文章编号 1004-924X(2017)11-2968-07

融合量子密钥真随机性的二值图像水印

吴佳楠[1,2],王世刚[1*],张 迪[2],刘桂霞[3],周 柚[3]

(1.吉林大学 通信工程学院,吉林 长春 130022;
2.长春大学 计算机科学技术学院,吉林 长春 130021;
3.吉林大学 计算机科学与技术学院,吉林 长春 130022.)

摘要:目前多数水印算法将伪随机数列作为水印,算法设计时多偏重于提高水印隐蔽性和鲁棒性,但忽略了水印自身的安全。本文提出了一种基于量子密钥真随机性的,可进行篡改定位的、面向安全通信的空域水印算法来提高水印的安全性。该算法使用基于 BB84 协议原理、通过量子密钥分发机制生成的具有真随机性和绝对安全性的量子密钥制备二值图像水印,并结合首次提出的量子密钥矩阵模型与 8-邻域随机定位理念,将量子水印动态随机地嵌入到载体图像中。传输完成后,接收方可以快速提取水印信息,精确判断水印图像完整性及传输过程安全性,并能够对篡改进行定位。对算法进行了隐蔽性、鲁棒性以及篡改定位测试,结果表明:提出的算法简单,具有高安全性和隐蔽性,同时兼顾鲁棒性,篡改定位精度达 3 pixel×3 pixel,可以广泛应用于数字图像的安全传输中。

关 键 词:数字水印;二值图像;图像融合;量子密钥;随机性

中图分类号:TP391.4 **文献标识码**:A **doi**:10.3788/OPE.20172511.2968

Binary image watermark fusionbased on quantum key true randomness

WU Jia-nan [1,2], WANG Shi-gang [1*], ZHANG Di[2], LIU Gui-xia[3], ZHOU You[3]

(1. *College of Communication Engineering, Jilin University, Changchun* 130022, *China*;
2. *College of Computer Science and Technology, Changchun University, Changchun* 130021, *China*;
3. *College of Computer Science and Technology, Jilin University, Changchun* 130022, *China*)
* *Corresponding author, E-mail: wangshigang@vip.sina.com*

Abstract: Current watermarking algorithms use mostly pseudo random sequences to generate watermarks. These algorithms emphasize the improvement of imperceptibility and robustness of the watermarking but ignores its safety. To improve the watermarking safety, a new secure communication oriented airspace watermarking algorithm with a tamper locating function was proposed based on the true randomness of quantum key. According to the principle of BB84 protocol, the quantum key with real randomness and absolute security generated by quantum key distribution mechanism was used to generate binary image watermarks. Then, in combining with a quantum key matrix model and 8-neighborhood random location idea, the quantum watermarks were embed into a

收稿日期:2017-05-23;**修订日期**:2017-07-15.

基金项目:国家自然科学基金重点资助项目(No. 61631009);国家自然科学基金资助项目(No. 61373051);教育部春晖计划资助项目(No. Z2015024);吉林省科技发展基金资助项目(No. 20150204006,20160101259JC,20170204023GX);吉林省省级经济结构战略调整引导资金专项资助项目(No. 2015y040)

carrier image dynamically and randomly. At the end of the transmission, the receiver could quickly extract watermark information, accurately judge the integrity of the watermark image and the security of the transmission process, and could perform tamper localization. The concealment, robustness and tamper location of the algorithm were tested. The experimental results show that the algorithm is simple, safe, and has higher safety and covert and its tamper locating accuracy is 3 pixel×3 pixel. The algorithm can be widely used in the secure transmission of digital images.

Key words: digital watermark; binary image; quantum key; randomness

1　引　言

在利用计算机网络传输多媒体数字化信息过程中存在着诸如对信息的恶意攻击及非法复制等安全隐患，这主要源于网络信道安全和信息自身安全两方面的因素。数字水印技术通过在被保护的数字对象中嵌入不可见信息来证明其版权归属，确保信息自身安全[1]。

数字水印算法基于域的不同可以分为空域算法和变换域算法。空域算法中最为典型的是 L. F. Turner[2] 于 1994 年提出的最低有效位算法(Least Significant Bits，LSB)，通过修改原始数据中的最低有效位来实现水印嵌入，该算法操作简单、隐蔽性好，但抗攻击性能较差；变换域算法通过改变变换系数(如颜色、纹理、频域)来嵌入水印。如 Cox 等[3-4] 在 1995 年提出的将水印嵌入到原始图像的离散余弦变换(Discrete Cosine Transform，DCT)域中，具有较好的抗压缩、抗几何攻击能力，但算法采用伪随机序列替换原始图像中的 DCT 系数，使得该算法在安全性上存在一定的隐患；1999 年 Ruanaida 等人[5] 采用离散傅里叶变换控制水印的嵌入量，提出了一种新的将数字水印嵌入到原始图像的离散傅立叶变换(Discrete Fourier Transform，DFT)域中的算法，从通信理论角度证明了相位调制更适合鲁棒性水印，但是傅里叶变换无法完成信号的时域分析，且处理效率低；随后 Kunder 等[6] 提出了一种将水印嵌入到图像离散小波变换(Discrete Wavelet Transform，DWT)域中的方法，通过平移、伸缩等方法解决了傅里叶算法的许多瓶颈问题。变换域算法普遍具有较高的鲁棒性，但算法相对复杂[7]。

目前，多数方法已很好地解决了数字水印算法自身的鲁棒性和隐蔽性，但就如何保证通信信息的安全性及正确性的研究相对较少[8]。很多方法通常采用伪随机数列作为水印，试图保证其安全性和稳健性[8-9]；另外，多数结合空间域和变换域的数字水印算法利用视觉掩模来选择嵌入位置，但由于水印复杂度低、不利于通信保密，故采用伪随机数控制水印的嵌入位置，以增强水印的保密性[10]。另外，数字水印技术需要解决的一项核心问题是鉴别数字图像的真实性，即对图像进行篡改检测和篡改定位[11-13]，并由此推断出图像被篡改的程度和方式[14-17]。通过对现有高安全性水印算法的研究发现，普遍存在定位精度不高的问题，算法的篡改定位精度一般为 8×8 个像素。

通过上述分析，本文结合量子保密通信技术提出了一种新的基于量子密钥真随机性的，可进行篡改定位的空域水印随机嵌入算法。通过量子密钥分发(Quantum Key Distribution，QKD)技术使通信双方获得了绝对安全且具有真随机性的量子密钥作为水印数据源，结合量子密钥矩阵模型与 8-邻域随机定位理念，将量子水印动态随机地嵌入到载体图像中，使水印信息的嵌入位置具有极高的不定性，除非获得正确的密钥序列，否则几乎没有提取出水印信息的可能，极大地提升了水印自身的安全性；算法同时实现了精度为 3×3 个像素的图像篡改检测及定位功能；在兼顾了鲁棒性的基础上，基于空域算法最低位嵌入的理念使得水印具有更为出色的隐蔽性。

2　基本概念

2.1　8-邻域像素

载体图像中像素的相邻关系如图 1 所示。可选嵌入中心像素 C 与它周围的像素组成一个邻域，上下左右的 4 个像素点为 4 邻域，对角上的 4 个像素点为对角邻域，8 个像素点合为一个8-邻域。

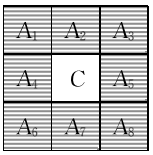

图 1　中心像素及 8-邻域

Fig. 1　Central pixels and 8-neighborhood

2.2　密钥矩阵

定义 1：密钥矩阵 Matrix$\boldsymbol{Q}_{ij}$，用于存贮量子密钥及相关嵌入度量参数。其中：$\boldsymbol{Q}_{ij}$ 为 1 bit 量子密钥（$j=6$，$i=n$），n 值大小根据载体图像像素确定。数据存储格式如图 2 所示。

Q_1	Q_2	Q_3			
D_1	D_2	D_3	D_4	D_5	D_6
Q_{11}	Q_{12}	Q_{13}	Q_{14}	Q_{15}	Q_{16}
…	…	…	…	…	…
Q_{n1}	Q_{n2}	Q_{n3}	Q_{n4}	Q_{n5}	Q_{n6}

图 2　密钥矩阵存储格式

Fig. 2　Key matrix storage format

定义 2：像素最低位嵌入值 Q_1 族，即嵌入像素点最低有效位的数值。

定义 3：嵌入选择参数 Q_2 族，用于决定 Q_1 族的嵌入位置。当 $D_2=0$ 时，嵌入位置为中心像素 C；当 $D_2=1$ 时，嵌入位置由 Q_3 族决定。

定义 4：水印嵌入坐标 Q_3 族，当 D_3 为 1（0）时，则以 A_1（A_2）为起点逆（顺）时针计算水印嵌入像素点在 8-邻域中的位置。其中，为避免逆时针与顺时针时个别像素点的位置重合，顺时针时以 A_2 为起点，逆时针时以 A_1 为起点。位置由 D_4、D_5、D_6 所组成的 3 bit 位二进制数决定，其中（000）代表起点，依次递增置位。例如：（1010）对应的水印嵌入的像素点是 A_6。

3　水印的生成

3.1　量子密钥

基于量子力学而衍生的量子保密通信技术采用量子态来编码通信双方之间的密钥，根据海森堡不确定性原理和量子不可复制定理，在理论上实现了通信密钥的绝对安全。本项研究采用量子密钥作为编码数据，创建水印图像。量子密钥的制备主要基于 Bennett 与 Brassard 提出的 BB84 协议[18]原理，通过 QKD 机制生成具有真随机性的量子安全密钥。方法如下：

步骤 1：通信双方 Alice 和 Bob 通过相关协议进行身份认证；

步骤 2：发送方 Alice 制备一系列的光子发送给接收方 Bob，每个光子的偏振态独立随机地选取；

步骤 3：接收方 Bob 随机选取＋基和×基测量 Alice 发送过来的光子偏振态，记录测量到的光子位置信息；

步骤 4：Alice 和 Bob 进行基矢比对，保留相同基测量的偏振态信息；

步骤 5：Alice 和 Bob 将保留的光子偏振态信息转换成相应的密钥比特信息；

步骤 6：Alice 和 Bob 通过经典信道对密钥比特进行纠错和私密放大，生成安全密钥，即具有真随机性的量子密钥；

步骤 7：结合密钥矩阵相关定义，在 Alice 端和 Bob 端分别生成量子密钥矩阵 Matrix$\boldsymbol{QA}$ 和 Matrix$\boldsymbol{QB}$，且 Matrix$\boldsymbol{QA}$=Matrix$\boldsymbol{QB}$。

3.2　量子水印

本文将量子密钥作为水印图像的数据源，创建并生成量子水印二值图。设输出二值图像函数为 $h(x,y)$，i 为密钥矩阵对应的行号，则有：

$$h(x,y)=\begin{cases}0,(Q_{i1}=0)\\1,(Q_{i1}=1)\end{cases}. \tag{1}$$

本文基于量子密钥矩阵元素信息生成的量子水印二值图像如图 3 所示。

图 3　量子水印二值图

Fig. 3　Binary image of quantum watermark

4　水印的嵌入与提取

4.1　水印的嵌入

Alice 端：基于 Matrix$\boldsymbol{QA}$ 嵌入水印步骤如下：

步骤 1：将原始载体图像以左上角为起点划分为 n 个互不重叠的 8-邻域，不足则丢弃；

步骤 2：生成量子密钥矩阵 Matrix$\boldsymbol{Q}_{ij}$；

步骤 3：读取 $D2$，若为 1，则用 $D1$ 替换根据 $Q3$ 族的各项参数决定的水印嵌入像素的最低有效位；若为 0，则替换中心像素的最低有效位；

步骤 4：步骤 3 重复 n 次后，输出嵌入了量子水印的载体图像。

4.2　水印的提取

Bob 端：基于 Matrix$\boldsymbol{QB}$ 提取量子水印步骤如下：

步骤 1：将接收到的载体图像（M× N）以左上角为起点划分为 n 个互不重叠的 8-邻域，不足则丢弃；

步骤 2：设 $p=\dfrac{M-M\%3}{3}$、$q=\dfrac{N-N\%3}{N}$，创建矩阵 Matrix$\boldsymbol{R}_{pq}$；

步骤 3：将 Matrix$\boldsymbol{R}_{pq}$的每个元素按照从左至右、从上至下的顺序与 n 个互不重叠的 8-邻域从左至右、从上至下进行关系匹配；

步骤 4：从 Matrix$\boldsymbol{QB}$ 中读取 D_2：若为 1，则结合定义 4 计算水印嵌入的像素位，并提取该像素的最低有效位值；若为 0，则提取中心像素的最低有效位值；

步骤 5：步骤 4 重复 n 次后，将提取的数值存入 Matrix$\boldsymbol{R}_{pq}$；

步骤 6：根据 Matrix$\boldsymbol{R}_{pq}$生成水印图像。

4.3　完整性验证及篡改定位

本文一项重要创新性工作，可以结合量子密钥矩阵精准验证水印图像的自身完整性，进而判断载体图像在传输过程中的安全性，并对载体图像进行较为准确地篡改定位，精度为 3×3 个像素。

4.3.1　完整性验证

步骤 1：根据 Matrix$\boldsymbol{QB}$ 的 D_2、D_3 从接收到的图像中提取水印信息 D_1^w；

步骤 2：将 D_1^w 与 Matrix$\boldsymbol{QB}$ 的 D_1 进行比对。设 v 为 D_1^w 与 D_1 吻合的个数，u 为 $Matrix$QB 中 D_1 的总个数，则吻合度 k 的表达式如下；

$$k=\frac{v}{u}. \tag{2}$$

步骤 3：若 $k=1$，则说明水印图像完整；若 $k<1$，可以判定载体图像已被篡改，即可对载体图像进行篡改定位。

4.3.2　篡改定位

步骤 4：创建一幅与接收图像等大的各像素点均为 1 的检测二值图（Detection Binary Image，DBI）；

步骤 5：对照 D_1^w 与 D_1，标记不匹配项，同时将 DBI 中对应的像素值置 0；

步骤 6：当所有的记录的像素点都比对完成时，生成攻击区域轮廓。

5　实验结果及分析

为了验证数字水印的好坏，本文结合隐蔽性和鲁棒性两个最基本特性对水印进行检测与分析。

5.1　隐蔽性测试

水印的隐蔽性可以采用峰值信噪比（PSNR）来衡量[19]。PSNR 越大，图像的质量保持得就越好，水印信息嵌入后对载体图像的影响越小，也就是隐蔽性越好。给定一幅大小为 $M\times N$ 像素的原始图像 $f(x,y)$和经过处理的图像 $g(x,y)$，图像 $g(x,y)$的 PSNR 可表示为

$$PSNR=10\times\lg\left(\frac{2^n-1}{\sqrt{MSE}}\right), \tag{3}$$

其中 MSE 的表达式为：

$$MSE=\frac{1}{M\times N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[g(x,y)-f(x,y)]^2. \tag{4}$$

实验中利用 34×34 pixel 的二值量子水印图像，分别对 102×102 pixel 的 Lena、Barbara 和 Baboon 3 个原始载体图像进行量子水印的加密与提取，实验结果如图 4 所示。可以看出嵌入水印后的图像视觉上与原始载体图像无明显差异。为了客观衡量水印隐蔽性，本文利用公式(1)计算了嵌入水印后 3 幅图像的 PSNR，如表 1 所示，结果均在 60.5 dB 左右，表明本加密算法具有较高的水印隐蔽性。为了进一步展现本方案的优越

性，将本文算法与空域算法中隐蔽性很好的 LSB 算法[2]以及 DCT[3]、DWT[6]、两种经典变换域算法进行了比较分析。表 1 给出了几种算法水印加密后 3 幅原始载体图像的 PSNR 值。LSB 算法加密后的 PSNR 均在 50.1 dB 左右，明显高于 3 种变换域算法。而本文算法 PSNR 高于 LSB 算法近 10 dB，说明本文算法具有极高的隐蔽性。

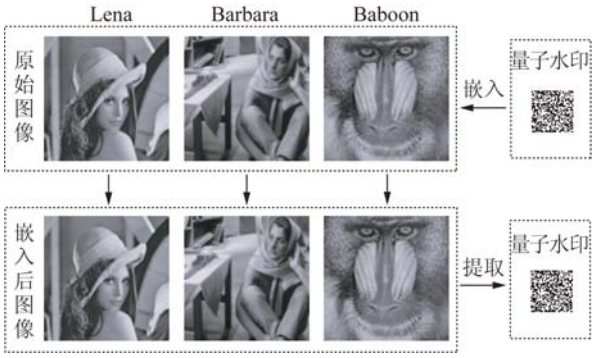

图 4　水印嵌入实验效果图

Fig. 4　Experimental results of watermark embedding

表 1　实验得出的 PSNR 值

Tab. 1　Experimentally obtained PSNR values (dB)

算法	Lena	Barbara	Baboon
本文	60.456 6	60.653 6	60.499 6
LSB	51.202 5	51.087 2	51.158 7
DCT	41.874 0	42.452 0	41.168 8
DWT	38.128 6	38.122 3	38.122 4

5.2　鲁棒性测试

水印的鲁棒性一般用相似系数(NC)来衡量，即计算原始水印和经过攻击后提取出的水印的相似系数。NC 的值越大，说明水印的鲁棒性就越好，抗攻击的能力就越强。给定一幅大小为 $M\times N$ 的原始载体图像 $f(i,j)$ 和嵌入水印后的图像 $g(x,y)$，则水印的相似系数为：

$$\mathrm{NC}=\frac{\sum_{i=1}^{N-1}\sum_{j=1}^{M-1}f(i,j)\,g(x,y)}{\sqrt{\sum_{i=1}^{N-1}\sum_{j=1}^{M-1}f^{2}(i,j)}\sqrt{\sum_{i=1}^{N-1}\sum_{j=1}^{M-1}g(x,y)}}. \quad (5)$$

为了验证本文算法的鲁棒性，对嵌入水印后的 Lena 图像分别进行了噪声和滤波两种攻击，并且通过计算得到提取水印与原始水印的 NC 值，如表 2 所示。本文算法与同样基于空域算法理念的 LSB[2]算法具有相近的抗噪性能。

表 2　水印鲁棒性检测结果

Tab. 2　Test results of watermark robustness

攻击算法	均值滤波	中值滤波	泊松噪声	高斯噪声 2%	高斯噪声 5%
本文	0.548 6	0.652 1	0.505 9	0.513 9	0.502 6
LSB	0.526 4	0.675 5	0.528 2	0.493 6	0.480 3

为了进一步验证算法的抗噪性能，选取 0.02，0.04，0.06，0.1，0.2 和 0.3 dB 的噪声对含水印图像分别进行了 10 次椒盐噪声攻击实验，得到 NC、PSNR 最大值 Max、最小值 Min 和平均值 Avg，如表 3 所示。同时截取了 NC 最大值时的 6 幅检测图像，如图 5 所示。由图像信息及实验数据可知，噪声越大，图像和水印的质量受影响越大。从实验结果可以看出，本文算法对于椒盐噪声攻击表现出了优越的抗噪性能，噪声低于 0.1 dB 时，NC 值处于 0.97 左右，与一些抗攻击性很好的变换域方法[20]具有相近的鲁棒性。

表 3　椒盐噪声检测结果

Tab. 3　Test results of salt and pepper noise (dB)

椒盐噪声		0.02	0.04	0.06	0.1	0.2	0.3
NC	Max	0.992 2	0.988 8	0.977 4	0.965 9	0.906 1	0.857 3
	Min	0.985 3	0.974 9	0.964 6	0.934 3	0.881 4	0.832 1
	Avg	0.989 5	0.980 3	0.971 1	0.950 9	0.895 8	0.847 2
PSNR	Max	23.258	19.881	17.910	15.816	12.665	10.814
	Min	22.200	18.978	17.380	15.265	12.373	10.568
	Avg	22.664	19.423	17.673	15.571	12.499	10.716

图 5　椒盐噪声实验

Fig. 5　Salt and pepper noise experiment

5.3　攻击篡改定位

为了验证本文算法对部分水印信息遭到篡改时的定位准确性，对图 1 中 3 幅嵌入水印图像分别在不同位置进行了可见（用实框圈出）与不可见（用虚框圈出）篡改攻击。

图 6　篡改定位示意图

Fig. 6　Sketch map of tamper location

如图 6 第一行篡改攻击图像所示，Lena 的攻击范围为 65～85 行与 65～85 列的可见方形区域与 10～30 行与 10～30 列的不可见方形区域；Barbara 的攻击范围为20～40 行与 20～40 列的可见方形区域与 75～95 行与 75～95 列的不可见方形区域；Baboon 的攻击范围为 50～70 行与 50～70 列的可见方形区域与 80～100 行与 80～100 列的不可见方形区域。运用 4.3 节中攻击篡改定位方法，得到图 6 第 2 行攻击范围定位结果图，算法对 3 种不同图像、不同位置攻击均可进行攻击定位，另外对可见与不可见篡改攻击区域的定位同样有效，由此证明了本文方法对攻击篡改定位的灵活性与有效性。

6　结　论

本文针对目前多数水印算法自身安全性较差的问题，提出了一种新的基于量子密钥真随机性的水印嵌入、提取及篡改定位算法。该算法基于 BB84 协议原理，通过量子密钥分发机制生成具有真随机性的量子安全密钥作为制备二值图像水印的数据源；同时结合首次提出的量子密钥矩阵模型与 8-邻域随机定位理念，将量子水印动态随机的嵌入到载体图像中；传输后能够精确的判断水印图像自身完整性、进而推断传输过程的安全性并能够进行较为准确的篡改定位。实验结果表明：算法简单，具有高安全性和隐蔽性，同时兼顾鲁棒性。

随着网络多媒体数字化信息的快速发展，本文研究工作将推动数字水印技术、数据隐藏技术和数据加密技术走向更深层次的融合。

参考文献：

[1] WOLFGANG R B, PODILCHUK C I, DELP E J. Perceptual watermarks for digital images and video [J]. *Proceedings of the IEEE*, 1999, 87(7):1108-1126.

[2] VAN SCHYNDEL R G, TIRKEL A Z, OSBORNE C F. A digital watermark[C]. *Proceedings of the 1st International Conference on Image Processing*, *IEEE*, 1994(2):86-90.

[3] COX I J, KILIAN J, LEIGHTON T, *et al*.. Secure spread spectrum watermarking for images, audio and video[C]. *Proceedings of the 3rd IEEE International Conference on Image Processing*, *IEEE*, 1996:243-246.

[4] COX I J, KILIAN J, LEIGHTON F T, *et al*.. Secure spread spectrum watermarking for multimedia [J]. *IEEE Transactions on Image Processing*, 1997, 6(12):1673-1687.

[5] RUANAIDH J J K O, DOWLING W J, BOLAND F M. Phase watermarking of digital images[C]. *Proceedings of the 3rd IEEE International Conference on Image Processing*, *IEEE*, 1999, 3:239-242.

[6] KUNDUR D, HATZINAKOS D. A robust digital image watermarking method using wavelet-based fusion[C]. *Proceedings of International Conference on Image Processing*, *IEEE*, 1997:544-547.

[7] 赵博，秦贵和. 高鲁棒性的图像水印算法[J]. 吉林大学学报(工学版)，2017，47(1):249-254.
ZHAO B, QIN G H. High robustness image watermarking algorithm[J]. *Journal of Jilin University (Engineering and Technology Edition)*, 2017, 47(1):249-254. (in Chinese)

[8] 郑秋梅，金萧，顾国民，等. 一种基于 Data Matrix 的数字水印算法[J]. 中国石油大学学报(自然科学版)，2015，39(1):188-193.
ZHENG Q M, JIN X, GU G M, *et al*.. A digital

watermarking algorithm based on Data Matrix[J]. *Journal of China University of Petroleum*, 2015, 39(1):188-193. (in Chinese)

[9] 王沛，姚恒，李莉. 结合图像空间域和小波域特性的自适应盲水印算法[J]. 光学 精密工程，2006，14(6):1057-1062.
WANG P, YAO H, LI L. A adaptive digital watermarking algorithm combining spatial and DWT domain[J]. *Opt. Precision Eng.*, 2006, 14(6):1057-1062. (in Chinese)

[10] LOUKHAOUKHA K, NABTI M, ZEBBICHE K. A robust SVD-based image watermarking using a multi-objective particle swarm optimization[J]. *Opto-Electronics Review*, 2014, 22(1):45-54.

[11] QI X J, XIN X. A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization[J]. *Journal of Visual Communication and Image Representation*, 2015, 30:312-327.

[12] SUTHAHARAN S. Fragile image watermarking using a gradient image for improved localization and security[J]. *Pattern Recognition Letters*, 2004, 25(16):1893-1903.

[13] HE H J, ZHANG J SH, TAI H M. A secure fragile watermarking scheme for image authentication[C]. *Proceedings of 2006 International Conference on Computational Intelligence and Security*, IEEE, 2006:1180-1185.

[14] KUNDUR D, HATZINAKOS D. Digital watermarking for telltale tamper proofing and authentication[J]. *Proceedings of the IEEE*, 1999, 87(7):1167-1180.

[15] FRIDRICH J, GOLJAN M. Images with self-correcting capabilities[C]. *Proceedings of 1999 International Conference on Image Processing*, IEEE, 1999:792-796.

[16] LIN P L, HUANG P W, PENG A W. A fragile watermarking scheme for image authentication with localization and recovery[C]. *Proceedings of the 6th International Symposium on Multimedia Software Engineering*, IEEE, 2004:146-153.

[17] 王定成，田翠翠，陈北京，等. 基于四维四元数频域的彩色图像双重水印算法[J]. 吉林大学学报(工学版)，2015，45(4):1336-1346.
WANG D CH, TIAN C C, CHEN B J, *et al.*. Dual watermarking for color images based on 4D quaternion frequency domain[J]. *Journal of Jilin University (Engineering and Technology Edition)*, 2015, 45(4):1336-1346. (in Chinese)

[18] BENNETT C H, BRASSARD G. Quantum cryptography: public key distribution and coin tossing[C]. *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, IEEE, 1984.

[19] 王玉海，朱长青，苏守宝，等. 结合感知哈希与数字水印的遥感影像认证方法[J]. 光学 精密工程，2016，24(10):640-648.
WANG Y H, ZHU CH Q, SU SH B, *et al.*. An authentication method based on perceptual hashing and watermarking for remote sensing image[J]. *Opt. Precision Eng.*, 2016, 24(10):640-648. (in Chinese)

[20] SINGH A K, DAVE M, MOHAN A. Hybrid technique for robust and imperceptible image watermarking in DWT-DCT-SVD domain[J]. *National Academy Science Letters*, 2014, 37(4):351-358.

作者简介：

吴佳楠(1980－)，男，吉林长春人，博士，副教授，2007 年、2013 年于吉林大学分别获得硕士、博士学位，主要从事量子通信、数据挖掘等方面的研究。E-mail:jiananwu@126.com

导师简介：

王世刚(1962－)，男，吉林吉林市人，博士，教授，博士生导师，1983 年于东北大学获得学士学位，1997 年于吉林工业大学获得硕士学位，2001 年于吉林大学获得博士学位，主要从事真三维立体影像显示、视频分析与行为监测和视频通信等方面的研究。E-mail:wangshigang@vip.sina.com

(本栏目编辑：秦　思)