基于小波压缩的二值图像图视密码学的改进*

安 韶 君
(中山大学 科学计算与计算机应用系, 广东 广州 510275)

摘 要: 图视密码学方案最初由 Naor 和 Shamir 在 1994 年欧洲密码学会议上提出, 但像素扩展太大, 生成分存图像太大。采用小波变换对分存图像进行压缩, 有效地降低了分存图像规模。

关键词: 图视密码学; 小波变换; 图像压缩; 秘密共享
中图分类号: TP309 文献标识码: A 文章编号: 0529-6579 (2002) 05-0011-04

给定 n 个参与者的集合 P, 图视密码学方案是一种将秘密图像编码变换成 n 份图像(称作分存), 集合 P 中的每个参与者得到一份分存的方法。属于有资格的集合的参与者可以通过"图视的"方法恢复出秘密图像, 而对于被禁止的集合的参与者得不到有关秘密图像的任何信息。对于参与者的一个集合 $X \subseteq P$, "图视的"恢复方法是指将 X 中的参与者的分存图像分别影印到透明胶片上, 然后全部重叠起来, 属于有资格的集合的参与者不用知道任何密码学的知识, 也不用执行任何解密操作就可以看到秘密图像。

图视密码学方案的思想源于 (k, n) 阈值秘密共享方案, 1979 年 Shamir[1] 和 Blakley[2] 分别提出了 (k, n) 阈值秘密共享方案, 将秘密信息分成 n 份分存, 任意 k 个或 k 个以上分存可以有效地计算出原始秘密, 而少于 k 个分存则无法有效计算出原始秘密。Shamir 的阈值方案基于拉格朗日插值多项式构造, Blakley 的阈值方案基于线性几何投影法。

图视密码学方案最初由 Naor 和 Shamir 在 1994 年欧洲密码学会议上提出[3], 该方案将上述 (k, n) 阈值秘密共享方案扩展到了图像秘密共享的领域。随后 Ateniese 等[4] 将图视密码学方案扩展到广义访问结构, 提出了一种对广义访问结构来构造图视密码学方案的方法, 其结果在像素扩展方面优于文 [1] 中的结果。Blundo 等[5] 提出了对二值图像的黑像素较好地恢复的图视密码学方案, 其方法实现了对原图像的黑像素能够在恢复图像中的对应子像素全部为黑像素, 并提出可以用线性规划来求解其模型。Blundo 等[6] 提出了一种灰度图像的图视密码学方案, 将图视密码学方案从二值图像扩展到了灰度图像, 并提出了其方案存在的充要条件。但图视密码学方案也存在一些缺点, 如: 像素扩展太大, 生成分存图像太大。本文采用小波变换对分存图像进行压缩, 降低分存图像规模。

1 二值图像图视密码学模型

设 $P = \{1, \cdots, n\}$ 是一个集合, 其元素称为参与者, P 的幂集 2^P 表示 P 的所有子集构成的集合。设 $\Gamma_{qual} \subseteq 2^P$, $\Gamma_{qual} \cap \Gamma_{forb} = \phi$。把 Γ_{qual} 的元素(是 P 的子集) 称作有资格的集合, 把 Γ_{qual} 的元素(也是 P 的子集) 称作被禁止的集合。集合对 $(\Gamma_{qual}, \Gamma_{forb})$ 称作该模型方案的访问结构。

定义 1 设 $(\Gamma_{qual}, \Gamma_{forb})$ 是 n 个参与者的访问结构, m 为正整数, 2 个元素为 $n \times m$ 布尔矩阵的集合 C_0, C_1。如果下列 2 个条件满足:

(1) 对 P 的任意子集 $X = \{j_1, j_2, \cdots, j_p\} \in \Gamma_{qual}$ 都可以通过重叠他们的分存图像来恢复出原始秘密图像;

即, 任取 $M \in C_i (i = 0, 1)$, 对其第 $j_1, j_2, \cdots, j_p$ 行作"或(OR)"运算所得的向量 V, $\omega(V)$ 表示对 m 维向量 V 的海明权值, 存在实数值 α 和集合 $\{(X, t_X)\}_{X \in \Gamma_{qual}}$, 其中 t_X 为实数, 满足:

$$\omega(V) \leqslant t_X - \alpha \cdot m \qquad i = 0$$
$$t_X \leqslant \omega(V) \qquad i = 1$$

(2) 对 P 的任意子集 $X = \{j_1, j_2, \cdots, j_p\} \in \Gamma_{forb}$ 得不到任何有关原始秘密图像的信息;

即, 当 $i = 0, 1$, 对由限定 C_i 中的每个 $n \times m$ 矩阵的第 $j_1, j_2, \cdots, j_p$ 行, 所得到的 g 个 $p \times m$ 矩阵的集合 D_0 和 D_1 相互之间是不可区分的, 因为 D_0, D_1 中的所包含的矩阵是相同的, 而且每个矩阵出现的频率相同;

* 收稿日期: 2002-02-05
作者简介: 安韶君 (1971 年生), 男, 博士生, 工程师; E-mail: asj@21cn.com

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

这时称上述2个元素为 $n\times m$ 布尔矩阵的集合 C_0, C_1 构成一个在(Γ_{qual}, Γ_{forb}) 下、像素扩展为 m 的、二值图像图视密码学方案(简记为 Γ_{qual}, Γ_{forb}, m-VCS)。

应用该二值图像图视密码学方案对初始二值秘密图像进行秘密分发的过程可简述如下, 对初始秘密图像的每个像素, 如其为白像素, 则任取一个 $n\times m$ 矩阵 $\boldsymbol{M}\in C_0$, 将其第 j 行分发给第 j 个参与者($j=1, \cdots, n$), 每个分存都得到了 m 个子像素; 如其为黑像素, 则任取一个 $n\times m$ 矩阵 $\boldsymbol{M}\in C_1$, 将其第 j 行分发给第 j 个参与者($j=1, \cdots, n$), 每个分存都得到了 m 个子像素; 对初始秘密图像的每一个像素都这样操作, 则每个参与者都得到了各自不同的一个秘密分存图像。恢复的时候, 属于有资格的集合的参与者将其分存图像重叠起来, 就可以看到初始秘密图像。

定义1中的第1个条件称为对比度条件, 它保证了有资格的参与者能够正确恢复原图像, 恢复时黑像素和白像素在视觉上具有差异从而显示出原始秘密图像; 第2个条件称为安全性条件, 它保证被禁止的集合的参与者得不到有关秘密图像的任何信息。对于图视密码学模型来说, 像素扩展 m 越小, 分存图像就会越小; α 表示各子图像矩阵叠加后黑白像素间的海明权值的相对差, 其值越大越好, 生成图像则越清晰。

定义1与Naor等[3]定义的二值图像(k, n)-VCS阈值图视密码学方案不同, 这里不详述, 主要区别在于, 定义1是将(k, n)-VCS方案扩展到了更具一般性的访问结构, (k, n)-VCS阈值方案相当于一类强的访问结构, 这类强访问结构的直观意义可以理解为: 任意 k 个参与者可以恢复原始秘密图像, 则任意 $k+1$ 个参与者也可以恢复原始秘密图像; 而访问结构不一定都是强的。

选取一个二值图像图视密码学方案(Γ_{qual}, Γ_{forb}, m-VCS) 为:

(Γ_{qual}, Γ_{forb}) 是4($n=4$) 个参与者的访问结构,

$\Gamma_{qual}=\{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\},\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\},\{1,2,3,4\}\}$

$\Gamma_{forb}=\{\{1\},\{2\},\{3\},\{4\}\}$

$m=4$, C_0, C_1 为元素为 $n\times m$ 即 4×4 布尔矩阵的集合, 分别由以下2个矩阵(称为生成矩阵) 按照所有可能的方式进行列置换所得到:

$$\boldsymbol{S}_0=\begin{pmatrix}0&1&1&1\\0&1&1&1\\0&1&1&1\\0&1&1&1\end{pmatrix},\ \boldsymbol{S}_1=\begin{pmatrix}0&1&1&1\\1&0&1&1\\1&1&0&1\\1&1&1&0\end{pmatrix}$$

共有4!种置换方法, 即 C_0, C_1 的元素数均为4!个。

对 P 的任意子集 $X=\{j_1, j_2, \cdots, j_p\}\in\Gamma_{qual}$, 存在实数值 $\alpha=1/4$ 和集合 $\{(X, t_X)\}_{X\in\Gamma_{qual}}$, 取 $t_X=4$, 对 C_0 来说, $\omega(\boldsymbol{V})=3$, 对 C_1 来说, $\omega(\boldsymbol{V})=4$, 满足定义1中的条件。对任意 $X\in\Gamma_{forb}$, 可以直观看出, 各自的子像素矩阵在列置换的意义下是相同的, 所以得不到任何有关原始秘密图像的信息。

这个例子的访问结构是强的, 也是(2, 4)-VCS阈值方案, 即4个参与者中任意2个或2个以上参与者把他们的分存图像重叠起来可以在视觉上恢复原始秘密图像。

把4个子像素按照2×2矩阵排列, 这样就保证了生成图像的纵横比与原图像相同, 不致于造成变形。采用上述二值图像图视密码学方案计算, 原始秘密图像见图1(128像素×128像素)。

图1 秘密图像

Fig. 1 Secret image

生成的各分存图像均为256像素×256像素, 由于像素扩展, 是原图像的4倍, 为压缩篇幅, 只列出分存图像1(图2(a)) 和分存图像2(图2(b)) 以及将分存图像1与分存图像2恢复的秘密图像(图2(c))。其它分存图像与此类似。

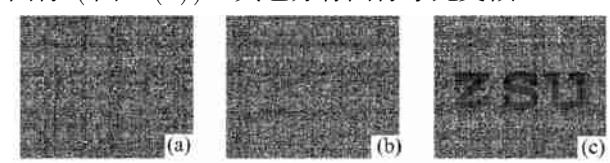

图2 分存图像及恢复图像

Fig. 2 Shares and recovered image

2 二值图像图视密码学方案的特点分析和改进

2.1 二值图像图视密码学方案的特点分析

(1) 像素扩展 m 太大, 生成分存图像太大

对于上述(2, 4)-VCS例子来说, 像素扩展 $m=4$, 生成的分存图像大小扩大为原图像的4倍。当参与者越多, 为满足对比度条件, 其访问结构所对应的矩阵就越大, 像素扩展 m 也会越大, 计算机运算和处理的时间就越长, 生成的分存图像就越大。

(2) 对比度降低

应用图视密码学方案处理图像, 恢复图像的对比度总会有不同程度的降低, 同时像素扩展 m 越

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

大, 即使采用不同的方案, 相邻灰度级(黑白像素) 之间的相对差保持不变, 恢复图像的对比度也会降低。

2.2　双正交样条小波

双正交样条小波具有紧支撑和对称性[7,8], 通过使用2 个小波, 分别用于分解和重构。其滤波器具有线性相位特性, 有助于减少边缘处的失真。

本文选取 $N_r=3$、$N_d=7$ 的双正交样条小波, 其滤波器系数分别为:

分解滤波器 {0.002 1　−0.006 4　−0.011 9　0.052 8
0.022 2　−0.213 0　−0.018 7　0.672 9
0.672 9　−0.018 7　−0.213 0　0.022 2
0.052 8　−0.011 9　−0.006 4　0.002 1}

重构滤波器 {0.125 0　0.375 0　0.375 0　0.125 0}

分解低通滤波器 {0.003 0　−0.009 1　−0.016 8　0.074 7
0.031 3　−0.301 2　−0.026 5　0.951 6
0.951 6　−0.026 5　−0.301 2　0.031 3
0.074 7　−0.016 8　−0.009 1　0.003 0}

分解高通滤波器 {0　0　0　0
0　0　−0.176 8　0.530 3
−0.530 3　0.176 8　0　0
0　0　0　0}

重构低通滤波器 {0　0　0　0
0　0　0.176 8　0.530 3
0.530 3　0.176 8　0　0
0　0　0　0}

重构高通滤波器 {0.003 0　0.009 1　−0.016 8　−0.074 7
0.031 3　0.301 2　−0.026 5　−0.951 6
0.951 6　0.026 5　−0.301 2　−0.031 3
0.074 7　0.016 8　−0.009 1　−0.0030}

其尺度函数、小波函数、分解滤波器和重构滤波器图形见图 3。

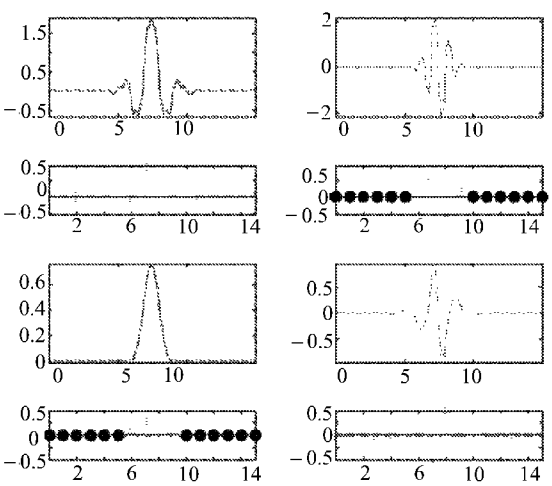

图 3　$N_r=3$、$N_d=7$ 的双正交样条小波

Fig. 3　Biorthogonal spline wavelets

2.3　小波变换低频系数用于分存图像压缩

由于阈值图视密码学方案中的矩阵比较大, 特别是对较多的参与者, 其生成矩阵的行列数将非常大, 而生成矩阵的列数决定了生成的分存图像大小与原图像大小相比较的倍数。考虑利用小波变换用于分存图像的压缩, 采用双正交样条小波对分存图像进行压缩处理。将图像分解为低频信号分量、水平方向高频信号分量、垂直方向高频信号分量和对角方向高频信号分量, 即小波变换后的低频系数和高频系数分量。只保留低频信号分量作为新的分存图像, 因为多数图像的统计特性表明, 图像信息基本保留在低频信号中, 高频信号为更进一步的细节, 从而降低了分存图像的存储规模。下面是对上文中的各分存图像进行小波变换图像压缩后的各对应分存图像, 为节省篇幅, 只列出 share1 和 share2 压缩后的各对应分存图像。经过第 1 层小波分解后, 对应的分存图像大小为 135 像素× 135 像素, 图像大小得到了显著的缩小, 压缩后的分存图像 1、2 重叠后恢复图像的效果也可以接受。因为是有损压缩, 恢复的图像的分辨率有所降低 (图 4)。

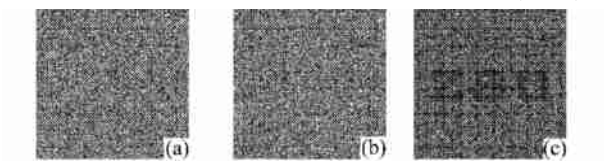

图 4　小波变换低频系数压缩的分存图像及恢复图像

Fig. 4　Low-fraquency coefficients wavelet-compressed shares and recovered image

2.4　小波变换用于分存图像压缩

由于上述小波变换直接采用低频系数用于分存图像压缩, 恢复的图像的分辨率有所降低。下面将分存图像的低频系数和高频系数结合起来恢复秘密图像。观察小波变换后的高频系数可以发现, 高频部分系数大部分点的数值都接近于 0, 对高频部分系数采用阈值量化处理, 只保留不为 0 的系数, 这样高频部分系数大部分点可以分配较少的比特位数, 从而对分存图像进行压缩。下面是对上文中的各分存图像进行小波变换图像压缩后恢复得到的各对应分存图像, 为节省篇幅, 只列出 share1 和 share2 压缩后的各对应分存图像。对 share1 小波压缩分解系数中置 0 系数的个数的百分比为 60.20%, 压缩后图像剩余能量的百分比是 91.78%。对 share2 小波压缩分解系数中置 0 系数的个数的百分比为 60.17%, 压缩后图像剩余能量的百分比是 91.78%。从图中可以看出, 恢复图像的效果接近于不作图像压缩的效果 (图 5)。

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

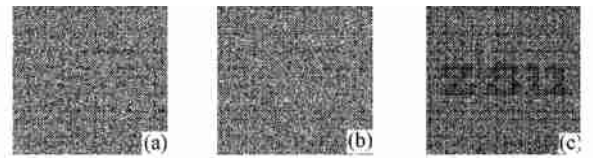

图5 小波变换压缩的分存图像及恢复图像

Fig 5 Wavelet-compressed shares and recovered image

致谢：感谢导师李岳生教授给予的指导和帮助。

参考文献：

[1] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 24(11): 612—613.

[2] BLAKLEY G R, MEADOWS C. A database encryption scheme which allows the computation of statistics using encrypted data[J]. Proceedings of the 1985 Symposium on security and privacy, IEEE Computer Society, 1985: 116—122.

[3] NAOR M, SHAMIR A. Visual cryptography[J]. Advances in Cryptology-Eurocrypt' 94, Lecture Notes in Comput Sci, 1995, 950: 1—12.

[4] ATENIESE G, BLUNDO C, De SANTIS A, et al. Visual cryptography for general access structures[J]. Information And Computation, 1996, 129(2): 86—106.

[5] BLUNDO C, De SANTIS A. Visual cryptography schemes with perfect reconstruction of black pixels[J]. J Computer&Graphics, Special issue: Data Security in Image Communication and Networking, 1998, 22(4): 449—455.

[6] BLUNDO C, De SANTIS A, NAOR M. Visual cryptography for grey level images[J]. Information Processing Letters, 2000, 75: 255—259.

[7] 丁玮, 齐东旭. 数字图像变换及信息隐藏与伪装技术[J]. 计算机学报, 1998, 21(9): 838—843.

[8] 胡昌华, 李军波, 夏军, 等. 基于MATLAB的系统分析与设计——小波分析[M]. 西安: 西安电子科技大学出版社, 1999: 109—246.

A Wavelet Compression Based on Scheme of Visual Cryptography for Binary Images

AN Shao-jun

(Department of Scientific Computation and Computer Applications, Sun Yat-sen(Zhongshan) University, Guangzhou 510275, China)

Abstract: Visual cryptography is a cryptographic paradigm introduced by Naor and Shamir in Cryptology-Eurocrypt' 94. Whereas the pixel expansion makes the size of the share transparencies big. This paper applies wavelet transform to compress the share images and reduces the size.

Key words: visual cryptography; wavelet transform; image compression; secret sharing

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net