文章编号：2095-2163(2021)02-0109-05 中图分类号：TP309.7 文献标志码：A

视觉密码方案概述

冯 琪，王洪君
（吉林师范大学 计算机学院，吉林 四平 136000）

摘 要：视觉密码（VC）是一种用于分享秘密图像的加密方案，与传统的密码技术相比具有简单性、安全性、隐蔽性等优点。其加密是将图像编码为分享，将分享打印在透明胶片上或以数字形式存储；其解密过程是对分享进行叠加，然后通过人类的视觉能力来实现。本文介绍了视觉密码的基本概念和各种不同的视觉密码方案，以及每种方案中使用的技术。此外，对视觉密码在不同领域上的应用做出了说明。

关键词：视觉密码；分享图像；秘密图像

Overview of visual cryptography scheme

FENG Qi, WANG Hongjun
(College of Computer, Jilin Normal University, Siping Jilin 136000, China)

【Abstract】Visual cryptography (VC) is an encryption scheme for sharing secret images. Compared with traditional cryptography, it has the advantages of simplicity, security and concealment. The encryption is to encode the image for sharing, and to print the sharing on a transparent film or store it in digital form; the decryption process is to superimpose the sharing, and then realize it through human visual ability. This article introduces the basic concepts of visual cryptography and various different visual cryptography schemes, as well as the technology used in each scheme. In addition, the application of visual cryptography in different fields is explained.

【Key words】visual cryptography; shared image; secret image

0 引 言

视觉密码由 Naor 和 Shamir 在 1994 年首次提出，是一种依靠人眼解密的秘密分享方法，也是一种简单、安全、有效的加密方案。总地来说，是将一个秘密图像分割成多个分享，不需要任何密码学的计算，仅凭人眼就可以通过分享获得原来的秘密图像，十分简单。具体工作方式如下：选择一个秘密图像，将图像加密为 n 个片段（称为分享）。当这些分享被打印到透明胶片上并堆叠在一起时（物理上叠加），人眼就可以解密。只有拥有至少 k 个分享的人才能解密图片，而任何少于 k 个分享均不会暴露任何关于秘密图像的信息。

本文研究内容安排如下：第一部分概述了基础视觉密码方案，其中包括(2,2)视觉密码方案、(k, n)视觉密码方案、灰度图像的视觉密码方案、半色调视觉密码方案、彩色视觉密码方案、多秘密分享视觉密码方案、区域递增视觉密码方案和可防欺骗视觉密码方案。第二部分阐述了视觉密码的各种应用。第三部分给出了结论和未来的工作。

1 基础视觉密码方案

1.1 (2,2)视觉密码方案

在(2,2)视觉密码方案[1]中，从原始图像生成 2 个分享，实现方法如图 1 所示。图 1 中的黑像素和白像素都是秘密图像像素，对于秘密图像中的每一个像素 p 都被分成 2 个子像素。参见图 1，如果像素 p 是白色，随机选择图 1 的左侧两行之一；如果像素 p 是黑色，随机选择右侧两行之一。如此一来，像素 p 被加密为图 1 中的 2 个子像素。在每种情况下，选择都是随机执行的，因此每一列都有 50% 的概率被选择。接下来，将所选列中的前两对子像素分别分配给分享 1 和分享 2。由于 p 被加密为一对子像素对，所以单个分享不会提供有关秘密图像的任何线索，只有一个分享的任何人都无法透露任何秘密信息。图 1 的最后一行展示了堆叠 2 个分享的结果，如果 p 为白色，则无论加密期间选择了子像素对的哪一列，叠加结果始终是一个黑色和一个白色子像素。如果 p 为黑色，则叠加结果为 2 个黑色子像素。因此，在重建图像中存在对比度损失。但是，

作者简介：冯 琪(1998-)，女，硕士研究生，主要研究方向：信息安全、密码学、视觉密码。
通讯作者：王洪君 Email：jlnuwhj@ sina. com

收稿日期：2020-11-18

由于人类视觉系统将其各自的黑白组合取平均值，因此解密后的图像对于肉眼是可见的。(2,2)视觉密码方案的实验结果见图 2。

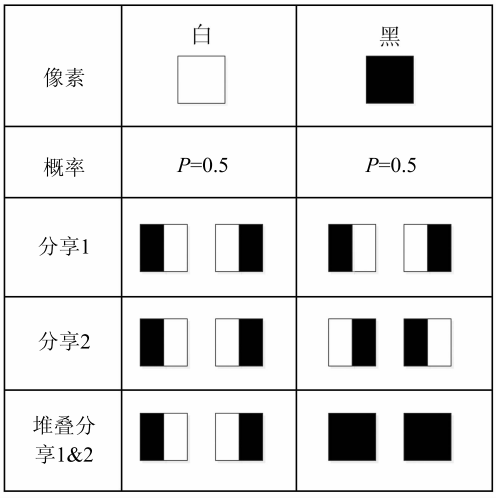
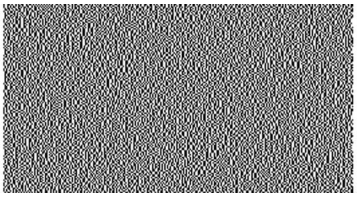


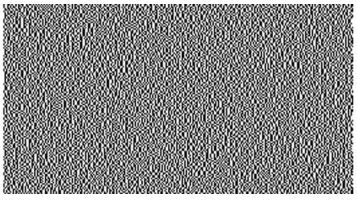
图 1 一种(2,2)视觉密码方案的实现方法

Fig. 1 A (2,2) realization method of visual cipher scheme



(a)分享图像 1

(a) Share image 1



(b)分享图像 2

(b) Share image 2

(c)恢复图像

(c) Recovery image

图 2 (2,2)视觉密码方案的实验结果

Fig. 2 Experimental results of the(2,2) visual encryption scheme

视觉密码方案中的重要参数是像素扩展(m)、对比度(α)和恢复图像的大小(r)。其中，像素扩展 m 用于加密秘密图像像素分享中的像素数量，越小越好。对比度 α 是重建图像中黑白像素之间汉明权重的相对差，这意味着重建图像的质量，研究中希望该值要尽可能地大。

1.2 (k,n)视觉密码方案

(k,n)视觉密码方案[2]是在(2,2)视觉密码方案上的延伸。在(2,2)视觉密码方案中，要恢复秘密图像即需将 2 个分享堆叠。对于(k,n)视觉密码方案来说，任何 k 个或更多数量分享都可以通过将其打印在透明胶片上并堆叠在一起来恢复秘密图像，任何 $k-1$ 个或更少份分享都不会提供秘密图像的信息。这样处理就具有了一定的灵活性，即使用户丢失了一些分享，只要获得的分享数量不少于 k，就仍然可以恢复秘密图像。

郭松鸽等人[3]提出了基于异或解密的(k,n)视觉密码方案，利用异或的自反性改进加密方式，不需要设计加密矩阵。该方案有 2 种解密方法：当没有计算设备时，使用传统的叠加解密，解密过程简单；当有计算设备时，使用异或解密，需少量计算，但具有更好的视觉质量，并且当所有分享份都参与异或解密时，可以无损恢复秘密图像。

1.3 灰度图像的视觉密码方案

以前在视觉密码方案上的工作仅限于二进制图像，Lin 等人[4]提出了一种通过抖动技术对灰度图像进行加密的方法。不是直接使用灰度子像素，而是使用抖动技术将灰度图像转换为近似二进制图像，在此基础上进行后续操作。通过引入空间填充曲线有序抖动技术将灰度图像转换为近似的二进制图像，再使用传统的视觉密码方法对灰度图像进行加密解密。郁滨等人[5]提出了基于快速响应码(一种二值的机器可识读符号图像)的灰度视觉密码方案，在像素不扩展的同时能够抵抗一般攻击。根据 QR 码模块识别单元的结构建立灰度值与二值系列模板之间的映射关系，设计不同的视觉密码分享矩阵集合，对秘密图像进行分享。

1.4 半色调视觉密码方案

Zhou 等人[6]提出了半色调视觉密码术，用于创建有意义的图像分享技术，有意义的图像分享可以减少攻击者对加密数据的怀疑。在半色调视觉密码方案中，秘密像素 p 被编码为 $Q_1 \times Q_2$ 的数组，称为半色调单元。通过使用具有适当大小的半色调单元，可以获得视觉上良好的半色调分享，同时也能保持对比性和安全性。Al-Khalid 等人[7]在 Hou、Saraireh 等学者基础上提出了一种基于视觉密码的彩色图像分享方法，加密过程是通过私钥生成与彩色秘密图像大小相同的 2 个分享(随机分享和密钥

分享）来加密半色调彩色图像；解密过程是在接收端将 2 个分享堆叠在一起来显示秘密彩色图像。此方案修改了生成随机和密钥分享的加密技术，使用发送方和接收方都知道的私钥生成随机分享，使用随机分享和半色调图像的层构造密钥分享的层，具有更高的安全级别、更少的存储空间、更少的计算时间以及更好的 *PSNR* 值。

1.5　彩色视觉密码方案

视觉密码方案在以前只应用于黑白图像。Verheul 等人[8]提出了第一个彩色视觉密码方案，将具有 c 种颜色的秘密图像分解成 n 个分享，k 个分享叠加即可恢复秘密图像。该方案工作原理类似于基本视觉密码方案，因此解密方法相同，其局限性在于像素扩展大，恢复的秘密图像质量下降。此后出现的另一种处理方法[9]是使用分开的 3 个颜色通道。红色、绿色、蓝色用于加性模型，青色、品红色、黄色用于减性模型，再将常规的视觉密码方案应用于每个通道。这种方法减少了像素扩展，但是图像的质量由于半色调处理而降低。张先环等人[10]提出了基于异或的完全恢复 $(2,n)$ 彩色视觉密码方案。该方案以构造行向量为基础，每个参与者携带一个分享，2 个分享异或即可完成秘密图像的恢复。这一方案降低了分享的管理难度，实现秘密图像完全恢复的同时降低了计算复杂度。

1.6　多秘密分享视觉密码方案

1.6.1　基础多秘密分享视觉密码方案

前文讨论的方案仅涉及一个秘密的分享，因此有研究者尝试如何隐藏多个秘密。多个秘密分享的主要优点是能够在一组分享中隐藏多个秘密。Wu 等人[11]最初研究了多重秘密分享问题，在 2 组分享 S_1 和 S_2 中隐藏了 2 个秘密。当 S_1 和 S_2 叠加时，能够恢复第一个秘密；当 S_1 逆时针旋转 90°后和 S_2 叠加时，能够恢复第二个秘密。这个方案最多只能分享 2 个秘密，除此以外，恢复秘密的角度限制为 90°、180°或 270°。经过深入研究，通过设计圆形分享，进一步发展了多重秘密分享，解决了角度的限制问题，当 S_1 叠加在 S_2 上并沿顺时针方向旋转 0° ~ 360°之间的某个角度时，就可以恢复秘密图像。后来研究者们引入其他方法进行多秘密分享，付正欣等人[12]针对信息损失的问题，在构造具有上下门限值的单门限视觉密码方案基础上，设计了旋转规则融合算法和区域合并算法，提出了完全恢复的多门限多秘密视觉密码方案，秘密图像实现完全恢复。

1.6.2　彩色多秘密分享视觉密码方案

Weir 等人[13]提出了允许使用有意义的彩色图像隐藏较小分享集方案，在真实的自然图像中隐藏彩色图像。此方案将加密产生的一部分分享嵌入到自然彩色图像中，另一部分分享作为公共密钥，还提出可以将分享隐藏到半色调图像中，有助于消除攻击者对加密的怀疑。何文才等人[14]提出了一种无损恢复的多级别视觉密码方案，该方案基于随机栅格理论和异或运算对多个级别的秘密图像进行处理，对各个级别的分享进行异或即可依次恢复所有级别的秘密图像。过程如下：对各级秘密图像均为大小相等的彩色图像，先采用 RGB 三基色原理将彩色秘密图像分解成红、绿、蓝三张分量图像 R、G、B，将其看作 3 张灰度子秘密图像，再将这 3 张图像分别生成分存图像，将位置相对应的 3 张图像进行合成，得到最后的 n 张彩色分享图像。秘密图像恢复需要先进行纠错解码，再将每个分享图像进行三基色分离，将所有分享图像的红、绿、蓝分量图像分别进行异或得到秘密图像的 3 张分量图像，最后进行三基色合成，即可恢复彩色秘密图像。恢复图像与秘密图像相比无失真且能满足安全性要求。

1.7　区域递增视觉密码方案

传统的视觉密码方案里，将一个完整的图像视为一个秘密，并且对这个完整图像的所有像素应用同一个加密规则。Wang[15]开发了一种区域递增视觉密码方案，用于在单个图像中分享多个保密级别的视觉秘密。在提出的区域递增视觉密码方案中，可以将秘密图像的内容指定到多个区域，其中每个区域都有自己的保密属性，每个生成的分享都具有类似噪声的外观。该方案特点是可以恢复的秘密数量与参与恢复过程的参与者数量成正比。

胡浩等人[16]提出一种基于异或运算的区域递增式视觉密码方案，设计自适应区域分配算法，优化性能参数。构造加密矩阵，以 (n, n)-*VCS* 为基本单位，最后将矩阵拼接输出。该方案适用于通用存取结构，可有效地减少分享份的存储和传输开销；像素不扩展，恢复图像不失真，白像素可以实现完全恢复；提高相对差，显著地改善了恢复图像的视觉效果。

1.8　可防欺骗视觉密码方案

尽管视觉密码具有安全性，但却跟普通秘密分享方案一样，存在欺骗问题。大多数视觉密码方案在构建时都是假设参与者诚实可信，恢复秘密时不会进行欺骗，但实际上参与者并非都诚实可信，可能会伪造分享来欺骗其他参与者，此外攻击者也可能

会冒充合法参与者以此破坏或骗取秘密信息。研究人员已经提出了许多防止欺骗的方法,比如 Liu 等人[17]提出了 2 种防欺骗算法。第一种算法可以从参与秘密恢复的 m 个用户中识别欺骗者;第二种算法参与用户可以与不参与秘密恢复的 $n-m$ 个用户合作,能够实现更好的识别欺骗者。

张逸凡等人[18]在 Liu 等人[17]方案基础上提出了可防内部欺骗的异步多秘密分享方案。利用二元多项式,为任意 2 个参与者提供会话密钥,防止攻击者窃取参与者信息;结合离散对数问题,在秘密重构阶段增加了检测内部欺骗的过程,能够检测出参与者在此阶段的内部欺骗行为;改变秘密的设置方法和参与者份额的分配方法,使方案具有异步性和灵活性。

2 视觉密码的各种应用

2.1 水印

水印是一种保护数字媒体版权的技术,将一些标识信息直接嵌入数字载体的同时不会影响原载体的使用价值,也不容易被发现,通过水印可以传送隐秘信息,也可以防伪。水印技术与视觉密码结合,处理过程包括 2 个步骤:水印嵌入和水印检索。研究者提出了许多具有不同方法的视觉密码水印方案。李春艳[19]首先对二值水印图像进行置乱,去除图像的像素相关性,并在像素不扩展的(2,2)视觉密码矩阵基础上部分修改载体图像的最不重要位,提取水印时通过比较最不重要位的取值即可得到水印信息。

2.2 身份认证

身份认证是一种重要的网络安全手段,既有访问控制,又有安全防护的作用。研究者将视觉密码应用在身份认证中,由于视觉密码自身特点,在实现安全性的同时,解密花费比较小,对使用者的密码知识水平要求也不高。樊攀星等人[20]将视觉密码技术应用到交互式的认证方案中,设计了一个交互式的挑战-响应方案。方案中用户 A、B 都使用随机算法生成一幅黑白二值图像,再经过一系列叠加或是异或操作互相确定对方身份。利用视觉密码具有伪随机数的特性,保证身份认证会话不被重用,在不使用复杂传统密码算法的前提下,提高了身份认证的便捷性和安全性。

2.3 证件防伪

各种证件的防伪,如票据等同样十分重要。传统防伪手段实现起来成本较高,于是研究者将视觉密码引入其中。骆骁[21]将证件中的重要信息编码生成 QR 码,再将 QR 码携带秘密信息的部分进行视觉密码分享,最后将分享份印刷在证件的四周,极大地减少了成本。

2.4 反网络钓鱼系统

诸如安全别针、借记卡信用卡号和密码之类的凭据信息是至关重要的信息,并且可能被攻击者窃取。网络钓鱼被广泛用于窃取秘密证书,为了避免网络钓鱼攻击,可以应用视觉密码技术,以确保用户在使用任何网站时的安全性。通过强加 2 个分享,其中一个分享是从服务器站点接收的,另一个分享是用户自己的分享,用户可以确保网站不被网络钓鱼。Abinaya 等人[22]提出了使用视觉密码的反网络钓鱼图像验证码验证方案,将原始图像验证码分解为存储在单独数据库服务器中的 2 个分享,动态生成验证码图像以保护图像验证码的私密性,这样只有当 2 个图像同时可用时才可以显示原始图像验证码,一旦原始图像验证码向用户显示,就可以用作密码。

3 结束语

本文对各种不同类型的视觉密码方案进行了概述,主要集中在加密的使用上,解密不需要计算,只要叠加分享份就能恢复秘密图像,人眼即可获得信息。对于视觉密码,希望在保持安全性的同时更好地恢复秘密图像,除此之外还有存储空间,计算复杂性等问题,可以进行进一步的工作来增强视觉密码机制,以提高信息的安全性。视觉密码在身份认证、证件防伪等方面已经有了许多成果,未来有可能适用于更广泛的安全应用领域,与更多处理技术结合使用。

参考文献

[1] NAOR M, SHAMIR A. Visual cryptography [C]//Proceedings of the Advances in Cryptalogy - Eurocrypt'94, Lecture Notes in Computer Science. Berlin: Springer-Verlag, 1995,950:1-12.

[2] 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 & Systems for Video Technology, 2012, 22(5):799-810.

[3] 郭松鸽,吕东辉,戴玉静,等. 基于异或解密的 (k,n) 视觉密码方案[J]. 上海大学学报(自然科学版),2020,26(1):21-32.

[4] LIN C C, TSAI W H. Visual cryptography for gray-level images by dithering techniques[J]. Pattern Recognition Letters, 2003, 24(1-3):349-358.

(下转第 118 页)