2^m)$ 上有唯一解向量 $\boldsymbol{\gamma}$,$\boldsymbol{\gamma}$ 的前 s 个分量即是 s 个秘密像素矩阵(s 幅秘密图像)在坐标 P 处对应的 s 个像素值。重复上述步骤,遍历所有 L 个坐标位置 P,即可重构出 s 幅秘密图像。以上恢复秘密图像的步骤可以扼要地理解为 AG 码的一种矩阵方式的译码过程。

例 1　单一秘密图像的(6,7)门限分享方案(AG 编码方法)。

如图 4 所示,图(a)是一幅秘密图像(即 $s=1$),图(b)~(h)是秘密图像(a)的 7 个份额(未经二次可视分享),其中图(b)~(f)是有外在直观视觉意义的影子图像,而图(g)和(h)是由图(a)和图(b)~(f)决定的,类似于随机噪声图像。影子图像(b)~(f)的视觉内容是可以任意选取的,且图像品质与秘密图像严格相同,其任何像素中均无噪声。图(i)是从随机选取的 6 个份额(比如图(c)~(h))重构恢复的秘密图像,它与原始秘密图像是完全相同的(对应的像素数据严格相等)。显然,该例子给出的图像门限分享方案是完全的和理想的(具体的分析见第 5 章),但它并不是优化的,因为它的某些份额像素矩阵没有外在的直观视觉内容。

图 4　单一秘密图像的(6,7)门限分享方案

3.3　$GF(2^m)$ 上图像分享的并行处理

一般而言,以上过程中涉及的计算都是基于像素值域 $GF(2^m)$ 的运算法则的。如果我们将这种 $GF(2^m)$ 上像素矩阵的秘密分享进一步分解为 $GF(2^{m/2})$ 上两个像素矩阵分别的秘密分享的某种组合,则本节中图像分享的计算效率还可以大大提高。具体做法如下:

不失一般性,设 m_1、m_2 和 m 为正整数,$m=m_1+m_2$,于是 $GF(2^m)$ 与 m 个比特位表示的像素值域同构。令 $GF(2^{m_1})$ 与某 m_1 个比特位表示的像素值域同构,而 $GF(2^{m_2})$ 与其余 m_2 个比特位表示的像素值域同构。以下过程称为 $GF(2^m)$ 上图像分享的并行处理:给定显示设备上任意一个像素值(μ_1, $\mu_2,\cdots,\mu_m$),$\mu_i=0$ 或 1(它是一个 m 位的比特值的向量,可以把它区分为前面 m_1 位的比特值与后面 m_2 位的比特值),存在唯一的对应元素 $\boldsymbol{\alpha}\in GF(2^m)$。于是可以将 $\boldsymbol{\alpha}\in GF(2^m)$ 视为 $\boldsymbol{\beta}_1\in GF(2^{m_1})$(对应于前面 m_1 位的比特值)和 $\boldsymbol{\beta}_2\in GF(2^{m_2})$(对应于后面 m_2 位的比特值)的某种“并列”。为减少 $GF(2^m)$ 上涉及 $\boldsymbol{\alpha}$ 的计算量,我们分别执行或并行执行 $GF(2^{m_1})$ 上涉及 $\boldsymbol{\beta}_1$ 的计算以及 $GF(2^{m_2})$ 上涉及 $\boldsymbol{\beta}_2$ 的计算,然后取两方面计算结果的形式“并列”即可,这就取代了 $GF(2^m)$ 上涉及 $\boldsymbol{\alpha}$ 的直接计算。例如,将 8 位的比特值(μ_1, $\mu_2,\cdots,\mu_8$)表示的像素值 $\boldsymbol{\alpha}\in GF(2^m)$ 看作是由 4 位的比特值(μ_1, μ_2, μ_3, μ_4)与(μ_5, μ_6, μ_7, μ_8)分别表示的两个像素值

$\boldsymbol{\beta}_1 \in GF(2^{m_1})$ 与 $\boldsymbol{\beta}_2 \in GF(2^{m_2})$ 的某种“并列”，其中 $\mu_i = 0$ 或 $1(i = 1,2,\cdots,8)$。这样，就可以用更小的域 $GF(2^4)$ 上的两次快速计算取代更大的域 $GF(2^8)$ 上的一次慢速计算。这样的方式同样可以实现数字图像分享的各种方案，而且能够极大地降低有关像素域 $GF(2^m)$ 的计算复杂性。

4 二次可视分享

按照第 3 章所述，对于给定的秘密图像，我们可以获得其具有 (t,n) 门限结构的 n 个份额，其中 $t-s$ 个份额 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_{t-s}$ 可以是自由选取的具有任何视觉内容的影子图像，其他 $n-(t-s)$ 个份额 $\boldsymbol{G}_{(t-s)+1},\cdots,\boldsymbol{G}_{(t-s)+n-(t-s)}$ 是由秘密图像和 $t-s$ 个具有视觉内容的影子图像所决定的，通常不具有外在的直观视觉意义。本章介绍一个所谓“二次可视分享”过程来进一步改进 $n-(t-s)$ 个份额 $\boldsymbol{G}_{(t-s)+1},\cdots,\boldsymbol{G}_{(t-s)+n-(t-s)}$ 的外在视觉效果，通过该过程，我们能够把第 3 章得到的 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_{t-s}$ 和 $\boldsymbol{G}_{(t-s)+1},\cdots,\boldsymbol{G}_{(t-s)+n-(t-s)}$ 改进为 n 个新的影子图像 $\boldsymbol{G}_1',\boldsymbol{G}_2',\cdots,\boldsymbol{G}_n'$。改进后的诸影子图像不仅都具有了各自独立的外在视觉内容，而且还保持着同一(t,n) 门限结构。以下为叙述方便起见，$\boldsymbol{V}_1,\cdots,\boldsymbol{V}_{t-s}$ 和 $\boldsymbol{G}_{(t-s)+1},\cdots,\boldsymbol{G}_{(t-s)+n-(t-s)}$ 统称为原始份额，$\boldsymbol{G}_1',\boldsymbol{G}_2',\cdots,\boldsymbol{G}_n'$ 称为最终份额。

本章中的符号 s，t，n，(t,n)，m，$GF(2^m)$，L 和 P 仍如第 2 章和第 3 章的定义，$\boldsymbol{D}_{n\times t}$ 和 $\boldsymbol{H}_{n\times(n-t)}$ 分别是第 2 章定义的生成矩阵和校验矩阵，另设$\lceil L/t\rceil$为 L/t 的 Ceiling 函数。如前所述，第 3 章中得到的 $t-s$ 个影子图像 $\boldsymbol{V}_k(k = 1,2,\cdots,t-s)$ 可以自由选取，不妨假设每个 $\boldsymbol{V}_k(k = 1,2,\cdots,t-s)$ 均为第 2 节所定义的一个“$d(P)$ 比特缺省图像”，亦即一种宿主图像[42-43]。

4.1 二次可视分享步骤

对 $n-(t-s)$ 个没有外在视觉意义的原始份额 $\boldsymbol{G}_{(t-s)+1},\cdots,\boldsymbol{G}_{(t-s)+n-(t-s)}$ 中的每个 $\boldsymbol{G}_k(k = (t-s)+1,\cdots,(t-s)+n-(t-s))$，二次可视分享手续包括以下 3 个步骤。

第 1 步　将 $\boldsymbol{G}_k$ 分拆为两个部分：

$$\boldsymbol{G}_k = \boldsymbol{V}_k + \boldsymbol{U}_k; k = (t-s)+1,\cdots,(t-s)+n-(t-s)$$

其中：“+”是指域 $GF(2^m)$ 上的两个像素值矩阵 $\boldsymbol{V}_k$ 和 $\boldsymbol{U}_k$ 的加法运算；$\boldsymbol{V}_k$ 是随机指定了视觉内容的一幅“$d(P)$ 比特缺省图像”；$\boldsymbol{U}_k$ 是由 $\boldsymbol{G}_k$ 和 $\boldsymbol{V}_k$ 决定的一像素值矩阵（一般没有独立的视觉意义）。显然，这种在域 $GF(2^m)$ 上的矩阵分拆总是可行的，而且 $\boldsymbol{G}_k$、$\boldsymbol{V}_k$ 和 $\boldsymbol{U}_k$ 的像素总数仍是 L。这样可以又得到 $n-(t-s)$ 幅图像 $\boldsymbol{V}_{(t-s)+1},\cdots,\boldsymbol{V}_{(t-s)+n-(t-s)}$。加上第 3 章得到的 $(t-s)$ 幅图像 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_{t-s}$，至此一共可以得到 n 幅各具随机选定视觉内容的图像 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_{t-s},\boldsymbol{V}_{(t-s)+1},\cdots,\boldsymbol{V}_{(t-s)+n-(t-s)}$，按约定，它们都是 $d(P)$ 比特缺省图像，本节以下也把它们称为宿主图像。对每一个 $\boldsymbol{U}_k$，继续施行以下步骤：

第 2 步　生成 $\boldsymbol{U}_k$ 的 n 个缩小份额。首次从一幅图像获得 n 个缩小份额的工作[6] 是基于插值多项式的，这里将它发展为更一般的编码方式：将 $\boldsymbol{U}_k$ 的 L 个像素值按每 t 个像素值一组划分为$\lceil L/t\rceil$个集合（若除不尽，某一集合所含像素较少，此时可以随意用其他值补齐它），每个集合记为 $\boldsymbol{\alpha}_r = (a_{r_1},a_{r_2},\cdots,a_{r_t})^{\mathrm{T}}(r = 1,2,\cdots,\lceil L/t\rceil)$。类似第 3 章的步骤，通过方程式 $\boldsymbol{\beta} = \boldsymbol{D}_{n\times t}\cdot\boldsymbol{\alpha}$ 可从已知向量 $\boldsymbol{\alpha}_r$ 得到未知向量 $\boldsymbol{\beta}_r = (b_{r_1},b_{r_2},\cdots,b_{r_n})^{\mathrm{T}}(b_{r_i} \in GF(2^m))$，将获得的每个 b_{r_i} 记入相关集合 $W_{k_i}(i = 1,2,\cdots,n)$，即：将第 i 个值 b_{r_i} 置入第 i 个集合 W_{k_i} 中。重复该过程，从 $r = 1$ 到$\lceil L/t\rceil$遍历所有 $\boldsymbol{\alpha}_r$ 和 $\boldsymbol{\beta}_r$，于是由 $\boldsymbol{U}_k$ 可以得到 n 个集合 W_{k_i}。每个集合 W_{k_i} 显然正含$\lceil L/t\rceil$个像素值，称 W_{k_i} 为 $\boldsymbol{U}_k$ 的 n 个缩小份额。

利用校验矩阵 $\boldsymbol{H}_{n\times(n-t)}$ 的性质，按照第 3 章的类似步骤，容易从任意 t 个以上的缩小份额 W_{k_i} 恢复得到 $\boldsymbol{U}_k$。亦即，这 n 个缩小份额依然保持着第 3 章所述的(t,n) 门限性质，但缩小份额一般没有独立的视觉意义。

第 3 步　将 $\boldsymbol{U}_k$ 的 n 个缩小份额分别嵌入到上述得到的 n 幅宿主图像：对于 $\boldsymbol{U}_k$ 的第 i 个缩小份额 W_{k_i}，把该份额中包含的每个 b_{r_i} 值转换成为对应的 m 个比特位的二进制数据。将这些数据统一排列成一种比特序列，并从该序列中取每 $d(P)$ 个比特值为一个数据分块，依次将每个数据分块逐个嵌入到 W_{k_i} 所对应的宿主图像 $\boldsymbol{V}_i$ 中尚未填充的像素缺省比特位上，直到将 W_{k_i} 的所有数据分块都逐步嵌入 $\boldsymbol{V}_i$ 中。从 $i = 1$ 到 n，对每个 W_{k_i} 都施行如上操作，直到把当前 $\boldsymbol{U}_k$ 的 n 个缩小份额分别嵌入到 n 幅宿主图像 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_{t-s},\boldsymbol{V}_{(t-s)+1},\cdots,\boldsymbol{V}_{(t-s)+n-(t-s)}$ 中。

对所有的 $\boldsymbol{U}_k(k = (t-s)+1,\cdots,(t-s)+n-(t-s))$ 逐个重复第 2 ~ 3 步。这样，原来的 n 幅宿主图像 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_{t-s},\boldsymbol{V}_{(t-s)+1},\cdots,\boldsymbol{V}_{(t-s)+n-(t-s)}$ 被更新（填充）为 n 个最终份额 $\boldsymbol{G}_1',\cdots,\boldsymbol{G}_{t-s}',\boldsymbol{G}_{t-s+1}',\cdots,\boldsymbol{G}_{(t-s)+n-(t-s)}'$，它们显然仍保持着先前的$(t,n)$ 门限结构，并且其中每个最终份额 $\boldsymbol{G}_k'$ 还具有和 $\boldsymbol{V}_k$ 相同的视觉内容，$k = 1,2,\cdots,t-s,(t-s)+1,\cdots,(t-s)+n-(t-s)$。至此，可以称 n 个最终份额 $\boldsymbol{G}_1',\cdots,\boldsymbol{G}_{t-s}',\boldsymbol{G}_{t-s+1}',\cdots,\boldsymbol{G}_{(t-s)+n-(t-s)}'$ 为秘密图像的 n 个影子图像。

按照二次可视化手续的逆过程，从 n 个最终份额中的任何 t 个份额，容易恢复出每一个原始份额 $\boldsymbol{G}_k$。步骤如下：首先，从第 i 个最终份额 $\boldsymbol{G}_i'$ 中提取出第 i 个缩小份额 W_{k_i}，这样从任意 t 个最终份额可以提取出 $\boldsymbol{U}_k$ 的 t 个缩小份额，从而由这 t 个缩小份额利用校验矩阵 $\boldsymbol{H}_{n\times(n-t)}$ 按第 3 章的方法可以恢复出 $\boldsymbol{U}_k$。其次，为恢复宿主图像 $\boldsymbol{V}_k$，只要将与之相应的最终份额 $\boldsymbol{G}_k'$ 的所有像素的 $d(P)$ 个缺省比特重新置为 0 即可。最后，由式(1) 可得到原始份额 $\boldsymbol{G}_k$。

为恢复秘密图像，需要 t 个原始份额。如果 $n-(t-s) \geqslant t$，则原始份额 $\boldsymbol{G}_k$ 已经足够；如果 $n-(t-s) < t$，除了 $\boldsymbol{G}_k$ 之外还需要附加 $r(r = t-(n-(t-s)))$ 个原始份额 $\boldsymbol{V}_j(j = 1,2,\cdots,r)$。这可以在 t 个已知的最终份额中再另选定 r 个最终份额，并将它们的 $d(P)$ 个缺省比特位全都重新置为 0 来获得。

显然，在每幅宿主图像中，只要被嵌入的比特数据总量与宿主图像中所有 $d(P)$ 比特缺省数据总量之比 δ 满足 $\delta = (n-(t-s))/t < 1$ 以上二次可视分享的步骤就是可行的。4.2 节表明，并且当$\delta \geqslant 3/8$时，嵌入数据前后的宿主图像在视觉上没有很明显的区别。

例 2　两幅秘密图像的(8,9)门限分享方案（基于 AG 编码）。

在图 5 中，图（a）和（b）是两幅秘密图像（$s = 2$），图（c）~（k）是用本文 AG 编码方法生成的 9 个影子图像（最终份额）。该方案是完全的和优化的，但并非理想的，因为每个影子图像的像素信息空间显然小于两幅秘密图像的像素信息空间。图(l)和(m)表示从图（c）~（k）中的任意 8 幅图像

重构恢复的秘密图像,它们分别与图(a)和(b)相同(对应位置上的每个像素值都是严格相等)。此外,影子图像(c)~(k)的视觉内容是任意选择的,只是在它们的广义最低有效位(Least Significant Bit, LSB)有一点人为的噪声。但这种噪声对影子图像视觉效果的影响并不明显(见 4.2 节或文献[43])。

图 5　两幅秘密图像的(8,9)门限分享方案

例 3　基于 AG 编码的(9,11)门限分享的完备方案与其他方案比较。

图 6 给出了基于 AG 编码方法的一个(9,11)门限分享方案,它是完全的、理想的和优化的完备方案。其中图(a)是一幅秘密图像($s=1$),图(b)~(l)是秘图的影子图像(最终份额)。作为对比,图 7 是按文献[6](也见文献[25-29,33]等)构造的(9,11)门限分享方案,其中图(b)~(l)是秘密图像(图(a))的 11 个缩小份额,每个份额的大小约为秘密图像的1/t。按文献[26-27,33]推荐的做法,我们进一步假定 11 个缩小份额可以被分别嵌入到其他某 11 幅宿主图像(不妨假定其尺寸分别与图 6 中的(b)~(l)相同)中隐藏起来。这两种方案在安全性上最根本的区别在于:第一,按文献[6,26-27,33]等提出的方案,其宿主图像中,除嵌入的缩小份额数据之外,其他更多的像素数据仅仅用来掩饰缩小份额(冗余的像素越多,掩饰效果越好),而与 (t,n) 门限毫无关系。于是,在任何 9 个宿主图像中,只要获得其中的一小部分数据(9 个缩小份额的数据),就足以通过 (t,n) 门限恢复出秘图(a)。相比之下,按本文方案,对于恢复秘图(a)来说,至少要有 9 幅影子图像,且这 9 幅影子图像中所有的像素值对于(9,11)门限结构都是必要的(缺一则不能重构相应的秘密像素)。第二,假定敌手获得了 $t-1=8$ 幅影子图像(例如,本文方案的图(b)~(i),或者文献[6,25]等方案中含缩小份额(图 7 中的图(b)~(i))的某 8 幅宿主图像),敌手据此得到 (t,n) 门限所需的 8 个数据集。此际敌手可通过以下两个步骤来搜寻秘密图(a):1)在门限函数 $Secret\ Image = F(\boldsymbol{X}_1, \boldsymbol{X}_2, \cdots, \boldsymbol{X}_8, \boldsymbol{X}_9)$ 中用 8 个已知数据集 $C_1, C_2, \cdots, C_8$ 代替 8 个未知数据集 $\boldsymbol{X}_1, \boldsymbol{X}_2, \cdots, \boldsymbol{X}_8$,其中函数 F 是拉格朗日插值函数或编码公式;2)由于 $Secret\ Image = F(C_1, C_2, \cdots, C_8, \boldsymbol{X}_9)$,敌手只需在第 9 个未知数 $\boldsymbol{X}_9$ 空间中搜索秘图(图(a))。在这种情况下,本文方案仍然还是安全的,这是因为第 9 个影子图像的像素信息空间与秘密图像的像素信息空间大小相同(都等于数量级 2^{Lm}),故敌手的这种行为无异于在秘密像素空间中盲搜索。相比之下,文献[6]等所提方案在面对敌手的这种搜索时明显脆弱了许多,这是因为破解门限结构所需的每个份额的数据空间大小都大为缩小(到数量级 $2^{Lm/9}$,远小于 2^{Lm})。

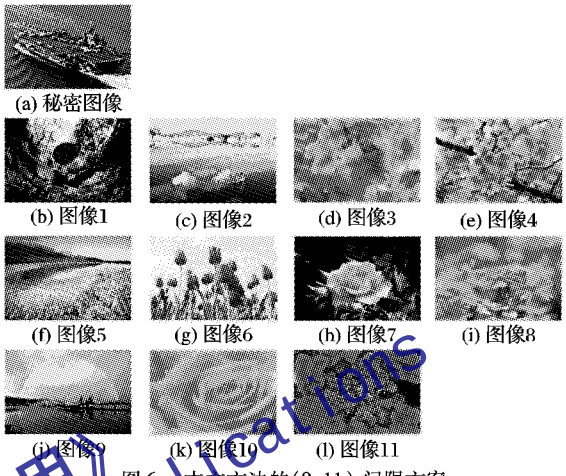


图 6　本文方法的(9,11)门限方案

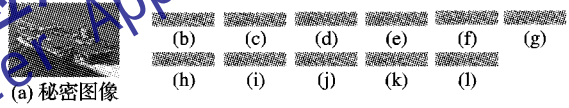


图 7　文献[6]的(9,11)门限方案

4.2　$d(P)$ 位缺省图像定义

设正整数 $d<m$,如果一幅图像的每个像素的 d 个最低有效位LSB[43] 上均置为 0,则称该图像为 d 位缺省图像。更一般地,设 $d(P)$ 是坐标 P 的一个正整数函数,$d(P)<m$,且函数 $d(P)$ 满足方程:

$$\sum_{P=1}^{L} d(P) = (n-(t-s)) \cdot m \cdot \lceil L/t \rceil$$

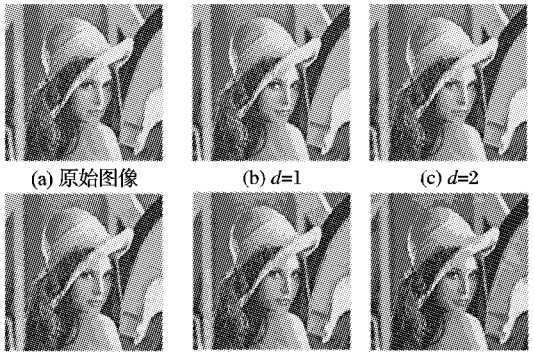
如果一幅图像的每个像素的 $d(P)$ 个最低有效位(广义 LSB)上均置为 0,则该图像称为 $d(P)$ 位缺省图像。显然,当 $(n-(t-s))/t = \delta (0<\delta \leqslant 1)$ 时,函数 $d(P)$ 总是存在。如果 t 能整除 L,且有一个正整数 d 满足等式:

$$d/m = (n-(t-s))/t = \delta;\ 0<\delta \leqslant 1$$

则可以用整数 d 来代替函数 $d(P)$。鉴于在 $d(P)$ 或 d 个缺省比特位中隐藏信息后的视觉效果,本文取 $\delta \leqslant 3/8$。图 8 是取不同 δ 的 d 位缺省图像示例。

实验证明,$\delta = (n-(t-s))/t < 3/8$ 时,$d(P)$ 位缺省图像与其原图像的差异对视觉感受几乎没有影响(不论在 $d(P)$ 位上嵌入何种数据或者置 0)。因此,$d(P)$ 位缺省图像的所有 $\sum_{P=1}^{L} d(P)$ 个缺省位可用来隐藏信息,故本文称它为宿主图像[42],$d(P)$ 个缺省比特位也就简称为广义最低有效位。换句话说,尽管在宿主图像的广义最低有效位上时常有人为噪声(嵌入了其他数据),但人眼不易察觉它与原图像在图像质量上的差别。而且,函数 $d(P)$ 确实保证了 $d(P)$ 位缺省图像中缺省比特位数的总和等于 $(n-(t-s)) \cdot m \cdot \lceil L/t \rceil$,这正

好是 4.1 节中所述的$(n-(t-s))$个像素数据集合中像素比特位数的总和,其中每个像素数据集合恰有$\lceil L/t \rceil$个像素值。



(a) 原始图像 (b) d=1 (c) d=2

(d) d=3 (e) d=4 (f) d=5

图 8 d 位缺省图像

5 本文方案的性能分析

5.1 安全性

根据第 3 ~ 4 章,如果已知任意 t 个以上的最终份额(影子图像),很容易恢复出 t 个原始份额,进而由 t 个原始份额重构恢复 s 幅秘密图像;另一方面,如果只有 $t-1$ 个或更少的最终份额,则无法恢复出秘密图像的任何一部分部分像素值(只有盲搜索一条路可走),因为此时必须求解一个至少有 $k+1$ 个未知数而至多只有 k 个方程的线性方程组,其中 $k=n-t$。因此本文所提方案的门限结构是完全的。

根据第 4 章所述,当 $s=1$(即一幅秘密图像的情形),本文方案中每个影子图像(或每个份额)的像素数量都等于秘密图像的像素数量(均等于 L),每个影子图像(或每个份额)的所有像素数据都是(t,n)门限结构所必需的,也就是说,门限结构中的每个实质性份额的信息空间大小和秘密信息空间大小是等同的(例如均为 2^{Lm})。亦即,此际信息率 ρ 满足:

$$\rho=\frac{\text{lb}(\text{秘密像素信息空间大小})}{\text{lb}(\text{每个实质性份额的像素信息空间大小})}=1$$

这表明了当 $s=1$ 时本文所提方案的门限结构是理想的。应当指出,当 $s>1$ 时本文方案就不再是理想的,因为此时每个影子图像的尺寸(像素信息空间)明显小于 s 幅秘密图像的尺寸(像素信息空间)之和。

相比之下,文献[6,26 - 30]等所提方案都不是理想的(不论 $s=1$ 或 $s>1$),因为对门限结构不可或缺的每个实质性份额的信息空间大小(像素数据量)缩小到了 $2^{Lm/t}$ 级。从 $2^{Lm/t} \ll 2^{Lm}/t < 2^{Lm}$ 的事实,可以得出结论:门限参数 t 越大,这些方案的理想安全性就越脆弱。

5.2 视觉效果

在本文方案中,图像质量和图像内容均不受到任何限制,域 $GF(2^m)$ 上的像素值阵列足以描述任何分辨率(Definition)和解析度(Resolution)的数字图像。此外,本文方案在图像分享过程中没有任何像素值损失,所以恢复的秘密图像与原秘密图像精确相等。相比之下,其他数字图像分享方案[6]26-30 则是基于近似像素值域 $F_p=\{0,1,2,\cdots,p-1 \bmod p\}$ 的,其中像素值大于 $p-1$ 的部分要么不得不删掉(造成失真),要么需要把额外计算的结果追加到门限结构中的份额上(造成数据冗余)。至于视觉秘密分享方案,由于其固有的技术风格和技术体系所限,它们的影子图像被限制在比较简单的内容或低品质图像,迄今为止它们的视图仍局限于较粗糙的图像,且只能刻画较简单的视觉内容。

如第 3 章和例 1 所述,与其他数字图像秘密分享方案相较,本文方案不依赖于图像隐藏技术[42-44],本文方案(在"二次可视分享手续"之前)生成的 n 个原始份额不仅具有完全的和理想的(t,n)门限结构,而且当中$(t-s)$个份额已经具有了独立的视觉意义(其视觉内容随机选择,其图像质量与秘密图像完全相同),这是本文方案的一个鲜明特点。

进一步施行"二次可视分享手续"后,由于在 $d(P)$ 个缺省比特位上嵌入了数据,即有人为噪声的影响(参见 4.2 节),本文方案中的影子图像(最终份额)与秘密图像在图像质量上存在着客观差异。然而当 $\delta=(n-(t-s))/t<3/8$ 时,这种差异不易被肉眼察觉(参见 4.2 节),而且也不影响每个影子图像具有各自随机选取的视觉内容,不等式 $\delta=(n-(t-s))/t<3/8$ 保证了影子图像能够自由选取品质足够高的任意视觉内容。

此外,本文基于 AG 编码的方案很自然地避免了许多其他方案通有的瑕疵[6]26-27,即:影子图像易于泄露秘密图像中相邻像素间的视觉联系(所以不得不采取一些附加的补救措施[31],但这又增加了运算开销)。

5.3 计算和存储开销

本文方案的基本思想也完全可以通过插值多项式的传统方法来实现(以下简称 LS 方案)。但是,基于 AG 编码的图像分享方案具有更一般的表述形式,也具有更丰富的手段来进一步提升方案的计算时间效率和存储空间效率。另一方面,基于 AG 编码模型产生的影子图像数据的存储量通常要小于基于插值多项式模型的 LS 方案的数据存储量,这是因为 AG 编码的生成矩阵和校验矩阵均是独立于方案中所涉及的所有图像的。相比之下,LS 方案中每个具体的插值多项式都须与所涉及的图像像素数据密切关联才行,而这种关联要带入存储中。3.3 节建议了一种具体的快速计算方法,它可以将一个较大像素值域 $GF(2^m)$ 中的计算转换为若干较小像素域(比如 $GF(2^{m/2})$)中的并行计算。我们的实验表明,对于像素值域 $GF(2^m)$ 上图像分享方案来说,当计算效率优先时,这是大幅度减少时间代价的有效方法。

表 1 概要地归纳了不同图像秘密分享方案的性能对比。

6 结语

本文给出了一种 s 幅秘密图像(t,n)门限分享的新方法。利用这种方法,当 $s=1$ 时能获得一个图像(t,n)门限分享的完备方案:它是完全的、理想的和优化的图像门限秘密分享方案。显然,该方案在保证影子图像高品质的同时,比现有各种方案都更加安全。

新方法是基于完全像素域 $GF(2^m)$ 上 AG 码的,消除了传统上基于近似像素域 F_p 的插值多项式方法的不足:F_p 上的像素计算必然导致数字图像秘密分享方案中的像素数据损失或者冗余,因为当 $p>2$ 时,域 $F_p=\{0,1,2,\cdots,p-1\}$ 与 $GF(2^m)$ 恒不同构。本文方法不仅修复了此前数字图像分享工作中像素值处理的缺陷[6]26-29,而且还提供了更多样化的可能手段来提升图像分享方案的计算时间效率与存储空间效率。

为防范具有关键视觉意义的少部分像素遭受重点攻击,可以在图像分享之前先对秘密像素矩阵进行置乱排序(虽然不是必须的),然后再实施本文第 2 章和第 3 章的方法。本文利用迭代函数的混沌性质[48],对像素矩阵(看成是 L 个像素

的一个序列）进行了置乱排序,而置乱排序的密钥信息(迭代函数的初值）取为全体像素值之和(即:L 个像素的 m 位的比特值的异或,它仍是一个 m 位的比特值)。显然,由于加法运算的可交换性,全体像素值之和与像素的排序无关,故这种密钥信息无需存储在图像分享方案中,理由如下:若已知 t 个影子图像,则通过(t,n) 门限结构可得到秘密图像的乱序像素矩阵,它的全体像素值之和就是置乱排序的密钥信息,据此可恢复置乱前的秘密图像;若不足 t 个影子图像,则无法得到秘密图像的全部像素数据,当然更无从获得置乱排序的密钥信息。于是,在图像分享方案中补充这种特定的置乱措施,不仅使集中攻击一小部分敏感像素值的企图失去了意义,而且也自然地避免了密钥保管引起的其他安全问题。

表 1　不同图像秘密分享方案性能对比

方　　案	像素值域	完全的	理想的	优化的	恢复的数据或图像	计算复杂度	存储复杂度
本文方案($s=1$),不使用任何图像隐藏技术	$GF(2^8)$ 中的 256 个值	是	是	除少数份额之外	完整的和精确的恢复	$GF(2^m)$ 上的 $\sim O((n-t)^2)$	一幅秘密图像存储量的 n 倍
本文方案($s=1$),含二次可视分享手续	$GF(2^8)$ 中的 256 个值	是	是	是	完整的和精确的恢复	$GF(2^m)$ 上的 $\sim O((n-t)^2)$	一幅秘密图像存储量的 n 倍
本文方案($s=1$),采用 3.3 节中的方法加速计算	$GF(2^8)$ 中的 256 个值	是	是	是	完整的和精确的恢复	较小的域 $GF(2^{m/2})$ 上 $\sim O((n-t)^2)$	一幅秘密图像存储量的 n 倍
文献[6]等为代表的方案(不使用图像隐藏)	$\{0\sim250\}$/mod 251 产生的 251 个值	是	否	否	完整的和精确的恢复	F_p 上的 $\sim O(t^2)$	一幅秘密图像存储量的 n/t 倍
文献[26－30]等为代表的方案类(使用图像隐藏)	$\{0\sim250\}$/mod 251 产生的 251 个值	是	否	是	完整的和精确的恢复	F_p 上的 $\sim O(t^2)$	一幅秘密图像存储量的 n 倍
代表性的 VSS 方案(有像素扩张)	在{0,1}或类似集合中的符号	是,但实际的(t,n) 门限参数一般很小	否	否	粗略与秘密图像相似	不用计算或只需少量计算	大于一幅秘密图像存储量的 n 倍
兼顾计算复杂度性能和门限安全性的其他方案	在{0,1}或 F_{251} 上的符号	是,但仅局限于门限参数的平凡情况 $t=n$ 或 $t<4$	未见研究报道	是,但局限于门限参数(t,n)的平凡情况如 $t=n$	不保证数据恢复的完整性	约 $\sim O(t)$	一幅秘密图像存储量的 n 倍

致谢　感谢张景中院士和杨路教授对我们承担的中国科学院知识创新工程子课题的指导和支持,特别感谢马里兰大学 Shaw W 博士的深刻见解和诚挚帮助。

参考文献:

[1] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612－613.

[2] BLAKLEY G R. Safeguarding cryptographic keys [C]// Proceedings of the National Computer Conference. New York : AFIPS, 1979: 313－317.

[3] DAWSON E, DONOVAN D. The breadth of Shamir's secret－sharing scheme[J]. Computer and Security, 1994, 13(1): 69－78.

[4] van DIJK M . On the information rate of perfect secret sharing schemes[J]. Designs, Codes and Cryptography, 1995, 6(2): 143－169.

[5] CHANG C C, HUANG R J. Sharing secret images using shadow codebooks[J]. Information Sciences, 1998, 111(1/2/3/4): 335－345.

[6] THIEN C C, LIN J C. Secret image sharing [J]. Computers & Graphics, 2002, 26(5): 765－770.

[7] NAOR M, SHAMIR A. Visual cryptography[C]// Proceedings of Eurocrypt '94. Berlin: Springer-Verlag, 1995: 1－12.

[8] ITO R, KUWAKADO H, TANAKA H. Image size invariant visual cryptography[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 1999, E82－A(10): 2172－2177.

[9] HOU Y C, LIN C F, CHANG C Y. Visual cryptography for color images without pixel expansion[J]. Journal of Technology, 2001, 16(4): 595－603.

[10] HOU Y C. Visual cryptography for color images[J]. Pattern Recognition, 2003, 36(7): 1619－1629.

[11] HOU YONGCHANG , DU SHUFEN . Visual cryptography techniques for color images without pixel expansion[J]. Journal of Information, Technology and Society, 2004, 109(1): 95－110.

[12] ZHOU Z, ARCE G R, CRESCENZO G D. Halftone visual cryptography[J]. IEEE Transactions on Image Processing, 2006, 15(8): 2441－2453.

[13] HOU YONGCHANG, LIN FANGZHU, ZHANG ZHAOYUAN. A new approach on 256 color secret image sharing technique[J]. MIS Review, 2000(9): 89－105.

[14] 苏中民,林行良.图视秘密的任意分存[J].计算机学报,1996,19(4): 293－299.

[15] ATENIESE G, BLUNDO C, de SANTIS A, *et al*. Constructions and bounds for visual cryptography[C]// ICALP'96: Proceedings of the 23rd International Colloquium on Automata, Languages and Programming, LNCS 1099. Berlin: Springer-Verlag, 1996: 416－428.

[16] ATENIESE G, BLUNDO C, de SANTIS A, *et al*. Visual cryptography for general access structures[J]. Information and Computation, 1996, 192(2): 86－106.

[17] ATENIESE G, BLUNDO C, de SANTIS A, *et al*. Extended capabilities for visual cryptography[J]. Theoretical Computer Science, 2001, 250(1/2): 143－161.

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

[19] BLUNDO C, de SANTIS A. Visual cryptography schemes with perfect reconstruction of black pixels [J]. Computer & Graphics,

1998, 12(4): 449 - 455.
[20] BLUNDO C, de SANTIS A, NAOR M. Visual cryptography for grey level images[J]. Information Processing Letters, 2000, 75(6): 255 - 259.
[21] WANG DAOSHUN, ZHANG LEI, MA NING, *et al.* Two secret sharing schemes based on Boolean operations[J]. Pattern Recognition, 2007, 40(10): 277 - 278.
[22] SHYU S J. Efficient visual secret sharing scheme for color images[J]. Pattern Recognition, 2006, 39(5): 866 - 880.
[23] CIMATO S, de PRISCO R, de SANTIS A. Probabilistic visual cryptography schemes[J]. The Computer Journal, 2006, 49(1): 97 - 107.
[24] YANG C-N. New visual secret sharing schemes using probabilistic method[J]. Pattern Recognition Letters, 2004, 25(4): 481 - 494.
[25] TSAI C-S, CHANG C-C. A generalized secret image sharing and recovery scheme[C]// Proceedings of the 2nd IEEE Pacific Rim Conference on Multimedia, LNCS 2195. Berlin: Springer-Verlag, 2001: 963 - 968.
[26] LIN T. An image-sharing method with user-friendly shadow images[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(12): 1161 - 1169.
[27] WU Y-S, THIEN C-C, LIN J-C. Sharing and hiding secret images with size constraint[J]. Pattern Recognition, 2004, 37(7): 1377 - 1385.
[28] CHANG C-C, LIN C-C, LIN C-H, *et al.* A novel secret image sharing scheme in color images using small shadow images[J]. Information Sciences: an International Journal, 2008, 178(11): 2433 - 2447.
[29] TSAI C-S, CHANG C-C, CHEN T-S. Sharing multiple secrets in digital images[J]. Journal of Systems and Software, 2002, 64(2): 163 - 170.
[30] FENG J-B, WU H-C, TSAI C-S, *et al.* A new multi-secret images sharing scheme using Largrange's interpolation[J]. Journal of Systems and Software, 2005, 76(3): 327 - 339.
[31] WANG R-Z, SU C-H. Secret image sharing with smaller shadow images[J]. Pattern Recognition, 2006, 27(6): 551 - 555.
[32] ALVAREZ G, ENCINAS A A, ENCINAS L H, *et al.* A secure scheme to share secret color images[J]. Computer Physics Communications, 2005, 173(1/2): 9 - 16.
[33] THIEN C-C, FANG W-P, LIN J-C. Sharing secret images by using base-transform and small-size host images[J]. International Journal of Computer Science and Network Security, 2006, 6(6): 219 - 225.
[34] MASSEY J L. Minimal codewords and secret sharing[C]// Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory. Piscataway, NJ: IEEE Press, 1993: 276 - 279.
[35] BLAKLEY G R, KABATIANSKI G A. Ideal perfect threshold schemes and MDS codes[C]// ISIT'95: Proceedings of IEEE International Symposium on Information Theory. Piscataway, NJ: IEEE Press, 1995: 488.
[36] McELIECE R J, SARWATE D V. On sharing secrets and Reed-Solomon codes[J]. Communications of the ACM, 1981, 24(9): 583 - 584.
[37] MacWILLIAMS F J, SLOANE N J A. The theory of error-correcting code[M]. New York: North-Holland Publishing Company, 1977.
[38] LIN S, COSTELLO D. Error control coding[M]. Englewood Cliffs, NJ: Prentice-Hall, 1983.
[39] HOHOLDT T, van LINT J H, PELLIKAAN R, *et al.* Algebraic geometric codes[J]. IEEE Transactions on Information Theory, 1998, 44(6).
[40] WU H-C, WANG H-C, YU R-W. Color visual cryptography scheme using meaningful shares[C]// ISDA'08: Proceedings of the 8th International Conference on Intelligent Systems Design and Applications. Piscataway, NJ: IEEE Press, 2008: 173 - 178.
[41] CHANG C-C, LIN I-C. A new (t, n) threshold image hiding scheme for sharing a secret color image[C]// ICCT 2003: International Conference on Communication Technology Proceedings. Piscataway, NJ: IEEE Press, 2003: 196 - 202.
[42] KATZENBEISSER S, PETITCOLAS F. Information hiding techniques for steganography and digital watermarking[M]. London: Artech House, Inc., 2009.
[43] CHANG C C, LIN M H, HU Y C. A fast and secure image hiding scheme based on LSB substitution[J]. International Journal of Pattern Recognition and Artificial Intelligence, 2002, 16(4): 399 - 416.
[44] ZHOU W, BOVIK A C, SHEIKH H R, *et al.* Image quality assessment: From error visibility to structural similarity[J]. IEEE Transactions on Image Processing, 2004, 13(4): 600 - 612.
[45] RUDOLF L, HARALD N. Finite fields[M]. 2nd ed. Cambridge: Cambridge University Press, 1997.
[46] SHEIKH H R, BOVIK A C. Image information and visual quality[J]. IEEE Transactions on Image Processing, 2006, 15(2): 430 - 444.
[47] BOSE R. Information theory, coding and cryptography[M]. Singapore: McGraw-Hill, 2003.
[48] 郝柏林. 从抛物线谈起: 混沌动力学引论[M]. 上海: 上海科技出版社, 1993.

(上接第 657 页)

[4] CHEN Y L, CHENG L C. A novel collaborative filtering approach for recommending ranked items[J]. Expert Systems with Applications, 2008, 34(4): 2396 - 2405.
[5] 洪文兴, 翁洋, 朱顺痣. 垂直电子商务网站的混合型推荐系统[J]. 系统工程理论与实践, 2010, 30(5): 928 - 935.
[6] LI J, XU Y, WANG Y F, *et al.* Strongest association rules mining for efficient applications[C]// Proceedings of the Fourth IEEE Conference on Service Systems and Service Management. Piscataway, NJ: IEEE Press, 2007: 502 - 507.
[7] 李杰, 徐勇, 王云峰, 等. 面向个性化推荐的强关联规则挖掘[J]. 系统工程理论与实践, 2009, 29(8): 144 - 152.
[8] 刘建国, 周涛, 汪秉宏. 个性化推荐系统的研究进展[J]. 自然科学进展, 2009, 19(1): 1 - 15.
[9] WAND J C, CHIU C C. Recommending trusted online auction sellers using social network analysis[J]. Expert Systems with Applications, 2008, 34(3): 1666 - 1679.
[10] ZHOU T, REN J, MEDO M, *et al.* Bipartite network projection and personal recommendation[J]. Physical Review E, 2007, 76(4): 6116 - 6123.
[11] NEWMAN M E J. The structure and function of complex networks[J]. SIAM Review, 2003, 45(2): 167 - 256.
[12] HOLME P, LILJEROS F, EDLING CR, *et al.* Network bipartivity[J]. Physical Review E, 2003, 68(5): 6108 - 6119.
[13] LILJEROS F, EDLING C R, AMARAL L A N, *et al.* The Web of human sexual contacts[J]. Nature, 2001, 411(6840): 907 - 908.
[14] LILJEROS F, EDLING C R, AMARAL L A N. Sexual networks: Implications for the transmission of sexually transmitted infections[J]. Microbes and Infection, 2003, 5(2): 189 - 196.
[15] JEONG H, TOMBOR B, ALBERT R, *et al.* The large-scale organization of metabolic networks[J]. Nature, 2001, 407(6804): 651 - 654.