文章编号: 1001- 2486(2009) 01- 0086- 04

一种可验证的可视密码方案*

韩妍妍[1], 王夙颖[2], 胡 予濮[1], 何文才[3]

(1. 西安电子科技大学 计算机网络与信息安全教育部重点实验室, 陕西 西安 710071;
2. 空军指挥学院 科研部, 北京 100089; 3. 北京电子科技学院 科研工作处, 北京 100070)

摘 要: 可视密码是一项可以实现可视秘密共享的重要密码技术。它是将生成的分享图像分配给多个参与者, 将一定数量的分享重叠就可恢复出原秘密, 而不需要任何密码学计算。提出了一种可验证的可视密码方案, 该方案引入了行为值得信赖的可信第三方, 并引入了基于消息认证模型的公钥密码体系结构, 使得每个参与者都可以验证其分享的权威性。该方案解决了分发中心或者分发者的不诚实问题, 提高了可视密码方案实施的安全性。

关键词: 可验证的可视密码; 可信第三方; 经授权的分享
中图分类号: TP309. 7 文献标识码: A

A Verifiable Visual Cryptography Scheme

HAN Yan-yan[1], WANG Su-ying[2], HU Yu-pu[1], HE Wen-cai[3]

(1. Ministry of Education Key Laboratory of Computer Networks & Information Security, Xidian University, Xi' an 710071, China;
2. Department of Scientific Research, Air force Command College, Beijing 100089, China;
3. Department of Scientific Research, Beijing Electronic Science and Technology Institute, Beijing 100070, China)

Abstract: Visual cryptography is a cryptographic technique to achieve visual secret sharing. Shares are distributed to several participants and overlapping a number of shares can recover the original secret without any cryptographic computation. A verifiable visual cryptography scheme is proposed to verify whether the share is authorized by introducing the Third Trusted Party (TTP) whose action is guaranteed and the public key cryptographic infrastructure based on message identification model. The scheme solves the problem of dishonest distribution center to improve the security of visual cryptography schemes.

Key words: verifiable visual cryptography; third trusted party; authorized share

1995 年, Naor 和 Shamir 提出了秘密共享的一个新的分支, 被称为可视密码(VCS, Visual Cryptography Scheme)[1]。可视密码是将秘密(如秘密图像)分成多个分享(图像), 并将分享(图像)打印在透明的胶片上分给参与者。足够多的参与者可以通过将透明胶片叠加在一起恢复出秘密而不需要任何的密码学计算。可视密码已被应用在很多领域并进行了扩展, 如可视鉴别与验证[2], 隐写术[3]等。

传统的秘密共享方案都是基于所有成员都是诚实的这个普遍的假设, 其中隐含了两个问题: (1) 分发中心或分发者是不诚实的。他们可能给参与者分配未经授权的分享或伪造分享, 致使拥有这些分享的参与者无法恢复出秘密。(2) 分享的拥有者也就是参与者可能是不诚实的[4-5]。他们可以在秘密恢复的过程中出示一份伪造的分享, 致使秘密的恢复不成功。事实上, 要求所有成员都是诚实的是不容易的。因此, 未经改进的传统秘密共享方案是不安全的。

在秘密共享方案中, 如果经授权集合中的参与者 P_{i1}, …, P_{it} 想要恢复出秘密 K, 他们只需将手中的分享叠加就可以得到。然而在恢复秘密的过程中, 分发者可能给参与者分配了一个伪造的分享或者参与恢复秘密的分享在分配的过程中遭到破坏, 在这种情况下, 拥有分享的参与者就无法恢复出秘密。Clor 和 Goldwasser 等提出了可验证的秘密共享方案, 以防止参与者的欺骗行为[6]。可验证的秘密共享方

* 收稿日期: 2008- 09- 20
基金项目: 国家重点基础研究发展规划项目(2007CB31120); "十一五"国家密码发展基金项目
作者简介: 韩妍妍(1982—), 女, 博士生。

案允许每个参与者和其他的分享一起验证自己的分享。但这类方案存在的问题是, 不但参与者可能有欺骗行为, 分发者同样可能。文献[6] 提出了这个问题。Sadler 在文献[7] 中提出了一种新的可公开的可验证秘密分享方案, 该方案采用了通用的访问结构和门限秘密共享方案。可公开的可验证秘密共享方案被认为性能优于可验证的秘密共享方案。该方案可应用于软件密钥托管密码系统以及可取消匿名性的电子现金系统等[8- 9]。

可视密码是秘密共享的一个新的分支, 它的提出是为了解决秘密共享中恢复秘密的困难问题, 但同时也延续了秘密共享的一些性质与问题。文献[6- 9] 提出的防止欺骗的解决方案都是应用在秘密共享中。同样, 在可视密码中也存在上面提出的隐含问题, 其中已经有人针对参与者的欺骗行为提出了解决方案[10- 11], 但还没有针对分发者的不诚实行为提出的解决方案。

在秘密共享中, 可验证的秘密共享方案已经被广泛应用。在可视密码中, 也同样存在着如何验证分发中心或者分发者诚实性的问题。本文将可验证方案引入可视密码, 提出了可验证的可视密码方案。

1 可验证的可视密码方案

本文通过引入可信赖的第三方(TTP: Third Trusted Party) 提出了一种可视密码方案可验证分享的权威性。构造方案的中心思想是使每个参与者都可以向 TTP 申请验证他的分享是否是经授权的, 最终由 TTP 给出结论, 就可以得知分发中心诚实与否。但同时假设方案中的参与者都是诚实的, 而且分享在分配过程中都是安全的。

方案引用了基于消息认证模型的公钥基础结构来建立基于消息认证模型的可视密码方案[8], 实施过程如图 1 所示。在本方案中, 首先, 分发者提供给 TTP 一幅标识图(logo) , 其中可能包含与秘密有关的信息。TTP 根据(2, 2) 可视密码分享方案生成两幅分享图像, 一幅作为公用分享图像, 另一幅作为私有分享图像, TTP 同时保管两幅分享。然后, TTP 将公用分享图像与分发者根据(k, n) 可视密码分享方案生成的分享图像一起交由分发者分配给(k, n) 方案的各个参与者。当有参与者怀疑其分享的权威性而向 TTP 提出验证时, TTP 只需将参与者提供的公用分享图像与 TTP 拥有的私有分享图像叠加, 检验是否能恢复出原标识图信息。如果可以恢复, 则说明申请验证的分享是经授权的分享; 否则表明分发者给参与者分配了一个伪造的分享或分享遭到破坏。方案的具体执行过程如图 1 所示。

本方案采用了文献[1] 中所给出(2, 2) 可视密码构造方案来实现公用和私有分享图像的生成。其中, 公用分享图像与私有分享图像的选取是任意的。矩阵集合 C_T^0 和 C_T^1 是分别对矩阵 S_T^0 和 S_T^1 的列进行任意排列获得的, 这里称 S_T^0 和 S_T^1 为方案的基本矩阵, 定义为 $S_T^0 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$ 和 $S_T^1 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$。每个分享图像的子像素个数 m 为 4, 相对差 α 为 1/2。

2 分 析

2.1 性能分析

本文提出的可验证的可视密码方案只需要 1 次 2 个标识图分享图像的叠加就可以确定分享图像是否具有权威性, 并且不需要其他的附加信息。(2, 2) - 标识图分享方案以及(k, n) - 秘密图像分享方案中的参数 m 和 m' 是不同的。对于(2, 2) - 可视密码分享方案, 为了防止恢复的秘密图像发生扭曲变形, 通常选择 m= 4。而对于(k, n) - 可视密码分享方案, 在存储的空间复杂度上, 文献[2] 中的(k, n) 门限构造方法略优于文献[1], 如果采用文献[2] 中的对于一般门限构造的方法, 则本文构造的方案的 m' 值为 $O\left(2^k (\log_2 n)^{\log_2\left(\left(\frac{k}{2}\right)+1\right)}\right)$。

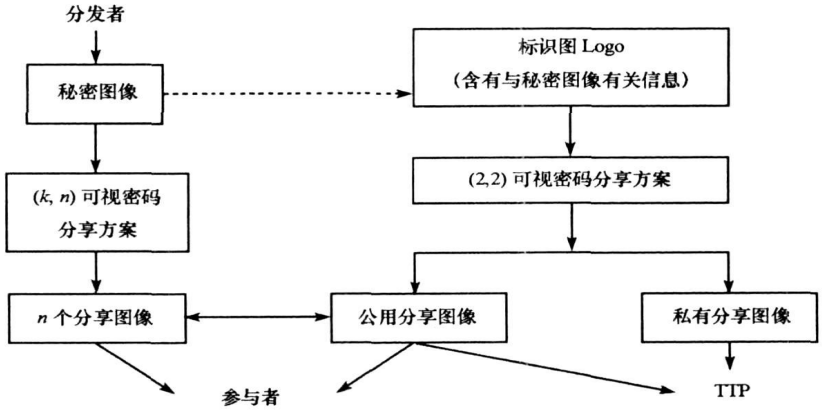

图 1 方案实施过程

Fig. 1 Performance process of the scheme

输入:

(1) 标识图(logo) T。

(2) 令 C_T^0 和 C_T^1 是基本布尔矩阵 S_T^0 和 S_T^1 的集合。

(3) 秘密图像 I(秘密图像与标识图大小不一定相同)。

(4) 令 C_I^0 和 C_I^1 是基本布尔矩阵 S_I^0 和 S_I^1 的集合。

分发过程:

(1) TTP 将标识图 T 分成 2 个分享图像 T_i, $i = 1, 2$。在分享图像 T_i 中的白或黑像素由 S_T^0 和 S_T^1 中的 $2 \times m$ 维矩阵表示。TTP 为了表示一个白(黑) 像素, 需进行以下操作:

1) 随机选择 C_T^0 中的矩阵 $S_T^0 = [s_{i,j}]$ (C_T^1 中的矩阵 $S_T^1 = [s_{i,j}]$)。

2) 对于每个参与者 i, 如果 $s_{i,j} = 0$($s_{i,j} = 1$), 则分享图像 T_i 为白(黑) 像素。

(2) 分发者将秘密图像 I 分成 n 个分享图像 I_p, $p = 1, \cdots, n$。分享图像 I_p 中的白或黑像素由 S_I^0 和 S_I^1 中的 $n \times m'$ 维矩阵来表示。分发者为了表示一个白(黑) 像素, 需进行以下操作:

1) 随机选择 C_I^0 中的矩阵 $S_I^0 = [s_{i,j}]$ (C_I^1 中的矩阵 $S_I^1 = [s_{i,j}]$)。

2) 对于每个参与者 i, 如果 $s_{i,j} = 0$($s_{i,j} = 1$), 则分享图像 I_p 为白(黑) 像素。

(3) 分发者将随机选择的标识图分享图像 T_1(T_2) 作为公用分享图像以及秘密分享图像 I_p($p = 1, \cdots, n$) 分配给 n 个参与者。

(4) TTP 同时保管有标识图的分享图像 T_1 和 T_2。

验证过程:

如果参与者 i($i = 1, \cdots, n$) 怀疑其拥有分享图像的权威性, 可以向 TTP 申请验证, 需进行以下操作:

(1) 参与者将其拥有的公用分享图像 $T_{i,j}$ ($i = 1, 2$, $j = 1, \cdots, n$) 提供给 TTP 进行验证。

(2) TTP 根据 $T_{i,j}$ 选择与其相配的私有分享图像 T_i ($i = 1, 2$)。

(3) 将 2 个分享图像进行或(OR) 运算得到图像 T'。

(4) 如果 $T' = T$, 则说明验证成功, 申请验证的分享图像是经授权的分享。

重构过程:

(1) 随机选择 $Q = \{i_1, \cdots, i_k\}$ 作为参与恢复秘密图像的参与者集合。

(2) 对所有的分享图像 I_p, $p \in \{i_1, \cdots, i_k\}$, 进行或(OR) 运算得到图像 I。

输出:

重构秘密图像 I 以及标识图 T。

如果 $T' \neq T$, 说明申请验证的秘密分享图像不具有权威性, 即为伪造分享, 因此该分享图像不具备可以恢复出秘密图像的能力。

图 2 方案具体执行过程

Fig. 2 Detailed performance process of the scheme

在本方案中, 分发者要向 TTP 提供一幅可能包含与秘密有关的信息的标识图, 以及在 TTP 生成标识

图分享图像后, 还要与分发者提供的根据(k, n) 可视密码分享方案生成的分享图像结合。在这个过程中, TTP 可以将所得到的 n 个秘密分享图像取其中任意 k 个相叠加, 均可得到原秘密信息。如果分发者提供了 1 个伪造的分享, 那么 TTP 执行 1 次 k 个分享图像叠加可以检测出伪造分享的概率为 C_{n-1}^{k-1}/C_n^k。

本方案易于实施, 且不需大量存储空间。验证时, 参与者只需将标识图分享图像提交给TTP 进行验证即可。由于其本身是类伪随机噪声图像, 无法获得关于标识图的任何线索。

2.2 安全性分析

如果有人想要在门限为 k 时伪造分发者的分享图像 I_p, $p = 1, \cdots, n$(某个基本矩阵中的一行) , 那么就必须同时伪造在(2, 2) 门限下用来申请验证的标识图分享图像 T_i, $i = 1, 2$。但是标识图分享图像是由 TTP 生成的, 不容篡改, 所以这种攻击是不可行的。

再考虑标识图分享图像中的像素 P_s, 在生成分享图像的过程中, 每个分享的子像素都包含有两个白像素, 两个黑像素。此外, 白- 黑和黑- 白出现的概率是相同的, 都是 1/2, 并且都与原像素的黑或白无关。因此, 分享图像 T_1 和 T_2 不能给出有关原像素黑或白的任何线索。由于对于标识图中所有的像素都是分别独立处理的, 所以观察分享图像中的任何像素集都无法得到有关原标识图的任何信息。除非采用穷尽的办法, 否则在所有可能的条件下无法得知每个像素的黑或白。

在传统的公钥密码解决方案中, 如果密文消息内容被恶意地修改过, 甚至只是 1 比特的修改, 原秘密都无法正确恢复出来而将会变成随机的数据。然而在可视密码解决方案中, 假设公用分享图像内容被恶意修改过, 那么将公用的与私有分享图像相叠加得到的将是类伪随机噪声图像, 但原来的标识图像仍是可视存在的。

3 结束语

可视密码是一项已经被广泛应用的秘密共享技术。提出的新型的可验证可视密码方案, 为参与者提供了可以验证其分享权威性的功能。方案引入了可信且公正的可信第三方(TTP) 以及公钥密码思想; 将(2, 2) 可视密码分享方案生成的两个分享图像作为两个密钥, 其中公用密钥分发给参与者, 两个密钥又同时由 TTP 保存; 而分发者掌管的公用密钥的作用就是用来验证(k, n) 可视密码方案生成的分享的权威性。验证过程简单, 只需判断两个密钥叠加的结果是否可以显示出标识图信息, 易于实现。

参 考 文 献:

[1] Naor M, Shamir A. Visual cryptography[C]// Advances in Cryptology—Proceedings of Eurocypt' 94, Lecture Notes in Computer Science, Springer-verlag, New York, 1995, 950: 1- 12.

[2] Naor M, Pinkas B. Visual Authentication and Identification [C]// Advances in Cryptology—Proceedings of Crypt' 97, Lecture Notes in Computer Science, Springer-verlag, New York, 1997, 1294: 322- 336.

[3] Chang C C, Chuang J C. An Image Intellectual Property Protection Scheme for Gray-level Image Using Visual Secret Sharing Strategy[J]. Pattern Recogn. Lett., 2002, 23: 931- 941.

[4] Horng G, Chen T, Tsai D S. Cheating in Visual Cryptography[C]// Science Business Media, Designs, Codes and Cryptography, Springer-verlag, Manufactued, 2006, 38: 219- 236.

[5] 郭洁, 颜浩, 刘妍, 等. 一种可防止欺骗的可视密码分享方案[J]. 计算机工程, 2005, 31(6): 126- 128.

[6] Chor B, Goldwasser S, Milica S, et al. Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults[C]// Proceedings of the 26th IEEE Symposium on Foundations of Computer Science, Washington: IEEE Computer Society Press, 1985: 383- 395.

[7] Stadler M. Publicly Verifiable Secrete Sharing[C]// Eurocypt' 96 Proceedings, LNCS 1070 1996: 190- 199.

[8] Camenishch J, Piveteau J M, Stadler M. An Efficient Fair Payment System[C]// Proc. 3rd ACM Conference on Computer and Communications Security, 1996.

[9] Naor M, Pinkas B. Visual Authentication and Identification[C]// Advances in Cryptology-CRYPTO' 97, Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1997, 1294: 322- 336.

[10] 颜浩, 甘志, 陈克非. 可防止欺骗的可视密码分享方案[J]. 上海交通大学学报, 2004, 38(1): 107- 110.

[11] Chih-ming H, Wen-guey T. Cheating Prevention in Visual Cryptography[J]. IEEE Transactions on Image Processing, 2007, 16(1): 36- 45.