一个新的图像单幅可视隐藏方案

刘 铎[1),2)] 戴一奇[2)]

[1)](北京交通大学软件学院 北京 100044)

[2)](清华大学计算机科学与技术系 北京 100084)

摘 要 作为一种数字水印的技术方法,提出了一种新的单幅图像可视隐藏方案.在该方案中,仅使用一幅加密图便能可视恢复密图,加密图本身既是编码又是解码.与已有的基于移位的方案不同,该方案通过加密图逆时针旋转90°后和自身的叠加来恢复原图.给出了实现单幅图像可视隐藏的新方案的设计方法,对方案的性能进行了分析,并且指出新方案具有较好的抗压缩性、抗破损性、抗放缩性,且能充分利用密图的容量.

关键词 信息安全;信息隐藏;可视隐藏;数字水印

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2009.02247

A New Visual Hiding Scheme Using One Secret Image

LIU Duo[1),2)] DAI Yi-Qi[2)]

[1)](*School of Software Engineering, Beijing Jiaotong University, Beijing* 100044)

[2)](*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084)

Abstract For presenting a new technique of digital watermarking, a new scheme on hiding a secret image into single shadow image is proposed. Differ from any existed methods of visual hiding schemes using one secret image, the new scheme based on the rotation of the shadow image. In the new scheme, the single shadow image acted both encoder and decoder function. Therefore the secret image can be recovered by stacking the shadow image and the shadow image after rotated 90 degree anticlockwise. The new method has the property of anti-compression, anti-distortion and anti-shrink. Furthermore, the new scheme can use the shadow image sufficiently.

Keywords information security; information hiding; visual hiding; digital watermarking

1 引 言

Naor 和 Shamir 在 1994 年欧洲密码学会上介绍了一种密图可视分存技术[1],并给出(k,n)阈值方案:当且仅当 k 个影段的透明片重合在一起时这个密图可视;少于 k 个,则无从得到密图的任何信息.与以往的技术相比,可视密码技术具有隐蔽性、安全性、秘密恢复的简单性以及通用性等突出的特点.目前,已经提出了许多可视密码技术的拓展形式,如S-扩展型[2]、限制可视空间型[3]、可跟踪型[4]、彩色型[5]、欺骗型[6]、自叠加型[7-8]等.也有许多关于对比度及信息扩展冗余等理论方面的研究[9-10].

文献[7]指出,在实际应用中,由于需要两幅以上互异的分存图像叠加到一起才能恢复隐藏的秘密,如果其中的一幅图像因压缩或几何变形等处理导致失真,则很难再恢复隐藏的秘密.为了解决此问题,文献[7-8]给出了两种新的可视隐藏方案,仅使用一幅加密图便可以恢复秘密:即用加密图按照一定的方式错位,再与原密图叠加,可恢复秘密.

收稿日期:2006-09-15;最终修改稿收到日期:2009-07-13. 本课题得到国家自然科学基金(60673065)资助.**刘 铎**,男,1978 年生,博士,讲师,研究方向包括网络安全、椭圆曲线密码学、组合算法的设计与分析. E-mail: bat@mail.tsinghua.edu.cn. **戴一奇**,男,1946 年生,硕士,教授,博士生导师,研究领域包括信息安全、网络安全、算法的设计与分析.

但是这两种方法都是基于错位的，而且不能充分利用掩图：秘密只能隐藏在下图的阴影部分.

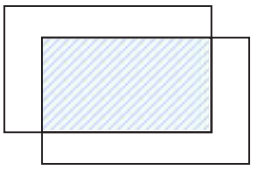


图 1 基于错位的单幅图像隐藏

在本文中我们提出一种新的单幅图像的方法，其基于图像的旋转，方法是将掩图逆时针旋转 90°后和自身叠加即恢复出密图，模式说明如图 2 所示（其中密图用 $\boldsymbol{S}$ 表示，掩图用 $\boldsymbol{G}$ 表示）.

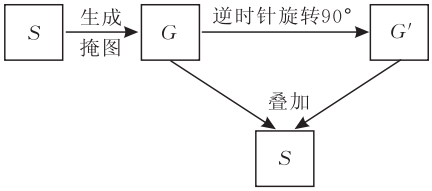


图 2 基于旋转的单幅图像隐藏

2 定义与记号

为行文和算法描述的方便，首先定义 $\hat{i}=2n+1-i$，$\hat{j}=2n+1-j$.

我们的方案是基于旋转的，即图像旋转 90°后大小应能与自身重合，且任何一个像素旋转后叠加时不与自身重合——因此图像必须是 $2n\times 2n$ 的；另外，从轮换的角度来讲，图像旋转 90°相当于 n^2 个 4 轮换. 由此我们给出如下定义.

定义 1. 将二值图像表示成为一个 $2n\times 2n$ 的 0-1 矩阵 $\boldsymbol{S}=(s_{i,j})_{2n\times 2n}$，并定义该图像的 (i,j) 子图为 $\boldsymbol{S}_{i,j}=\begin{bmatrix} s_{i,j} & s_{j,\hat{i}} \\ s_{\hat{j},i} & s_{\hat{i},\hat{j}} \end{bmatrix}$.

在下文中，如不加特殊声明，所提及的图像和子图均是如定义 1 所定义的.

下面定义两个图像的叠加.

定义 2. 假定 $\boldsymbol{G}^1=(g^1_{i,j})_{2n\times 2n}$ 和 $\boldsymbol{G}^2=(g^2_{i,j})_{2n\times 2n}$ 是两张图像，则定义 $\boldsymbol{G}^1$ 与 $\boldsymbol{G}^2$ 的叠加图像为 $(g^1_{i,j}\vee g^2_{i,j})_{2n\times 2n}$.

下面通过定义子图的掩存来定义掩图.

定义 3. $\begin{bmatrix} g_{1,1} & g_{2,1} & g_{3,2} & g_{1,2} \\ g_{3,1} & g_{4,1} & g_{4,2} & g_{2,2} \\ g_{2,4} & g_{4,4} & g_{4,3} & g_{3,3} \\ g_{1,4} & g_{3,4} & g_{2,3} & g_{1,3} \end{bmatrix}\in\{0,1\}^{4\times 4}$ 称为是 $\begin{bmatrix} s_1 & s_2 \\ s_4 & s_3 \end{bmatrix}\in\{0,1\}^{2\times 2}$ 的一个掩存，若

$$s_i=1\Leftrightarrow\begin{bmatrix} g_{1,i}\vee g_{1,i+1} & g_{2,i}\vee g_{2,i+1} \\ g_{3,i}\vee g_{3,i+1} & g_{4,i}\vee g_{4,i+1} \end{bmatrix}=\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix},$$

$i=1,2,3,4$（取模 4 加法）.

定义 4. 假定 $\boldsymbol{S}=(s_{i,j})_{2n\times 2n}$ 是一张图像，则称 $\boldsymbol{G}=(g_{i,j})_{4n\times 4n}$ 是 $\boldsymbol{S}$ 的一个掩图，若

$$\begin{bmatrix} g_{2i-1,2j-1} & g_{2i-1,2j} & g_{2j-1,2\hat{i}-1} & g_{2j-1,2\hat{i}} \\ g_{2i,2j-1} & g_{2i,2j} & g_{2j,2\hat{i}-1} & g_{2j,2\hat{i}} \\ g_{2\hat{j}-1,2i-1} & g_{2\hat{j}-1,2i} & g_{2\hat{i}-1,2\hat{j}-1} & g_{2\hat{i}-1,2\hat{j}} \\ g_{2\hat{j},2i-1} & g_{2\hat{j},2i} & g_{2\hat{i},2\hat{j}-1} & g_{2\hat{i},2\hat{j}} \end{bmatrix}$$

是 $\boldsymbol{S}_{i,j}=\begin{bmatrix} s_{i,j} & s_{j,\hat{i}} \\ s_{\hat{j},i} & s_{\hat{i},\hat{j}} \end{bmatrix}$ 的一个掩存，$1\leq i,j\leq n$.

3 新方案的设计与分析

3.1 设计的规则

为描述方便，引入如下记号：

$$\boldsymbol{A}_1=\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix},\ \boldsymbol{A}_2=\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix},\ \boldsymbol{A}_3=\boldsymbol{A}_2^{\mathrm{T}},\ \boldsymbol{A}_4=\boldsymbol{A}_1^{\mathrm{T}},$$

$$\boldsymbol{B}_1=\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix},\ \boldsymbol{B}_2=\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},\ \boldsymbol{B}_3=\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix},\ \boldsymbol{B}_4=\boldsymbol{B}_2^{\mathrm{T}},$$

$$\boldsymbol{C}_1=\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ \boldsymbol{C}_2=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

而且，在下面的设计规则中，$\boldsymbol{A}$、$\boldsymbol{B}$ 的下标是模 4 进行运算的，$\boldsymbol{C}$ 的下标是模 2 进行运算的.

下面的引理表明，可以由一个子图的掩存图像得到旋转后的另一个子图的掩存图像，其证明是平凡的.

引理 1. 若 $\begin{bmatrix} g_{1,1} & g_{2,1} & g_{3,2} & g_{1,2} \\ g_{3,1} & g_{4,1} & g_{4,2} & g_{2,2} \\ g_{2,4} & g_{4,4} & g_{4,3} & g_{3,3} \\ g_{1,4} & g_{3,4} & g_{2,3} & g_{1,3} \end{bmatrix}$ 是 $\begin{bmatrix} s_1 & s_2 \\ s_4 & s_3 \end{bmatrix}$ 的一个掩存，则 $\begin{bmatrix} g_{1,2} & g_{2,2} & g_{3,3} & g_{1,3} \\ g_{3,2} & g_{4,2} & g_{4,3} & g_{2,3} \\ g_{2,1} & g_{4,1} & g_{4,4} & g_{3,4} \\ g_{1,1} & g_{3,1} & g_{2,4} & g_{1,4} \end{bmatrix}$ 是 $\begin{bmatrix} s_2 & s_3 \\ s_1 & s_4 \end{bmatrix}$ 的一个掩存.

故而在下面的设计规则中只考虑子图在旋转意义下彼此不同的情况.

表 1 中给出了设计所采用的规则，每行的各个规则以等概率随机选取，其中 $j=i+2$ 或 $i+3$，$l=$

$i+1$ 或 $i-1$,$k=i$ 或 $i+2$, $m=i$ 或 $i+1$.

表 1　设计规则

子图	设计的规则
(1) $\begin{bmatrix}1&0\\0&0\end{bmatrix}$	$\begin{bmatrix}B_i&A_j\\C_{i+1}&B_i\end{bmatrix}$, $\begin{bmatrix}C_i&B_i\\B_l&A_i\end{bmatrix}$, $\begin{bmatrix}A_j&B_{i+2}\\B_{i+2}&C_{i+1}\end{bmatrix}$, $\begin{bmatrix}B_{i+2}&C_i\\A_i&B_l\end{bmatrix}$
(2) $\begin{bmatrix}1&0\\1&0\end{bmatrix}$	$\begin{bmatrix}B_i&C_i\\C_i&B_k\end{bmatrix}$, $\begin{bmatrix}A_m&B_i\\B_{i+2}&C_{i+1}\end{bmatrix}$
(3) $\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}B_i&C_i\\C_{i+1}&B_l\end{bmatrix}$, $\begin{bmatrix}C_i&B_k\\B_{i+1}&C_{i+1}\end{bmatrix}$
(4) $\begin{bmatrix}0&0\\0&0\end{bmatrix}$	$\begin{bmatrix}B_i&C_{i+1}\\C_{i+1}&B_k\end{bmatrix}$, $\begin{bmatrix}C_{i+1}&B_k\\B_i&C_{i+1}\end{bmatrix}$
(5) $\begin{bmatrix}1&1\\1&1\end{bmatrix}$	$\begin{bmatrix}B_i&C_i\\C_i&B_k\end{bmatrix}$, $\begin{bmatrix}C_i&B_k\\B_i&C_i\end{bmatrix}$
(6) $\begin{bmatrix}0&1\\1&1\end{bmatrix}$	$\begin{bmatrix}B_i&C_{i+1}\\B_{i+1}&C_{i+1}\end{bmatrix}$, $\begin{bmatrix}C_i&B_{i+1}\\C_i&B_i\end{bmatrix}$

3.2　掩图生成的算法流程

1. 初始化模式:$\boldsymbol{A}_1,\boldsymbol{A}_2,\boldsymbol{A}_3,\boldsymbol{A}_4,\boldsymbol{B}_1,\boldsymbol{B}_2,\boldsymbol{B}_3,\boldsymbol{B}_4,\boldsymbol{C}_1,\boldsymbol{C}_2$;

2. 将密图 $\boldsymbol{S}=(s_{i,j})_{2n\times 2n}$ 分成子图

$$\left\{\boldsymbol{S}_{i,j}=\begin{bmatrix}s_{i,j}&s_{j,\hat{i}}\\s_{\hat{j},i}&s_{\hat{i},\hat{j}}\end{bmatrix}\right\}_{1\le i\le n,1\le j\le n};$$

3. 对每一个子图 $\boldsymbol{S}_{i,j}=\begin{bmatrix}s_{i,j}&s_{j,\hat{i}}\\s_{\hat{j},i}&s_{\hat{i},\hat{j}}\end{bmatrix}$,采用引理 1 和表 1 中的规则产生子图的掩图

$$\boldsymbol{G}_{i,j}=\begin{bmatrix}g_{1,1}^{i,j}&g_{2,1}^{i,j}&g_{3,2}^{i,j}&g_{1,2}^{i,j}\\g_{3,1}^{i,j}&g_{4,1}^{i,j}&g_{4,2}^{i,j}&g_{2,2}^{i,j}\\g_{2,4}^{i,j}&g_{4,4}^{i,j}&g_{4,3}^{i,j}&g_{3,3}^{i,j}\\g_{1,4}^{i,j}&g_{3,4}^{i,j}&g_{2,3}^{i,j}&g_{1,3}^{i,j}\end{bmatrix};$$

4. 由各个子图的掩图 $\boldsymbol{G}_{i,j}$ 生成掩图 $\boldsymbol{G}=(g_{i,j})_{4n\times 4n}$,其中

$$g_{2i-1,2j-1}=g_{1,1}^{i,j},\ g_{2\hat{j}-1,2i-1}=g_{2,4}^{i,j},$$
$$g_{2j-1,2\hat{i}-1}=g_{3,2}^{i,j},\ g_{2\hat{i}-1,2\hat{j}-1}=g_{4,3}^{i,j},$$
$$g_{2i-1,2j}=g_{2,1}^{i,j},\ g_{2\hat{j}-1,2i}=g_{4,4}^{i,j},$$
$$g_{2j-1,2\hat{i}}=g_{1,2}^{i,j},\ g_{2\hat{i}-1,2j}=g_{3,3}^{i,j},$$
$$g_{2i,2j-1}=g_{3,1}^{i,j},\ g_{2\hat{j},2i-1}=g_{1,4}^{i,j},$$
$$g_{2j,2\hat{i}-1}=g_{4,2}^{i,j},\ g_{2\hat{i},2\hat{j}-1}=g_{2,3}^{i,j},$$
$$g_{2i,2j}=g_{4,1}^{i,j},\ g_{2\hat{j},2i}=g_{3,4}^{i,j},$$
$$g_{2j,2\hat{i}}=g_{2,2}^{i,j},\ g_{2\hat{i},2\hat{j}}=g_{1,3}^{i,j},$$
$$1\le i,\ j\le n.$$

3.3　新方案的性能分析

首先,定理 1 表明不存在一种方法使得掩图每个像素为黑或为白的概率都恰好为 1/2.

定理 1.　记

$$p_{\boldsymbol{R}}=\min_{\forall \boldsymbol{S}}\left\{\max_{1\le i,j\le 4n}\begin{Bmatrix}P(g_{i,j})=1;\\\boldsymbol{G}\text{ 是 }\boldsymbol{S}\text{ 由规则集}\\\boldsymbol{R}\text{ 生成的掩图}\end{Bmatrix}\right\},$$

则 $p_{\boldsymbol{R}}>1/2$ 对任意规则集 $\boldsymbol{R}$ 成立.

证明.　假设存在一个规则集 $\boldsymbol{R}$ 使得

$$\left(P(g_{i,j}=1)=\frac{1}{2};\boldsymbol{G}\text{ 是图像 }\boldsymbol{S}\text{ 的一个掩图}\right)_{\forall \boldsymbol{S}},$$

则特别地,取 $\boldsymbol{S}=\begin{bmatrix}0&1\\1&1\end{bmatrix}$,假定 $\boldsymbol{R}$ 中针对 $\boldsymbol{S}$ 的规则子集为 $\{R_k\}_{1\le k\le t}$,每个规则 R_k 以概率 p_k 选取,记由规则 R_k 产生的掩图为

$$\begin{bmatrix}g_{1,1}^k&g_{2,1}^k&g_{3,2}^k&g_{1,2}^k\\g_{3,1}^k&g_{4,1}^k&g_{4,2}^k&g_{2,2}^k\\g_{2,4}^k&g_{4,4}^k&g_{4,3}^k&g_{3,3}^k\\g_{1,4}^k&g_{3,4}^k&g_{2,3}^k&g_{1,3}^k\end{bmatrix},$$

则

$$P(g_{i,j}=1)=\sum_{k=1}^{t}p_k\cdot g_{i,j}^k.$$

由于

$$\begin{bmatrix}g_{1,2}^k\vee g_{1,3}^k&g_{2,2}^k\vee g_{2,3}^k\\g_{3,2}^k\vee g_{3,3}^k&g_{4,2}^k\vee g_{4,3}^k\end{bmatrix}=\begin{bmatrix}g_{1,3}^k\vee g_{1,4}^k&g_{2,3}^k\vee g_{2,4}^k\\g_{3,3}^k\vee g_{3,4}^k&g_{4,3}^k\vee g_{4,4}^k\end{bmatrix}=\begin{bmatrix}1&1\\1&1\end{bmatrix}.$$

因此有

$$\sum_{i-1}^{4}(g_{i,2}^k+g_{i,3}^k)\ge 4\text{ 且 }\sum_{i=1}^{4}(g_{i,4}^k+g_{i,3}^k)\ge 4;$$

另一方面很容易验证,不存在使

$$\sum_{i=1}^{4}(g_{i,2}^k+g_{i,3}^k)=\sum_{i=1}^{4}(g_{i,4}^k+g_{i,3}^k)=4$$

的掩存图.

若 $P(g_{i,j}=1)=\frac{1}{2}$ 对所有 $1\le i,j\le 4$ 成立,则

$$\sum_{k=1}^{t}p_k\cdot\sum_{i=1}^{4}(g_{i,2}^k+g_{i,3}^k)=8\cdot\frac{1}{2}=4$$

且
$$\sum_{k=1}^{t}p_k\cdot\sum_{i=1}^{4}(g_{i,3}^k+g_{i,4}^k)=4.$$

又对任意 k 满足 $\sum_{i=1}^{4}(g_{i,2}^k+g_{i,3}^k)\ge 4$ 且 $\sum_{i=1}^{4}(g_{i,3}^k+g_{i,4}^k)\ge 4$,因此必然有对任意 k,满足

$$\sum_{i=1}^{4}(g_{i,2}^k+g_{i,3}^k)=\sum_{i=1}^{4}(g_{i,4}^k+g_{i,3}^k)=4,$$

与上述矛盾,假设不能成立.

故而不存在一类规则,使得

$$\left(P(g_{i,j}=1)=\frac{1}{2};\boldsymbol{G}\text{ 是图像 }\boldsymbol{S}\text{ 的一个掩图}\right)_{\forall \boldsymbol{S}}$$

证毕.

特别地,对于本文提出的方案而言,有下面定理.

定理 2. 若表 1 中每条规则都以等概率选取,则概率$P(g_{i,j}=1)=5/8$对任意$1\leq i, j\leq 4n$成立.

证明. 直接验证即可.

上述两个定理说明本文提出的方案就掩图的每个像素而言,是不可区分的.而下面的定理给出了由本文方案生成的掩图的对比度.

定理 3. 假定

$$\begin{bmatrix} g_{1,1} & g_{2,1} & g_{3,2} & g_{1,2} \\ g_{3,1} & g_{4,1} & g_{4,2} & g_{2,2} \\ g_{2,4} & g_{4,4} & g_{4,3} & g_{3,3} \\ g_{1,4} & g_{3,4} & g_{2,3} & g_{1,3} \end{bmatrix} \in \{0,1\}^{4\times 4}$$

是由表 1 中规则生成的$\begin{bmatrix} s_1 & s_2 \\ s_4 & s_3 \end{bmatrix} \in \{0,1\}^{2\times 2}$的一个掩存,则

$$s_i=1 \Leftrightarrow \sum_{j=1}^{4}(g_{j,i} \vee g_{j,i+1})=4;$$

$$s_i=0 \Leftrightarrow \sum_{j=1}^{4}(g_{j,i} \vee g_{j,i+1})=3.$$

其中$i=1,2,3,4$(取模 4 加法).

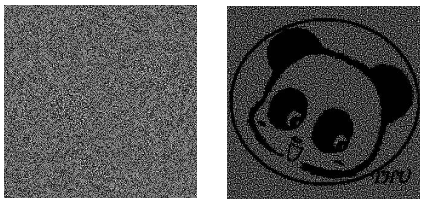
证明. 直接验证即可.

注. 由算法可知,此处只要证明子图的对比度如定理所述,即可平凡性地推广到掩图的对比度情况.

4 结 论

本文给出了一个单幅图像可视隐藏的新方案,采用的不是已有的错位方法而是旋转的方法,而且信息膨胀是 4,已达最小可能.由于是用自身一张图而得到密图,因此该方案可作为一种可视数字水印使用.特别地,该方案可抗放缩处理,而基于错位的方案则对放缩很敏感.

图 3 实验所用密图



掩图 叠加图

图 4 掩图叠加图

4.1 实验结果

4.2 健壮性分析

接下去,我们对于本文提出的方案的健壮性进行一些实验和说明:

(1) 掩图经过 jpg25 压缩.

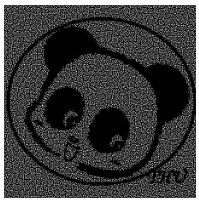


图 5 掩图经过 jpg25 压缩后恢复出来的叠加图

(2) 掩图存在一定程度的破损(左图是破损的掩图,右图是由破损的掩图旋转后得到叠加图中恢复出的图像).

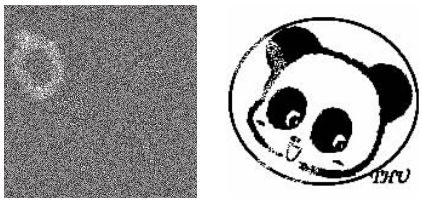


图 6 破损掩图的实验结果

(3) 放缩.

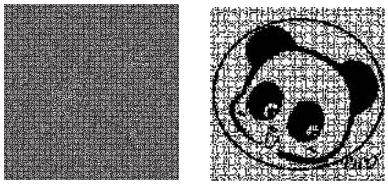


图 7 掩图经过缩小后的实验结果(左图是缩为 90% 的掩图,右图是由该掩图旋转后得到的叠加图中恢复出的图像)

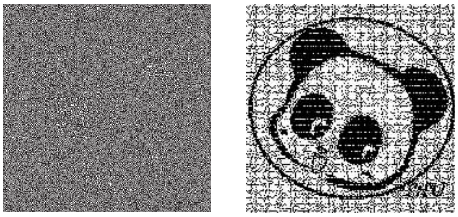


图 8 掩图经过放大后的实验结果(左图是放大为 120% 的掩图,右图是由该掩图旋转后得到的叠加图中恢复出的图像)

4.3 进一步的工作

在本文基础上,我们的进一步研究工作是:

(1) 在有意义的图片中隐藏信息.我们在这方面已经取得了一些阶段性成果,将继续改进和完善,并另撰文描述;

(2)改进成为正多边形的旋转,如正七边形,可旋转的角度增多,提高安全性.

参 考 文 献

[1] Naor M, Shamir A. Visual cryptography//Proceedings of the EUROCRYPT'94. LNCS 950. Berlin: Springer-Verlag, 1994: 1-12

[2] Droste S. New results on visual cryptography//Proceedings of the CRYPTO'96. LNCS 1109. Berlin: Springer-Verlag, 1996: 401-415

[3] Kobara K, Imai H. Limiting the visible space visual secret sharing schemes and their application to human identification//Proceedings of the ASISCRYPTO'96. LNCS 1163. Berlin: Springer-Verlag, 1996: 185-195

[4] Bieh I, Wetzel S. Traceable visual cryptography//Proceedings of the ICICS'97. LNCS 1334. Berlin: Springer-Verlag, 1997: 61-71

[5] Koga H, Yamamoto H. Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images. IEICE Transactions on Fundmentals, 1998, E81-A(6): 1262-1269

[6] Xia Guang-Sheng, Yang Yi-Xian. A new secret sharing scheme: Image covering. Journal of Beijing University of Posts and Telecommunications, 1999, 22(1): 57-61 (in Chinese)
(夏光升,杨义先. 一种新的密钥分享方案——叠像术. 北京邮电大学学报, 1999, 22(1): 57-61)

[7] Wang Dao-Shun, Yang Lu. Visual hiding scheme using one secret Image. Chinese Journal of Computers, 2000, 23(9): 943-948(in Chinese)
(王道顺,杨路. 图像的单幅可视隐藏方案. 计算机学报, 2000, 23(9): 943-948)

[8] Xia Guang-Sheng, Yuan Zhong-Lan, Yang Yi-Xian, Hu Zheng-Ming. A new visual cryptography algorithm to hide a two color image in a single shared image. Journal of Beijing University of Posts and Telecommunications, 2002, 25(3): 12-16(in Chinese)
(夏光升,袁中兰,杨义先,胡正名. 一种新的图像单幅可视隐藏算法. 北京邮电大学学报, 2002, 25(3): 12-16)

[9] Ateniese G, Blundo C, De Santis A et al. Constructions and bounds for visual cryptography//Proceedings of the ICALP'96. LNCS 1099. New York: Springer-Verlag, 1996: 416-428

[10] Ateniese G, Blundo C, De Santis A et al. Visual cryptography for general access structures. Information and Computation, 1996, 129(2): 86-106

LIU Duo, born in 1978, Ph. D., lecturer. His current research interests include network security, elliptic curve cryptology, combinational algorithm, etc.

DAI Yi-Qi, born in 1946, professor, Ph. D. supervisor. His main research interests are information security, network security, cryptology and combinational algorithm.

Background

Visual cryptography, which is invented by Naor & Shamir in 1994, is a method for securely encrypting messages in such a way that the recipient won't need a computer to decrypt them. The underlying cipher is essentially the one time pad; so the system is unbreakable in the information theoretical sense. Since then, many extensions and improvements of visual cryptography were proposed.

However these schemes need to stack at least two secret shares to recover the secret image. In the case that one share is deformed or is not be true to the original, the secret image is hard to recover. To overcome this disadvantage, some visual hiding schemes using one secret image were proposed.

This paper presents a new scheme on hiding a secret image into single shadow image. It can also be used as a technique of digital watermarking.

Differ from any existed methods of visual hiding schemes using one secret image, the new scheme based on the rotation of the shadow image. In the new scheme, the single shadow image acted both encoder and decoder function. Therefore the secret image can be recovered by stacking the shadow image and the shadow image after rotated 90 degree anticlockwise. The new method has the property of anti-compression, anti- distortion and anti-shrink. Furthermore, the new scheme can use the shadow image sufficiently.

This work was supported by the National Natural Science Foundation of China (grant No. 60673065)