基于空域可恢复信息隐藏的图像安全人工退化算法

雷正桥[1] 肖 迪[2]
(重庆工业职业技术学院教务处 重庆 401120)[1] (重庆大学计算机学院 重庆 400044)[2]

摘 要 为了满足数字图像先用后买的商务模式的需要,提出了一种基于空域可恢复信息隐藏的数字图像人工退化算法。该算法使用可恢复信息隐藏算法中的直方图平移技术来嵌入补偿矩阵,以达到最终恢复精确原始图像的目的。通过控制嵌入深度,可得到与原始图像相比有较大失真但又能获知主要信息的公开图像。在嵌入过程中采用置乱以及加密技术,使得入侵者在没有得到授权文件的情况下无法强行恢复出原始图像。实验结果表明,该算法既可以得到与原始图像相差较大的公开图像,又能在得到安全认可的情况下完整地恢复出原始图像。

关键词 图像人工退化,可恢复隐藏,控制因子,直方图平移,授权文件
中图法分类号 TP309.2 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.3.034

Artificial Image Security Degradation Algorithm Based on Invertible Information Hiding in Spatial Domain

LEI Zheng-qiao[1] XIAO Di[2]
(Academic Affairs Office, Chongqing Industry Polytechnic College, Chongqing 401120, China)[1]
(College of Computer Science, Chongqing University, Chongqing 400044, China)[2]

Abstract In order to meet the requirement of the digital image business model of try with option to buy, we proposed an artificial image security degradation algorithm based on invertible information hiding in spatial domain. The algorithm uses histogram shifting method of lossless hiding to embed the compensation matrix for recovering the original image precisely. By controlling the embedding depth, the algorithm can generate publishing image which has large distortion but also keeps the main information of the original image. The scrambling and encryption methods are used in the algorithm so that the invaders can not recover the original image correctly by brute-force method without authorized files. The experiment results demonstrate that the algorithm can not only obtain the publishing image which has big differences with the original one, but also recover the exact image when security permission is released.

Keywords Image artificial degradation, Lossless hiding, Control factor, Histogram shifting, Authorized files

为了适应数字图像先用后买的商务模式的需要,可以人为主动地造成图像视觉质量的退化以获得公开图像。虽然可以从公开图像中看出原始图像的一部分信息,但却无法获得原始图像的完整信息。当用户决定购买后,则需要申请授权文件(一般是密钥等),对公开图像进行提取解密,最终获得和原始图像相似的图像,从而实现互联网共享和商业赢利的双赢。在医学、军事等领域,要求图像能精确恢复,需要保证恢复的图像和原始图像之间完全相同。现有的思路主要是借助选择加密的原理来实现图像的人工退化,如文献[1]。而本文则提出另外一种思路,即利用特殊的信息隐藏方法,其不但可以实现图像人工退化的要求,而且还可以通过水印引入版权信息,实现在处理图像的同时恢复出无差别的原始图像。

目前,可恢复信息隐藏技术大致可分为两大类别:基于差分扩展的方法[2,3]和基于直方图平移的方法[4,5]。第一种方法适用性广,平均容量较高,但同样具有实现复杂、对图像破坏大和辅助信息大等缺点。第二种方法虽然在平均容量、局限性上都比不上第一种,但是其实现效率高,辅助信息小,特别是嵌入后对图像的破坏程度小。近年来,可恢复信息隐藏方法已有了进一步的发展[6,7]。考虑到图像人工退化所要用到的补偿矩阵往往都不是很庞大,本文在可恢复隐藏信息的算法上采取基于直方图平移的方法。

1 水印嵌入和图像退化

图像退化算法的水印嵌入过程分为两大步:首先将相应的水印信息有损地嵌入,然后以无损的方式嵌入加密后的补偿矩阵。第一步嵌入的是鲁棒水印[8,9],可以引入版权信息。水印嵌入和图像退化算法的流程如图1所示。

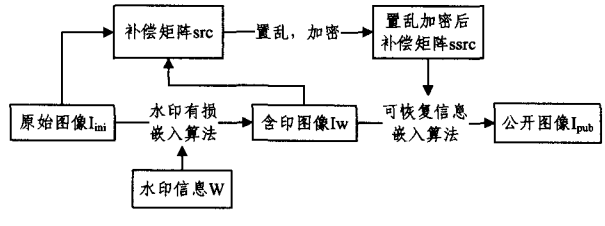

图1 水印嵌入和图像退化流程

1)水印信息 W 预处理:设待嵌水印为 $64*64$ 的二值图

到稿日期:2014-04-21 返修日期:2014-07-01 本文受应急通信重庆市重点实验室开放课题项目(CQKLEC,20140504)资助。
雷正桥(1973-),男,副教授,主要研究方向为网络安全技术,E-mail:leizhengq@163.com;肖 迪(1975-),男,教授,博士生导师,主要研究方向为信息安全技术。

像，将其用 Arnold 置乱进行 15 次置乱，如图 2 所示。Arnold 置乱变换即猫映射(Cat mapping)[10]，设图像为 $f(x,y)$，x 和 y 均属于$\{0,1,\cdots,N-1\}$范围，则置乱变换可表示为：

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N = C * \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \tag{1}$$

其中，a 和 b 均为正整数，x_n 和 y_n 表示变换前水平和垂直坐标的像素值，x_{n+1} 和 y_{n+1} 表示变换后的水平和垂直坐标的像素值。

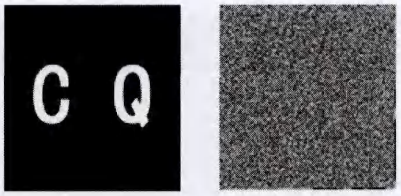

图 2　待嵌入的水印图像以及置乱后的水印图像

2)将被置乱的水印信息用简单的像素位替换的方式嵌入到原始宿主图像中。为了保证原始图像、最后得到的公开图像及恢复出来的图像之间的差距较大，引入控制因子 α 来控制水印图像的嵌入深度，α 越大则嵌入深度越深，图像失真得越严重。其过程可以用式(2)表示：

$$I_w = I_{ini}(1+\alpha W) \tag{2}$$

其中，I_{ini} 表示原始图像，I_w 表示得到的嵌有水印的图像。以 256 色灰度图为例，控制因子为 07，0 表示替换最低有效位，7 表示替换最高位，以此类推。

3)在得出嵌有水印的图像后，用补偿矩阵表示原始图像矩阵和水印图像矩阵的差值，如式(3)所示：

$$src = \| I_{ini} - I_w \| \tag{3}$$

如图 3 所示，补偿矩阵 src 的大小与图像一样。

$$\begin{bmatrix} 129 & 128 & \cdots & 136 \\ 133 & 129 & \cdots & 139 \\ \cdots & \cdots & \cdots & \cdots \\ 36 & 37 & \cdots & 36 \end{bmatrix} - \begin{bmatrix} 133 & 128 & \cdots & 136 \\ 129 & 133 & \cdots & 135 \\ \cdots & \cdots & \cdots & \cdots \\ 36 & 41 & \cdots & 36 \end{bmatrix} = \begin{bmatrix} -4 & 0 & \cdots & 0 \\ 4 & -4 & \cdots & 4 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & -4 & \cdots & 0 \end{bmatrix}$$

图 3　补偿矩阵 src 的产生过程

图中减号左、右两边的矩阵分别表示原始图像像素值和水印图像像素值。

4)补偿矩阵 src 的安全性直接决定了整个算法的安全性，因此需要对这个 src 矩阵进行 N 次置乱以及加密处理，获得一个新的加密后的补偿矩阵 $ssrc$，其计算过程如式(4)和式(5)所示。置乱的过程一般都需要是方阵，无论是否将图像进行分割，如果不是方阵，可通过末尾补 0 的方法组成一个方阵。

$$N_{src} = f_{scrambling}(src, N) \tag{4}$$

$$ssrc = E(src, K) \tag{5}$$

式中，N_{src} 表示置乱后的补偿矩阵，f 是置乱函数，当我们采用 Arnold 置乱算法进行置乱时，置乱次数为 N，加密函数是 E，密钥为 K。其中，N 和 K 组成了授权文件，只有已知 N 和 K，才可能恢复出补偿矩阵。同时，可利用 AES 加密算法作为加密方式。

5)在得到加密补偿矩阵之后，整个补偿矩阵被以可恢复信息隐藏的方法嵌入到已嵌有水印的图像之中，从而得到公开图像。加密后补偿矩阵按照从左到右、从上到下的扫描顺序转换成为一个一维的补偿矩阵向量，向量里面的数都被转换为二进制表示，从而得到一个比特流 L。这些二进制的比特流被以可逆的方式压缩为压缩过的比特流 L_{com}。采用直方图平移的可恢复信息隐藏方式，将压缩过的比特流作为负载嵌入到图像之中，根据图像的统计特征直方图，利用其统计图峰值的移动来嵌入信息。

如图 4 所示，对一幅图像的灰度值进行统计，灰度直方图的峰值出现在灰度值为 65 左右处，约 3000 个像素可以改灰度，图像的这一统计特征可被用于可恢复的信息嵌入：先在图像的灰度直方图中找出一个峰值点和一个零值点，若无特殊说明，峰值点都选统计图的最高点。如果在图像的统计直方图中找不到统计个数为 0 的像素值，也可任选一个个数较少的像素值，但此时则需将这个具体的像素值作为辅助信息的一部分和水印一起嵌入原始图像中。如图 4，选取的峰值点和零值点分别为 65 和 250 这两个像素点。在嵌入水印前，首先将选取出的峰值点和零点间的所有像素往零点方向移动一个灰度单位，这样峰值点的像素个数就变成了 0，如图 5 所示。

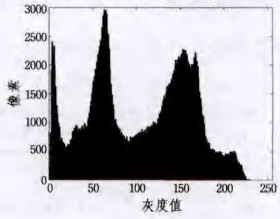

图 4　一幅图像的灰度直方图

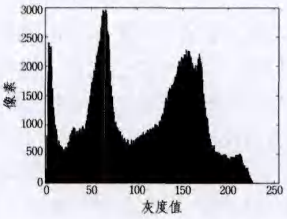

图 5　直方图平移效果

从图 5 可以看出，在峰值的位置出现一个空白槽，使用以下规则将水印嵌入到这个空槽之中：若水印位为'1'，则将移动后的峰值像素向空槽移动一位；若水印为'0'，则保持不变；在此过程中所需要的辅助信息(如峰值-零点对)，作为密钥予以保存。该方法简单快速，且容量相对较大，其容量等于峰值的个数，如果想要更大容量则可以采取多峰值-零点对或者多次嵌入的方式。为了增加容量，还可以对图像进行分块，然后统计出每一块的直方图信息，在每一块都进行直方图平移的水印嵌入方法，如图 6 所示。

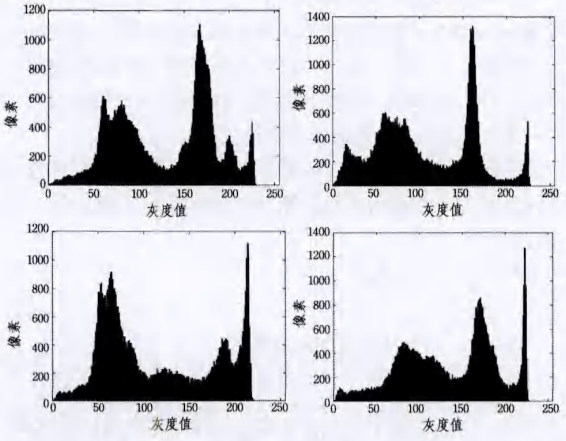

图 6　图像分为 4 块后的直方图

图 6 中，我们将图像分为 4 个部分以后，其峰值像素的个

数大约为两个 1100 加上两个 1300，即总峰值像素会有近 5000 个，远远超出了使用图像整体直方图的嵌入容量。

这一步的嵌入过程可以由下式表示：

$$L_{com}=Com(B(ssrc,8)) \tag{6}$$

$$I_{pub}=F(I_w,L_{com}) \tag{7}$$

在式(6)中，B 表示将加密后的补偿矩阵转化成为二进制流的函数，参数"8"表示将一个十六进制数用 8 位的二进制表示，Com 表示对的二进制流进行无损压缩，然后利用可恢复信息隐藏算法 F 得到公开图像 I_{pub}。

通过控制因子和两次嵌入过程，很容易使得最后得到的公开图像相对于原始图像有较大的差别；而在整个过程中公开图像都是根据原始图像得来的，所以又保证了公开图像和原始图像之间有很强的相关性。

2 水印提取和图像恢复

水印提取和图像恢复算法流程如图 7 所示。

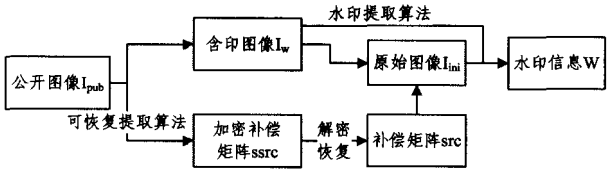

图 7 水印提取和图像恢复流程

在提取端，当用户获得公开图像之后，可以看到一个大概的图像，从而可以进一步确定是否对这个图像感兴趣。如果用户感兴趣，可以向添加水印的一方请求授权文件，在得到对方的同意后，对方将授权文件发送给用户，用户利用这个文件就可以将原始图像恢复出来并且能够得到水印信息。

如果在提取端的用户是试图对图像进行破坏的攻击者，那么在其得到公开图像之后，由于隐藏算法是公开的，攻击者可以提取出在公开图像中的加密补偿矩阵。但是由于这个补偿矩阵是加密处理过的，若攻击者强行使用水印图像加上这个补偿矩阵的方式对图像进行恢复，则肯定无法得到正确的图像；而且攻击者此时恢复的嵌有水印的图像失真度是较高的，所以这对于攻击者完全没有意义。

而对于一个合法的用户，在获得公开图像 I_{pub} 后，先使用直方图可恢复隐藏的提取算法提取出压缩后的密文状态的补偿矩阵 $ssrc$ 和嵌有水印的图像 I_w：

$$I_w,L_{com}=F'(I_{pub}) \tag{8}$$

$$ssrc=Hex(DeCom(L_{com}),8) \tag{9}$$

式(8)表示从公开图像中提取出嵌有水印的图像 I_w 和压缩后的比特流 L_{com}。式(9)表示在得到压缩比特流之后，使用解压缩算法 DeCom 恢复出原始比特流，然后将这些比特流以 8 位为一组转化成为十六进制的密文补偿矩阵 $ssrc$。

接着，利用解密函数 De、解密密钥 K 得到置乱后补偿矩阵 N_{src}，通过反向置乱恢复出原始补偿矩阵 src，如式(10)、式(11)所示。

$$N_{src}=De(ssrc,K') \tag{10}$$

$$src=F_{scrambling}(N_{src},N') \tag{11}$$

恢复 src 的具体流程如图 8 所示。

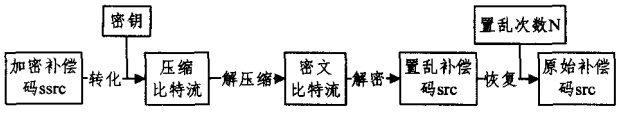

图 8 加密补偿矩阵 ssrc 恢复过程

在得到原始补偿矩阵 src 之后，将其与前面已经得出的嵌有水印的图像 I_w 相加，即可获取到原始的图像信息 I_{ini}，如式(12)所示。在得到了原始图像 I_{ini} 之后，通过比较原始图像 I_{ini} 和嵌有水印的图像 I_w，得到原始的水印 W。

$$I_{ini}=\| I_w+src \| \tag{12}$$

在处理过程中，在提取密文状态的补偿矩阵流时采用的是可恢复隐藏的算法，所以提取出的水印信息与得到的含水印的图像都是精确的。在对加密补偿矩阵流进行解压缩的过程中，因为使用的是无损压缩的方法，也就保证了解压缩得到的比特流的正确性。后续的解密和反向置乱步骤中都没有任何信息的损失。所以可以保证最终得到的原始图像准确无误。

3 实验结果

设实验图像为图 9 所示的 3 幅不同平滑度和纹理的512 * 512 的 256 灰度图，待嵌入的水印图像是 64 * 64 的二值图像，加密算法的密钥长度为 256bit，并使用分块直方图平移的可恢复信息隐藏算法嵌入加密后的补偿矩阵。本文中所有的实验程序都采用 C++语言和 OpenCV 库完成，并采用 OpenCV 绘图函数完成生成的统计图。算法中的授权文件(包括置乱次数 N、加密密钥 K)都以边信道的方式传送给接收端。

图 9 实验图像

峰值信噪比被用于评价最终图像的失真程度，如式(13)所示：

$$PSNR=10*\log(\frac{255^2}{MSE}) \tag{13}$$

其中，MSE 表示均方误差，最终图像和原始图像间的失真程度越大，则 $PSNR$ 值越小。

3.1 有损嵌入水印的效果实验

本文算法首先采用不同的控制因子嵌入置乱后的水印信息，在第一步的水印嵌入过程中，采用的是简单的像素位替换的方式。图 10 是实验获得的不同嵌入深度的含水印图像峰值信噪比折线图。

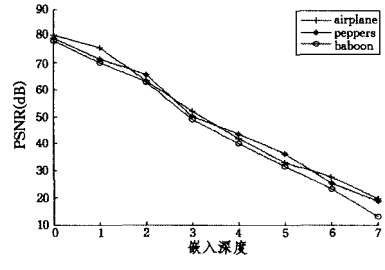

图 10 不同嵌入深度的含水印图像 I_w 峰值信噪比

从图 10 中可以看出，随着嵌入深度的加大，图像的峰值信噪比整体上呈现下降的趋势，当嵌入深度不大于 3 时，水印图像的 $PSNR$ 全部都在 40dB 以上，这也是传统水印的失真度要求。但是在图像人工退化的应用中，要求最后公开的图

像要和原始图像的失真度差距比较大，所以我们选择嵌入深度大于 3 的作为我们的控制因子。

3.2 可恢复嵌入补偿矩阵的实验

在嵌入了水印之后，下一步就需要计算出图像的补偿矩阵，按照式(3)分别计算出控制因子大于 3 的水印图像的补偿矩阵。由于本文算法采取的是简单的图像替换的方式，因此矩阵里面的元素不是 0 就是正负 2 的 α 次方，α 即控制因子。通过对这个矩阵进行置乱，再使用密钥对矩阵进行加密，从而完成对补偿矩阵的加密处理。接下来，使用无损压缩算法将这个补偿矩阵以二进制流的形式进行压缩，最后再将这个压缩后的加密补偿矩阵用直方图平移的方式可恢复地嵌入到图像中。

通过采用将水印图像分块进行直方图平移的方式，获得更大的容量，方法和整体直方图平移是完全相同的。使用直方图平移之后得到的公开图像如图 11 所示。

图 11 公开图像

如图 11 所示，在进行了直方图平移的可恢复信息嵌入之后，图像又有所失真。对比这 4 组图像，当嵌入深度为 4 和 5 时，公开图像仍然比较清晰，其效果与传统水印效果图像相似。当嵌入深度为 7 时，图像的内容已基本看不出来，很难从图中得出有意义的信息。所以，经过综合对比，嵌入深度为 6 比较符合图像人工退化的需求，也更有实际运用的价值。最终产生的公开图像峰值信噪比如图 12 所示。

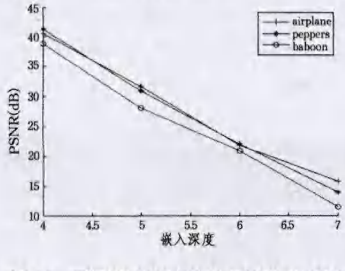

图 12 不同嵌入深度的公开图像 *PSNR*

根据人的视觉特点，*PSNR* 在 30dB 以上的公开图像可以呈现较为清晰的图像，在 40dB 以上的更是与原始图像相差不大。传统数字水印都要求最后的图像效果在 30dB 以上，而在人工退化应用中，一般取 *PSNR* 在 20dB 到 30dB 之间，图 12 中的结果也印证了上面选择控制因子的值为 6。

3.3 提取与恢复实验

通过对公共图像的提取，最终用户确认他们是否想要得到原始图像，如果确认希望看到原始图像，提取客户端可以请求有关的授权文件。根据获得的授权文件，首先使用可恢复隐藏的算法提取出含水印图像和加密后压缩补偿向量，进一步根据前文所述的提取算法提取出水印和原始图像。由于补偿矩阵是经过安全处理的，如果强行恢复，并不能获得正确有意义的原始图像。因此在没有授权文件的情况下，提取端很难获取正确的原始图像。图 13 和图 14 分别显示了从嵌入深度为 6 的那一组公开图像强行恢复和正确恢复的图像。

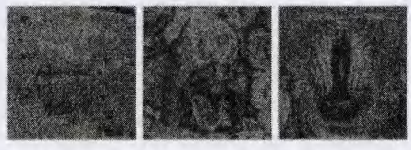

图 13 强行恢复的图像效果

图 14 正确恢复的图像效果

从图 13 可以看到，3 幅图像不仅与原始图像相差极大，而且效果还不如嵌有水印的图像，所以如果攻击者只是简单地使用补偿矩阵来恢复原始图像是完全行不通的。

对比图 13 和图 14 可以看到，如果用户得到授权，其恢复的图像是高清晰的，采用像素对比的方式可以发现它们与原始图像的像素是完全相同的。

3.4 水印嵌入容量分析

如前文所述，本图像退化算法的水印嵌入过程分为两次：第一次将相应的鲁棒水印信息有损地嵌入，第二次以无损的方式嵌入加密后的补偿矩阵。第一次嵌入的水印才是有效载荷，而第二次嵌入的是表示原始图像矩阵和水印图像矩阵的差值的补偿矩阵。所以，算法的水印嵌入容量应该主要考虑第一次的嵌入容量。在第一次嵌入时，算法引入了控制因子 α 来控制水印图像的嵌入深度，α 越大则嵌入深度越深，图像失真得越严重。根据前面的实验可知，嵌入深度为 6 即通过替换第 6 位来嵌入水印比较符合图像人工退化的需求，也更有实际运用的价值。此时，本算法的水印嵌入容量为 1bpp (Bit Per Pixel)。事实上，还可以根据需要同时替换第 5 到第 0 位来嵌入水印，这样水印的嵌入容量将成倍增加。

3.5 算法的安全性分析

如前文所述，补偿矩阵 *src* 的安全性直接决定了本算法的安全性。在算法中，补偿矩阵 *src* 进行了 N 次置乱以及加密处理。提取端的攻击者虽然可以提取出在公开图像中的密文态的补偿矩阵 *ssrc*，但无法得出解密的补偿矩阵 *src*。在第 3.3 节的实验中，我们已证明：攻击者若强行使用嵌有水印图

像加上密文态的补偿矩阵来对图像进行恢复，是无法得到正确的图像的。

结束语 本文基于空域可恢复信息隐藏，提出了一种可完整精确恢复原始图像的人工退化算法；利用控制因子实现了对嵌入深度的控制，使得嵌入端可以控制最后图像的失真程度；并且通过置乱、加密等安全措施，保证了只有合法的接收端可以获得正确的原始图像。

参 考 文 献

[1] 赵亮，廖晓峰，向涛，等. 基于Z矩阵映射和选择加密的彩色图像退化算法研究[J]. 物理学报，2010，59(3)：1507-1523

[2] Huang H-C, Chang F-C, Fang W-C. Reversible Data Hiding with Histogram-Based Difference Expansion for QR code Application[J]. IEEE Transactions on Consumer Electronics，2010，57(7)：779-787

[3] Wang J X, LU Z M. A Path Optional Lossless Data Hiding Scheme Based on VQ Joint Neighboring Coding[J]. Information Sciences，2009，19(9)：3332-3348

[4] Jung S W，Ha L T，Ko S J. A new histogram modification based reversible data hiding algorithm considering the human visual system[J]. IEEE Signal Processing Letters，2011，18(2)：721-724

[5] Lin C C，Tai W L，Chang C C. Multilevel Reversible Data Hiding Based on Histogram Modification of difference images[J]. Pattern Recognition，2009，41(12)：3582-3591

[6] 柳玲，陈同孝，曹晨，等. 一种随机嵌入抗SPAM检测的可逆数据隐藏算法[J]. 计算机应用研究，2013，30(7)：2111-2114

[7] 邱应强. 一种大嵌入容量的可逆数据隐藏方法[J]. 计算机应用研究，2014，31(3)：850-852

[8] Deng C, Gao X B, Li X L, et al. A local Tchebichef moments-based robust image watermarking[J]. Signal Processing，2009，89(8)：1531-1539

[9] Gao X-B，Deng C，et al. Geometric distortion insensitive image watermarking in affine covariant regions[J]. IEEE Transactions on System，Man and Cybernetics，2010，40(3)：278-286

[10] 肖旭韬，张雪锋. 基于线性反馈移位寄存器和组合猫映射的伪随机序列生成方法[J]. 计算机应用研究，2013，30(1)：161-164

(上接第135页)

[4] Tso R, Okamoto T, Okamoto E. Practical Strong Designated Verifier Signature Schemes Based on Double Discrete Logarithms[C]// CISC 2005. LNCS 3822，Berlin：Springer-Verlag，2005：113-127

[5] Huang Q, Yang G M, Wong D S, et al. Efficient Strong Designated Verifier Signature Schemes without Random Oracle or with Non-delegatability [J]. International Journal of Information Security，2011，10(6)：373-385

[6] Susilo W, Zhang F, Mu Y. Identity-based Strong Designated Verifier Signature Schemes [C]// Proceedings of the ACISP 2004. LNCS 3108，Berlin：Springer-Verlag，2004：313-324

[7] Huang X，Susilo W，Mu Y，et al. Short (Identity-Based) Strong Designated Verifier Signature Schemes [C]// Proceedings of the ISPEC 2006. LNCS 3903，Berlin：Springer-Verlag，2006：214-225

[8] 王晓峰，张璟，王尚平，等. 新的基于身份的广义指定验证者签名方案[J]. 电子学报，2007，35(8)：1432-1436

[9] Zhang Jian-hong. A Novel ID-based Designated Verifier Signature Scheme [J]. Information Science，2008，178(3)：766-773

[10] Yang Bo，Xiao Zi-bi，Hu Zheng-ming. A Secure ID-Based Strong Designated Verifier Signature Scheme [C]// Proceedings of the IC-NIDC 2009. IEEE，2009：543-547

[11] Kang Bao-yuan. A Novel Identity-based Strong Designated Verifier Signature Scheme [J]. Journal of Systems and Software，2009，82(2)：270-273

[12] 张学军. 高效的基于身份的指定验证者签名[J]. 计算机工程，2009，35(5)：131-132

[13] 邵健，曹珍富，魏立斐. 基于身份的强指定验证者签名方案 [J]. 计算机工程，2010，36(8)：167-169

[14] Huang X，Susilo W，Mu Y，et al. Certificateless Designated Verifier Signature Schemes[C]// Proceedings of the 20th International Conference on Advanced Information Networking and Applications 2006. IEEE，2006：15-19

[15] Chen Hu，Song Ru-shun，Zhang Fu-tai，et al. An Efficient Certificateless Short Designated Verifier Signature Scheme [C]// Proceedings of the Wireless Communications，Networking and Mobile Computing 2008. IEEE，2008：1-6

[16] Yang Bo，Hu Zheng-ming，Xiao Zi-bi. Efficient Certificateless Strong Designated Verifier Signature Scheme [C]// 2009 International Conference on Computational Intelligence and Security. IEEE，2009：432-436

[17] Ming Yang，Shen Xiao-qin，Wang Yu-min. Certificateless Universal Designated Verifier Signature Schemes [J]. The Journal of China Universities of Posts and Telecommunications，2007，14(3)：85-94

[18] 韩亚宁，王彩芬. 无证书的广义指定多个验证者签名体制 [J]. 计算机应用研究，2009，26(6)：2158-2161

[19] Miyaji A，Nakabayashi M，Takano S. New Explicit Conditions of Elliptic Curve Traces for FR-reduction [J]. IEICE Trans. on Fundamentals，2002，E85-A(2)：481-484

[20] Koblitz N，Menezes A. Pairing-based Cryptography at High Security Levels [C]// Cryptography and Coding' 2005. Berlin：Springer-Verlag，2005：13-36

[21] Chatterjee S，Hankerson D，Knapp E，et al. Comparing Two Pairing-based Aggregate Signature Schemes [J]. Designs，Codes and Cryptography，2010，55(2/3)：141-167

[22] Li Ji-guo，Teng Hui-yun，Huang Xin-yi，et al. A Forward-Secure Certificate-Based Signature Scheme in the Standand Model[J]. The Computer Journal，2012，7672：362-376

[23] Li Ji-guo，Du Hai-ting，Zhang Yi-chen，et al. Provably Secure Certificate-based Key-Insulated Signature Scheme[J]. Concurrency and Computation Practice and Experience，2014，26：1546-1560

[24] Naor M，Segev G. Public-key Cryptosystems Resilient to Key Leakage [J]. SIAM J. Comput，2010，41(4)：772-814