应用密码学论文——视觉密码（Visual Cryptography）

刘曼姝 1901210656 王淳颖 1901210680 李鼎 1901210421

2019.12.25

视觉密码是密码学中比较新的一个研究方向，在近年来形成了一个新的研究热点。本文简要介绍了视觉密码的研究背景及优势，综述了各类视觉密码方案，并介绍了一些视觉密码方案的应用场景实例。

1. 研究背景

视觉密码（Visual Cryptography，VC）最初由 Naor 和 Shamir[1]于 1994 年在欧洲密码学年会上提出，并于 1995 年在《Lecture Notes in Computer Science》上发表，它将秘密共享与数字图像相结合；在 2011 年，CRC 公司也出版了第一部有关视觉密码的专著《Visual Cryptography and Secret Image Sharing》。

视觉密码方案基于秘密共享。秘密共享将一个秘密 S 分解成 n 份，共享秘密 S 的群体的每个人都有一个共享份（share），其中任何 k（k≤n，对于普通秘密共享 k=n，对于门限秘密共享 k<n）个人可以重建秘密，但是少于 k 个人的群体则不能重建秘密，这称为(k, n)-秘密共享方案，它提供了一种在多个人之间共享秘密的方法。

视觉密码的秘密分享算法是：将秘密图像按照像素点编码到若干共享份的图像中，其中，黑白像素点的分布是随机的，从中得不到有关秘密图像的任何信息；其秘密恢复算法是：只需将一定数目共享份进行叠加（打印在透明胶片上等），人的视觉系统就可直接辨认出秘密信息。与其他加密方法相比，视觉密码加密的计算成本非常低，解密方法甚至不需要任何计算，因为它仅取决于人类的视觉。

由于图像蕴含丰富的信息量，且视觉密码具有理论安全性和秘密恢复简单性等优势，其具有非常广阔的应用前景。因为视觉密码是基于秘密共享提出的，故其可广泛地应用于需要群体参与的领域，如安全多方计算、口令分存等场景；还常用于身份认证、隐式通信、数字水印等场景；并且，因为视觉密码的使用简单，其还可在缺乏计算设备的特殊情况下提供应急方案。

2. 视觉密码方案

在视觉密码发展的 25 年中，有许多学者提出了有关视觉密码的方案。本部分将介绍 Naor 和 Shamir 的经典方案、对其改进的方案和一些新的方案。

2.1 Naor 和 Shamir 的经典方案

以（2, 2）-视觉密码秘密共享方案为例[2]：

2.1.1 准备原始图像

为了构建共享图像，需要准备一个原始图像，如图 2-1 所示，它包括秘密消息“0129”，对于当时 Naor 和 Shamir 提出的基础视觉密码，它需要由白色背景和黑色字母、数字或符号组成。

图 2-1 原始图像

2.1.2 准备图案和构造方法

为了进行加密，需要准备一些图案。这些图案由两个 2x2 阵列中的 4 个子像素组成，4

个子像素的一半用黑色填充，其余为透明，可以制作水平、垂直和对角线 6 种图案，视觉密码将原始图像的每个像素转换为其中之一。在共享图像中，构造背景像素和消息像素的方法不同，需要根据要转换的是原始图像中的背景像素还是消息像素，寻找相应的构造方法。图案是根据编号，由其中一种形式随机确定的，如图 2-2 所示。

pattern no	Background Pixel					Message Pixel				
1		+		=			+		=	
2		+		=			+		=	
3		+		=			+		=	
4		+		=			+		=	
5		+		=			+		=	
6		+		=			+		=	

图 2-2 背景像素和消息像素的 6 种图案对照

2.1.3 转换

如果要将原始图像中位置为(x, y)的像素转换为序号为 no: k 的图案，则在第一个共享图像中，(x, y)位置的像素应变为 no: k 对应的图案。当转换的是背景像素时，在第二个共享图像中，(x, y)位置的像素应与第一个共享图像中相同；当转换的是消息像素时，在第二个共享图像中，(x, y)位置的像素设为该图案对于全黑色像素的“补集”，从而正确共享两个图像。

为每一个像素的加密规则构建一个 n×m 的布尔矩阵 $B=(B_{ij})_{n\times m}$，其中，$B_{ij}=0$ 表示第 i 个分享者的第 j 个子像素的颜色为白色；$B_{ij}=1$ 表示第 i 个分享者的第 j 个子像素颜色为黑色。将矩阵中第 j 列的所有元素作“或”运算，得到的结果是重叠后分享图像中第 j 个子像素的颜色。依次处理完秘密图像的所有像素，就可以得到 n 幅分享图像。重叠后图像的灰度值与进行或运算之后的向量 V 的汉明重量 H(V)成正比。参与者利用视觉系统解释灰度值如下：如果 $H(V)\geq t$，则该点像素颜色为黑色，如果 $H(V)\leq t-\alpha m$，则该点像素颜色为白色。其中，t 为门限值，指解密之后图像中的像素被人眼解析为黑色与白色的灰度临界值；像素扩展度 m 指在分享图像中用来表示原像素的子像素的个数，代表原始图片在面积上的失真；而对比度 α 衡量了重构图像中黑像素与白像素的差异，指解密之后图片中原始黑白像素对应的灰度差值同扩展度的比值，代表的是原始图片在黑白两色对比上的失真。因此，当解密之后图像中像素的灰度值大于或等于 t 时，该像素被人眼解析为黑色；相应地，当像素的灰度值小于 $t-\alpha m$ 时，该像素被人眼被解析为白色。

2.1.4 结果

如图 2-3 所示，从视觉上来看，两个共享图像是灰色的且比较相似，而且黑色像素和透明像素是随机混合的，故两个共享图像都不会泄露秘密，也不会显示任何构建共享图像的规则。仅当两个共享图像堆叠在一起时，人的视觉才能确认消息；如果两个图像之一失真，则无法查看消息。其利用了字符比背景拥有更高的对比度，因此，视觉密码不需要任何解密处理。

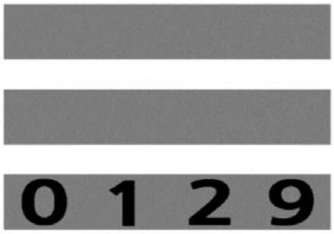

图 2-3 共享图像和秘密图像的恢复

2.1.5 存在的问题

I） 加密图像类型受限：该方案仅能针对二值图像即黑白图像进行加密，而在实际生活中，需要加密的图片多种多样，包括灰度图像和彩色图像，难于满足加密需求。

II） 共享图像无意义：Naor 和 Shamir 的视觉密码经典方案会产生无意义的共享图像，这会给参与许多秘密共享项目的人带来管理问题，因为他们必须跟踪许多不同但相似的无意义共享图像；此外，无意义图像的传输可能引起外界的怀疑，外界可能会意识到该图像可能带有某种类型的秘密消息，从而增强他们揭露秘密图像的愿望、降低了秘密图像的安全性[3]。

III）像素扩张导致对比度下降：由于在上述视觉密码方案中，将原图像中的每个像素点扩展为多个子像素点，故恢复得到的图像存在着像素扩张与对比度下降严重的问题，使得该图像与原图像在大小、长宽比例和分辨率等方面具有明显的差异，甚至可能出现失真。

2.2 改进的方案

为了解决 Naor 和 Shamir 的视觉密码经典方案存在的问题，已有许多研究者对其进行了改进或提出了新方案。

2.2.1 针对加密图像类型受限的改进方案

2003 年，Y. C. Hou[4]等基于对黑白视觉密码、半色调技术和颜色分解方法的以往研究，提出了三种用于灰度和彩色图像的视觉密码的方法，其对于先前的黑白视觉密码技术具有向后兼容性；其后又提出门限视觉密码方案也可以应用于灰度和彩色图像，其具有容错能力，即使在信道故障、存储设备崩溃或者被黑客破坏而导致共享图像之一生成出现延迟的情况下，仍然可以显示秘密图像，因为在门限方案中，彩色秘密图像将被分成 n 份，但是收集 n 份中的任何 k 份（k<n）即可恢复秘密图像。

2015 年，M.Karolin[5]等则进一步从 8 色 RGB 的彩色图像视觉密码方案扩展到 256 色的彩色图像视觉密码方案，提出了基于 Floyd-Steinberg 抖动算法将 256 色图像转换为 16 种标准 RGB 颜色格式的方法，然后可采用(2, 2)-基于 XOR 的视觉密码方案在不影响分辨率的情况下生成共享份，尽管所提出的方法将 256 色图像转换为 16 色代码格式以进行共享图像创建，但仍保持了原始图像的强度。

2.2.2 针对共享图像无意义的改进方案

早期针对共享图像无意义的改进方案应用了隐写术、半色调和颜色合成/分解技术等像素扩张方法[3]，其目的主要是生成有意义的共享图像，从而消除外界对图像藏有秘密消息的怀疑，增强秘密图像的安全性和管理的方便性，其中，有意义的图像部分称为“封面（cover）图像”。

隐写术是一种将信息、图像或文件隐藏于其他图像或文件中的技巧。隐写术最大的优点在于，只要有效荷载不被计算机检查者用于检查数据，就只有发送隐藏数据的人和接收数据的人知情，且对于其他人来说，包含隐藏数据的对象看起来就像是日常的普通对象。隐写术中的图像隐写将原始图像分成几个块，然后为像素二进制值的每个块创建图层成为矩阵，接下来在这些层的行和列中搜索，并试图在要隐藏的像素和原始图像二进制层的行列值之间找到最接近的匹配，将秘密像素隐藏在那里。

2015 年，Jainthi.k[6]等使用了一种新的 k-扩展视觉加密方案（EVCS）。在半色调视觉密码中，通过 Floyd-steinberg 的误差扩散算法将秘密图像编码为 k 个半色调有意义的图像共享份。同年，Hou[3]等提出了一种更加友好的视觉密码新方案，秘密被隐藏在两个有意义的图像部分中。共享图像是由秘密图像中的一些像素和封面图像中的一些像素生成的，每个 2×2 图像块可能包含 0~4 个黑色像素，因此它可以显示 16 种不同的图像模式，将黑色像素视为 1、白色像素视为 0，将图像图案对应到相应的二进制/十进制编码，并根据每个块中的黑色像素数将这些模式分为 5 个不同的集合；然后需要对封面图像的像素进行加密，使黑色区域变暗、白色区域变亮，以突出显示封面图像的内容。在不公开有关秘密图像的任何线索的情

况下，只能在共享图像上识别封面图像的内容，但是当它们堆叠在一起时，只有加密的秘密映像才会显示出来，而封面图像的内容将消失。研究人员提出了几个命名为(a, b)/(c, d)的模型，其中，a 个黑色像素代表共享图像上的黑色块、b 个黑色像素代表共享图像上的白色块、c 个黑色像素代表堆叠图像上的黑色块、d 个黑色像素代表堆叠图像上的白色块，在所有方案中，(4, 2)/(4, 2)是最好的设计，其共享图像和堆叠图像的对比度都可以达到 50%，将清楚地显示封面图像和秘密图像的内容，也一定程度上解决了经典方案对比度下降的问题。

2.2.3 针对像素扩张导致对比度下降的改进方案

2013 年，王欢[7]提出了一个基于异或操作的针对灰度图像的（n, n）-秘密共享方案（参与者数量为 n）。该方案构建一个二进制矩阵用来存储图像中每一像素点的灰度值，并构建一个加密矩阵用来存储 2n 个加密项。为二进制矩阵中每一比特二进制数产生随机数，并根据随机数来选取相应的加密项对其加密，从而得到 n 幅分享图像，分发给 n 个参与者分别保存。这 n 幅分享图像的大小均与原图像相同，不存在像素扩张，且具有较高的对比度。而随机数可看作一个随机密钥，用其确定加密项则类似于密码学中一次一密的理想加密方案，与此同时，也实现了对灰度图像的操作与处理。L M Varalakshmi[8]等提出了一种用于彩色图像的视觉加密技术，以减少解密图像的失真，该技术使用视觉信息像素（VIP）同步和抖动泛滥的错误扩散技术，与其他抖动技术相比，解密图像的质量有了改善，性能也有了提高。

3. 视觉密码方案的应用

视觉密码的应用场景十分丰富，本部分展开介绍近年来视觉密码方案在用户身份验证、隐式通信、数字水印等方面的应用。

3.1 用户身份验证

2017 年，Yang D[2]等为改进用户身份验证方法，提出了使用视觉加密（VC）——基于图像的增强型密码处理方案。并开发了相应的应用程序，用于互联网上用户和服务器之间的通信，用户部分的设备使用 Android 4.0，服务器部分的设备使用 Window7。

与基于哈希和文本的传统方案不同，其方案将文本类型的用户 ID 转换为通过视觉加密处理的两个图像。在客户端，用户使用带有个人信息的种子（SEED）通过随机功能制作两个由子像素组成的图像；在服务器端，只有用户 ID 和其中一张图像，而没有用户的密码。当用户登录并发送另一张图像时，服务器将此图像与先前拥有的图像重叠并去除背景以获得原始图像，然后利用 OCR（光学字符识别）Tesseract 算法提取 ID，从而可以通过将提取的 ID 与保存的 ID 进行比较，来对用户进行身份验证。

基于哈希的用户身份验证的传统密码学方案常使用 MD5、SHA-256 等流行哈希函数将用户密码口令转换为哈希值，易遭受暴力攻击、字典攻击或生日攻击等网络攻击。而该研究中提出的基于视觉密码的方案区别于传统方案，具有以下优点：在性能上，视觉密码仅需要很少的计算来创建每个像素的随机图案编号以进行加密，随机数发生器比散列函数具有较低的计算复杂度，解密更是不需要计算。在安全性上，该方案能够防止上述针对哈希的网络攻击：针对视觉密码的字典不存在，因为共享图像的大小与静态哈希大小不同，且通过图像而非文本搜索信息更困难；即使攻击者截获了保存的图像，也无法获取有关原始密码或子像素排列规则的任何信息；即使共享图像被扩展，它看起来也是无语义的；该方案还可以保护用户隐私，服务器仅保存一个共享图像而非密码，并接收另一个共享图像，不会显示诸如 ID 或密码等用户信息。

3.2 隐式通信

2019 年，邓传华[9]提出了采用文本隐写和图像隐写相结合的方法实现隐式通信。利用缩略语的基本概念，讨论了如何在短信中隐藏数据，如建议用“u”代替“You”或“l8ter”来代替“later”，并建议将数据隐藏在文本和图像中。数据首先被分成两部分，每部分与文本和

图像的大小成正比，并将数据大小保存在图像中以便进行解码，然后进行遍历，将一些数据隐藏在文本中，而另一些使用视觉密码方案隐藏在图像中。这种方法不需要在移动设备上使用复杂的设备或操作系统，可使用与大多数现代手机兼容的 J2ME 编程语言进行实现。

3.3 数字水印

2015 年，骆骁[10]将视觉密码技术应用于证件防伪，针对传统的防伪手段实现起来成本太昂贵的问题，提出了一种基于视觉密码和 QR 码的证件防伪方法：先将证件中的重要信息进行编码生成 QR 码，将其作为水印，再应用视觉密码技术结合水印图和特征图生成两个共享份，将其中的一个私有共享份作为零水印保存到零水印信息数据库，将 QR 码携带秘密信息的部分进行视觉密码分享，最终将共享份印刷在证件的四周；并针对现有数字水印技术在证件防伪的应用中存在的嵌入容量小和水印鲁棒性较差、安全性不高等问题，提出了一种基于视觉密码和矩阵谱范数的抗打印扫描零水印算法。实验结果表明，本文提出的基于视觉密码和 QR 码的证件防伪方案具有安全性高、携带信息容量大等特点，对常规的噪声、小角度旋转、剪切和缩放有良好的抵抗能力，并能有效地抵抗一次和二次打印扫描攻击。

4. 总结

综上所述，视觉密码基于秘密共享与数字图像技术。在 1994 年提出的第一个方案是开创性的，它提出了密码学研究的一个新的思路，此后发展出了诸多针对其加密图像类型受限、共享图像无意义和像素扩张导致对比度下降等问题的改进方案和新方案。因为视觉密码具有一定的安全性且秘密恢复不需计算，其具有非常多样的实际应用场景，在身份验证、隐式通信和数字水印等多方面均有所应用。

【参考文献】

[1] M. Naor and A. Shamir, “Visual cryptography,” Lecture Notes in Computer Science, vol. 950, pp. 1-12, 1995.

[2] Yang D , Doh I , Chae K . Enhanced password processing scheme based on visual cryptography and OCR[C]// 2017 International Conference on Information Networking (ICOIN). IEEE, 2017.

[3] Young-Chang Hou, Zen-Yu Quan, and Hsin-Yin Liao, ”New Designs for Friendly Visual Cryptography Scheme”, International Journal of Information and Electronics Engineering, Vol. 5, No. 1, January 2015.

[4] Y. C. Hou, “Visual cryptography for color images,” Pattern Recognition, vol. 36, issue 7, pp. 1619-1629, 2003.

[5] M.Karolin, Dr.T.Meyyapan,”RGB based secret sharing scheme in color visual cryptography”,International Journal of Advanced Research in Computer and Communication Engineering, ISSN : 2278-1021,Vol. 4, Issue 7, July 2015.

[6] Jainthi.k, Prabhu.P ,”A novel cryptographic technique that emphasis visual quality and efficieny by floyd steinberg error diffusion method”,International Journal of Research in Engineering and Technology, eISSN: 2319-1163 pISSN: 2321-7308,Volume: 04, Issue: 02 Feb2015.

[7] 王欢. 视觉密码技术的优化研究[D]. 西华大学, 2013.

[8] L M Varalakshmi, Prithy R and Radhika Parameswari.” Extended Visual Cryptography for Color Images and its PSNR Analysis”,International Journal of Computer Applications:67(17):17-22, April 2013.

[9] 邓传华. 计算机取证中的隐写术与视觉密码学. 广东电网有限责任公司河源供电局, 2019.

[10] 骆骁. 视觉密码在证件防伪中的应用研究[D]. 延边大学, 2015.