

彩色量子图像的水印方案

卢爱平, 李盼池*

(东北石油大学 计算机与信息技术学院, 黑龙江 大庆 163318)

摘要: 图像水印是信息安全领域的基本问题, 在经典图像处理中已被深入研究。然而在将来的量子计算机上如何实现水印图像的嵌入和抽取, 目前还不够成熟。文中提出了两种量子彩色图像水印方案, 其中水印图像为灰度图像, 封面图像为彩色图像, 水印图像的大小为载体图像的八分之一。首先, 将水印图像扩大八倍, 并使其每个像素的三基色颜色值仅为1个二进制位。然后, 采用 NEQR 模型将载体图像和扩大后的水印图像都转换为量子图像, 最后使用 Toffoli 门将水印像素的单比特颜色值, 嵌入到载体图像的最小显著位中, 完成水印嵌入过程。抽取过程为嵌入的逆过程。设计了可并行实现嵌入和抽取过程的量子线路, 在经典计算机上, 采用 MATLAB 矩阵模拟量子计算中的酉算子, 仿真结果验证了该方法的安全性。

关键词: 量子信息处理; 量子图像处理; 量子图像描述; 量子图像水印

中图分类号: TP391

文献标识码: A

文章编号: 1673-629X(2020)06-0109-05

doi:10.3969/j.issn.1673-629X.2020.06.021

Watermarking Scheme for Color Quantum Image

LU Ai-ping, LI Pan-chi*

(School of Computer and Information Technology, Northeast Petroleum University,
Daqing 163318, China)

Abstract: Image watermarking is a basic problem in the field of information security, which has been deeply studied in classical image processing. However, how to implement the embedding and extraction of watermarking image on future quantum computers is still not mature enough. We propose two quantum color image watermarking schemes, in which the watermark image is a gray-scale image and the cover image is a color image. The size of the watermark image is one eighth of the carrier image. Firstly, the watermark image is expanded by eight times so that the three primary color values of each pixel are only one binary bit. Next, the NEQR (novel enhanced quantum representation) model is used to transform the carrier image and the enlarged watermarking image into quantum image. Finally, the Toffoli gate is used to embed the single-bit color value of the watermark pixel into the least significant bit of the carrier image to complete the watermark embedding process. The extraction process is the inverse process of embedding. We design the quantum circuits to realize the embedding and extracting process in parallel. On the classical computer, the unitary operator in quantum computation is simulated by MATLAB matrix. The simulation results verify the security of the proposed method.

Key words: quantum information processing; quantum image processing; quantum image representing; quantum image watermarking

0 引言

在信息技术快速发展的今天, 多媒体信息安全越来越引起人们的高度重视。在经典计算机上, 作为信息重要载体之一的图像处理技术已研究的相当成熟^[1-8]。然而通过量子计算与图像处理交叉产生的量子图像处理相关研究才刚刚起步。由于量子计算机的运行机制与经典计算机完全不同, 大量成熟的经典图像处理算法根本无法移植到量子计算机上, 而必须重新设计, 从而导致了量子图像处理学科发展较为缓慢。

量子图像处理起步于图像在量子计算机上的存储和描述。在经典计算机上, 只需存储像素的颜色而无需存储其位置, 而在量子计算机上, 需要对二者(像素位置和颜色)同时存储^[9-15]。即使如此, 利用量子态的叠加特性, 所需的量子资源(比特数)仅是图像规模的线性函数。这正是量子计算的优势所在。在量子图像处理算法方面, 目前仅仅实现了经典图像处理中最基本最简单操作, 比如量子图像水印^[16-23]、加密^[24-29]等。

关于量子图像水印的相关研究, 目前主要有: 基于

图像预定区域几何变换的水印策略^[16],其缺点是嵌入容量较小;基于傅里叶变换的水印策略^[21]、基于小波变换的水印策略^[17]和基于 Hadamard 变换的水印策略^[18],这三个方案的缺点是设计的方案不能物理实现^[19-20,22]。

针对量子彩色图像的水印嵌入和抽取,文中采用量子计算原理设计了两种可以在量子计算机上执行的策略,基于经典计算机的 MATLAB 仿真环境,验证了两种方案的可行性。

1 量子图像的 NEQR 描述

量子图像的 NEQR 模型是目前最为流行的量子图像描述方法。其特点是像素位置和 RGB 颜色值都采用量子比特基态描述,对于一幅 $2^n \times 2^n$ 且 RGB 三通道颜色值范围均为 $\{0,1,\dots,255\}$ 的彩色图像,其 NEQR 可描述为:

$$|I\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |f(Y,X)\rangle |YX\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} \bigotimes_{i=0}^7 |C_{YXR}^i\rangle \bigotimes_{i=0}^7 |C_{YXG}^i\rangle \bigotimes_{i=0}^7 |C_{YXB}^i\rangle |YX\rangle \quad (1)$$

其中 $f(Y,X) = C_{YXR}^0 \dots C_{YXR}^7 C_{YXG}^0 \dots C_{YXG}^7 C_{YXB}^0 \dots C_{YXB}^7$, $C_{YXR}^k, C_{YXG}^k, C_{YXB}^k \in \{0,1\}$, $f(Y,X) \in \{0,1,\dots,2^{24}-1\}$ 。

2 彩色图像的量子水印方案

假定载体图像和水印图像的幅度分别为 $2^{n+1} \times 2^{n+2}$ 和 $2^n \times 2^n$ 。

2.1 水印图像的嵌入过程

文中提出的水印方案包括嵌入和抽取两部分,其中嵌入包括 3 个步骤,具体如下:(1)将 $2^{n+1} \times 2^{n+2}$ 的彩色载体图像转换为 NEQR 描述 $|C\rangle$;将 $2^n \times 2^n$ 的彩色水印图像放大 8 倍后,转换为 NEQR 描述 $|W\rangle$;(2)采用 Toffoli 门,将 $|W\rangle$ 嵌入 $|C\rangle$ 中得到 $|CW\rangle$;(3)将 $|CW\rangle$ 转换为经典图像。

在以上三个步骤中,核心是第二步。文中提出如下两种方案。

方案 I:水印图像嵌入到载体图像的最小显著位。具体方法如下:

放大之后的水印图像与载体图像大小相等,因此可以实施一对一的像素嵌入。将载体图像三基色的第二最小显著位(即颜色比特中第 7,15,23 位)和水印图像的三个颜色比特作为 Toffoli 门的控制位,将载体图像三基色的最小显著位(即颜色比特中第 8,16,24 位)作为 Toffoli 门的目标位。即可实现水印图像的嵌入。具体嵌入线路如图 1 所示。为简洁直观,图中只给出了颜色比特线路。

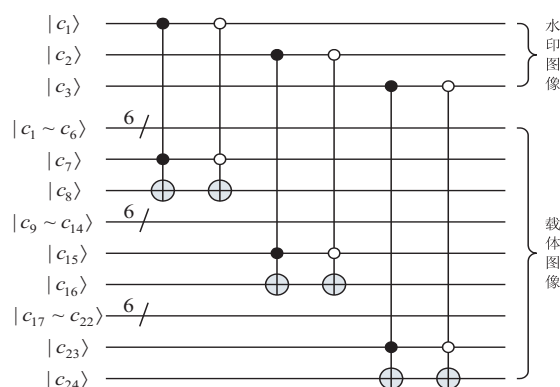


图 1 嵌入方案 I 的量子线路

方案 II:水印图像嵌入到载体图像的最小显著位和第二最小显著位。具体方法如下:

将载体图像三基色的第三最小显著位(即颜色比特中第 6,14,22 位)和水印图像的三个颜色比特作为 Toffoli 门的控制位,将载体图像三基色的最小显著位和第二最小显著位(即颜色比特中第 7,8,15,16,23,24 位)作为 Toffoli 门的目标位。即可实现水印图像的嵌入。具体嵌入线路如图 2 所示。为简洁直观,图中只给出了颜色比特线路。

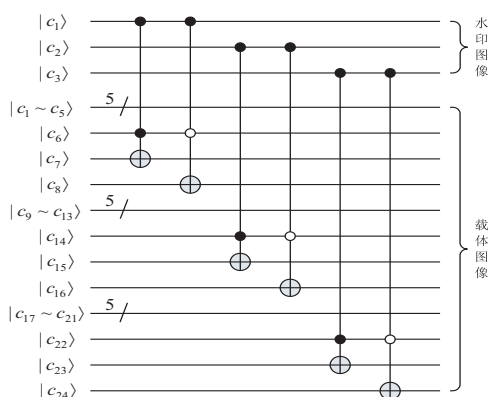


图 2 嵌入方案 II 的量子线路

以上两方案均用受控 Toffoli 门实现水印嵌入,嵌入水印后载体图像的最小显著位与嵌入的水印图像无任何关系,因而保证了嵌入水印的安全性。

2.2 水印图像的抽取过程

文中提出的两种嵌入方案均为非盲的,抽取时需要借助原始载体图像。

方案 I:以带水印载体最小显著位和第二最小显著位(即颜色比特中第 7,8,15,16,23,24 位)作为 Toffoli 门的控制位,以原始载体图像最小显著位(即颜色比特中第 8,16,24 位)作为 Toffoli 门的目标位,即可将原始载体图像的最小控制位转换为水印图像,再用 CNOT 门将其存入初态为 $|0\rangle^{\otimes 3}$ 的三个比特中,即可实现水印图像的抽取。具体量子线路如图 3 所示。

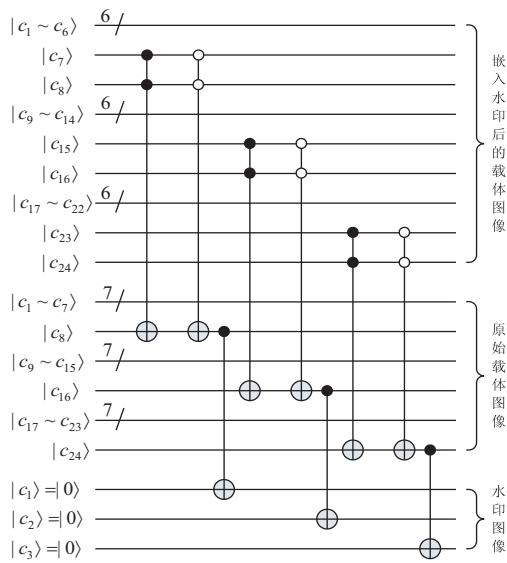


图3 方案I的水印抽取线路

方案II:以带水印载体的最小、第二最小、第三最小显著位(即颜色比特中第6,7,8,14,15,16,22,23,24位)作为 Toffoli 门的控制位,以原始载体图像的最小和第二最小显著位(即颜色比特中第7,8,15,16,23,24位)作为 Toffoli 门的目標位,即可将原始载体图像的最小控制位转换为水印图像,再用 CNOT 门将其存入初态为 $|0\rangle$ 的三个比特中,即可实现水印图像的抽取。具体量子线路如图4所示。

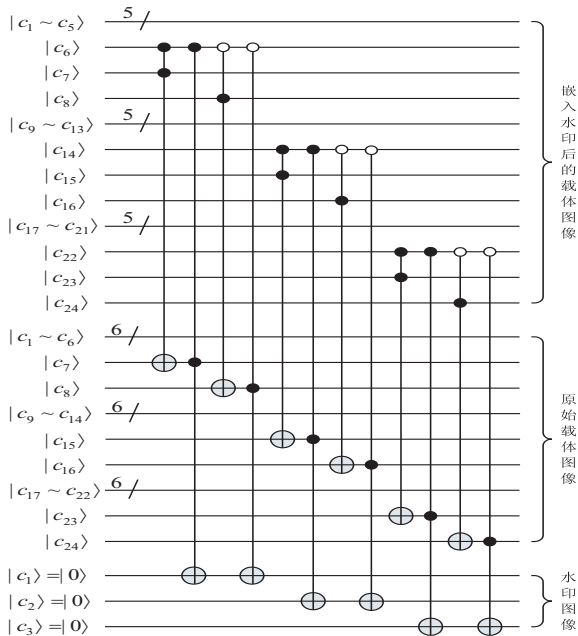


图4 方案II的水印抽取线路

抽取出的水印图像经过测量后即可得到经典的三通道二值图像,再将其缩小到原来的八分之一,并使每个像素颜色值为8比特二进制数,即可得到原始水印图像。

2.3 量子图像的检索

量子图像检索也称测量,是从储存图像的量子态

获得经典图像的过程。由于测量将导致量子态坍缩,所以每次测量仅能随机地获得一个像素的位置和颜色信息。因为像素颜色也存储在基态中,所以所得像素的颜色具有确定性。要获得整幅图像的信息,只能事先准备大量相同的图像并逐个实施测量才能得到。这是通过测量获得量子图像的缺点。然而目前国内外尚无其他更好的方法。

3 仿真实验

文中方案面向量子图像,要进行理想的验证,必须借助于量子计算机才能实现,这在目前阶段显然是不可行的。然而在经典计算机上,尽管不能仿真量子计算的并行性,但借助 MATLAB 矩阵运算,完全可以仿真方案的执行效果。图5给出了本仿真将要使用的8幅大小为 512×512 的载体图像,图6给出了8幅大小为 256×128 的水印图像。

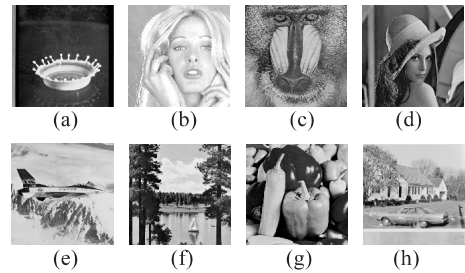


图5 实验采用的8幅载体图像

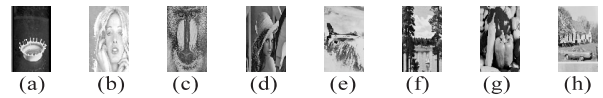


图6 实验采用的8幅水印图像

3.1 水印的嵌入和抽取

以自身嵌入为例(即第*i*幅水印嵌入第*i*幅载体),嵌入水印后的8幅载体图像,以及按抽取策略抽取出的水印图像在视觉上分别与图5和图6完全相同,没有任何变化,因此不在列出。若采用直接抽取带水印图像的最小显著位(这是攻击者的常用手段),得到的是没有任何实际意义的噪声图像。对于应用文中方案获得的水印图像,如果试图通过直接抽取最小显著位得到水印,结果如图7和图8所示,这表明两种方案都具有较强的抗攻击能力。

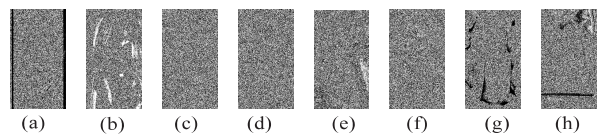


图7 方案I直接抽取最小显著位获得的水印图像

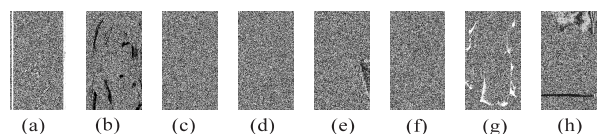


图8 方案II直接抽取最小显著位获得的水印图像

表 1 8 种图像各种组合下带水印载体图像的峰值信噪比

dB

载体图像	方案	水印图像							
		(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
(a)	I	51.040 3	51.181 1	51.148 0	51.125 7	51.160 0	51.140 4	51.130 6	51.152 3
	II	47.396 5	46.106 9	47.236 9	47.177 4	46.888 1	47.385 3	47.645 9	47.077 2
	文献[23]	44.377 4	42.731 4	44.117 7	44.184 9	43.807 4	44.267 1	44.444 8	43.845 7
(b)	I	51.061 3	50.476 8	51.102 9	51.073 5	51.066 3	51.137 0	51.123 0	51.119 1
	II	46.882 9	45.355 6	46.675 6	46.619 4	46.341 4	46.828 9	47.048 2	46.540 6
	文献[23]	44.111 8	42.213 9	43.880 2	43.932 4	43.539 4	44.053 0	44.173 4	43.602 2
(c)	I	51.135 1	51.136 4	51.146 9	51.133 3	51.146 6	51.134 6	51.141 0	51.138 2
	II	47.405 5	46.021 4	47.156 8	47.102 3	46.792 3	47.296 8	47.552 1	46.999 4
	文献[23]	44.425 0	42.781 0	44.158 5	44.228 7	43.865 5	44.318 4	44.485 2	43.887 2
(d)	I	51.132 2	51.152 5	51.147 0	51.153 3	51.152 7	51.139 6	51.140 8	51.147 4
	II	47.394 1	46.009 0	47.131 4	47.094 1	46.786 1	47.288 4	47.540 1	46.982 3
	文献[23]	44.421 1	42.777 2	44.152 8	44.221 2	43.872 5	44.312 0	44.485 9	43.897 4
(e)	I	51.133 6	51.154 7	51.141 1	51.139 1	51.145 2	51.141 6	51.134 5	51.139 2
	II	47.427 4	46.038 8	47.166 2	47.127 7	46.799 5	47.314 3	47.5683	47.016 8
	文献[23]	44.401 0	42.762 5	44.134 7	44.196 1	43.843 1	44.288 5	44.465 0	43.868 7
(f)	I	51.146 3	51.141 1	51.141 0	51.143 8	51.147 7	51.128 8	51.130 2	51.129 5
	II	47.400 5	46.018 9	47.133 2	47.091 3	46.787 2	47.285 3	47.538 5	46.988 5
	文献[23]	44.397 8	42.7610	44.137 2	44.204 4	43.840 1	44.292 2	44.467 2	43.871 1
(g)	I	51.124 4	51.176 4	51.139 3	51.137 4	51.164 4	51.119 9	51.000 9	51.146 0
	II	47.509 0	46.116 6	47.255 7	47.210 9	46.909 9	47.403 6	47.573 6	47.102 4
	文献[23]	44.340 8	42.719 9	44.086 6	44.163 2	43.788 1	44.241 2	44.431 9	43.805 5
(h)	I	51.140 7	51.128 0	51.134 2	51.132 6	51.138 5	51.132 1	51.142 5	51.114 7
	II	47.381 8	46.002 0	47.132 7	47.086 7	46.789 4	47.280 9	47.536 8	46.952 0
	文献[23]	44.420 2	42.784 6	44.149 5	44.223 7	43.876 5	44.322 9	44.488 9	43.899 3

3.2 水印嵌入后的峰值信噪比

为定量描述嵌入的水印对封面图像可视化质量的影响,文中采用峰值信噪比作为评价指标,具体定义如式(2)所示。

$$\text{PSNR} = 20 \log_{10} \frac{255}{\sqrt{\frac{1}{3mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \sum_{k=0}^3 \lambda_{ijk}^2}} \quad (2)$$

其中, $\lambda_{ijk} = I_d(i, j, k) - I_p(i, j, k)$, I_d 为封面图像, I_p 为 I_d 嵌入水印后的图像。显然, PSNR 越大表明 I_d 和 I_p 越接近。

为考察提出的两种水印方案的性能,将实验结果与文献[23]提出的水印方案作了对比。针对三种方案,表 1 给出了 8 种图像各种组合下带水印载体图像的峰值信噪比。

由表 1 可知,方案 I 带水印载体图像的峰值信噪比均超过 51 dB,方案 II 的峰值信噪比均在 47 dB 左右,而文献[23]中方案的峰值信噪比仅为 44 dB 左右。方案 I 和方案 II 的峰值信噪比分别高出文献[23]中

方案 7 dB 和 4 dB 以上。对于方案 I 比方案 II 的 PSNR 高出 4 dB 的原因是,方案 I 仅在载体图像的最小显著位嵌入,二方案 II 同时在最小显著位和第二最小显著位嵌入,从而使载体图像的像素灰度值改变量加大的缘故。

值得注意的是,水印嵌入量的大小直接关系到 PSNR 的高低,文中方案的 PSNR 较高的原因是因为水印的嵌入量较小。然而,在载体图像中嵌入水印的目的在于保护版权利益,关注点在于嵌入水印后对载体图像带来的影响(即 PSNR 的大小),而对于嵌入量的多少一般不予关注。这表明提出的针对彩色量子图像的两种水印嵌入及抽取方案,在提升水印方案的多样性方面有一定意义。

4 结束语

针对彩色量子图像的水印问题,提出了两种实施方案。在该方案中,约定封面图像的大小为 $2^{n+1} \times 2^{n+2}$,水印图像的大小 $2^n \times 2^n$ 。首先将水印图像扩展

为与载体图像相同大小,然后采用 NEQR 将载体和水印都描述为量子图像,最后使用 Toffoli 门将水印图像嵌入到载体图像的最小显著位和第二最小显著位中。水印图像的抽取是嵌入的逆过程。两种方案的优点是量子线路的设计简单。仿真实验结果表明,两种方案在嵌入水印后图像的视觉质量、抗攻击能力两方面都具有较好的实际效果。

参考文献:

- [1] AKHSHANI A, AKHAVAN A, LIM S C. An image encryption scheme based on quantum logistic map[J]. Communications in Nonlinear Science and Numerical Simulation, 2012, 17(12): 4653–4661.
- [2] LU D, HE W, PENG X. Optical image encryption based on a radial shearing interferometer[J]. Journal of Optics, 2013, 15(10): 105405.
- [3] SHI Y, LI T, LI H. Optical image encryption via ptychography[J]. Optics Letters, 2013, 38(9): 1425–1427.
- [4] SUN M, SHI J, LI H. A simple optical encryption based on shape merging technique in periodic direction correlation imaging[J]. Optics Express, 2013, 21(16): 19395–19400.
- [5] WANG X, ZHAO D. Simultaneous nonlinear encryption of grayscale and color images based on phase-truncated fractional Fourier transform and optical superposition principle[J]. Applied Optics, 2013, 52(25): 6170–6178.
- [6] WANG X, LIU L. Cryptanalysis of a parallel sub-image encryption method with high-dimensional chaos[J]. Nonlinear Dynamics, 2013, 73(1–2): 795–800.
- [7] ZANG J, XIE Z, ZHANG Y. Optical image encryption with spatially incoherent illumination[J]. Optics Letters, 2013, 38(8): 1289–1291.
- [8] CHEN L, ZHAO D, GE F. Image encryption based on singular value decomposition and Arnold transform in fractional domain[J]. Optics Communications, 2013, 291(3): 98–103.
- [9] YUAN S, MAO X, XUE Y, et al. SQR: a simple quantum representation of infrared images[J]. Quantum Information Processing, 2014, 13(6): 1353–1379.
- [10] VENEGAS S E, BALL J L. Processing images in entangled quantum systems[J]. Quantum Information Processing, 2010, 9(1): 1–11.
- [11] LE P, DONG F, HIROTA K. A flexible representation of quantum images for polynomial preparation image compression and processing operations[J]. Quantum Information Processing, 2011, 10(1): 63–84.
- [12] SUN B, ITIYASUA M, YAN F, et al. An RGB multi-channel representation for images on Quantum computers[J]. Journal of Advanced Computational Intelligence and Intelligent Informatics, 2013, 17(3): 404–417.
- [13] LI H, ZHU Q, ZHOU R, et al. Multi dimensional color image storage and retrieval for a normal arbitrary quantum superposition state[J]. Quantum Information Processing, 2013, 13(4): 991–1011.
- [14] SONG X, WANG S, NIU X. Multi-channel quantum image representation based on phase transform and elementary transformations[J]. Journal of Information Hiding and Multimedia Signal Processing, 2014, 5(4): 574–585.
- [15] ZHANG Y, LU K, GAO Y, et al. NEQR: a novel enhanced quantum representation of digital images[J]. Quantum Information Processing, 2013, 12(8): 2833–2860.
- [16] ILIYASU A, LE P, DONG F, et al. Watermarking and authentication of quantum images based on restricted geometric transformations[J]. Information Science, 2012, 186(1): 126–149.
- [17] SONG X, WANG S, LIU S, et al. A dynamic watermarking scheme for quantum images using quantum wavelet transform[J]. Quantum Information Process, 2013, 12(12): 3689–3706.
- [18] SONG X, WANG S, NIU X. Dynamic watermarking scheme for quantum images based on Hadamard transform[J]. Multimedia Systems, 2014, 20(4): 379–388.
- [19] YANG Y, XU P, TIAN J, et al. Analysis and improvement of the dynamic watermarking scheme for quantum images using quantum wavelet transform[J]. Quantum Information Process, 2014, 13(9): 1931–1936.
- [20] YANG Y, WANG Y, ZHAO Q. Letter to the editor regarding dynamic watermarking scheme for quantum images based on Hadamard transform by Song et al[J]. Multimedia Systems, 2014, 20(4): 379–388.
- [21] ZHANG W, GAO F, LIU B, et al. A watermark strategy for quantum images based on quantum Fourier transform[J]. Quantum Information Process, 2013, 12(4): 793–803.
- [22] YANG Y, JIA X, XU P, et al. Analysis and improvement of the watermark strategy for quantum images based on quantum Fourier transform[J]. Quantum Information Process, 2013, 12(8): 2765–2769.
- [23] MIYAKE S, NAKAMAE K. A quantum watermarking scheme using simple and small-scale quantum circuits[J]. Quantum Information Process, 2016, 15(5): 1849–1864.
- [24] 李盼池, 卢爱平. 基于量子比特绕轴旋转的彩色图像加密方法[J]. 控制与决策, 2016, 31(8): 1363–1371.
- [25] 郭海儒, 许权, 杜娅颖. 基于像素颜色置乱的彩色量子图像加密方法[J]. 量子电子学报, 2019, 36(1): 1–5.
- [26] 王菡. 基于量子线路模型的量子图像加密技术研究[D]. 北京: 北京交通大学, 2018.
- [27] 李春雨. 基于相移变换的量子图像加密算法[D]. 桂林: 广西师范大学, 2019.
- [28] 陈冰冰. 像素-色度联合量子图像加密方法的研究[D]. 哈尔滨: 哈尔滨工业大学, 2017.
- [29] 胡铁群. 基于猫脸变换和循环移位操作的量子图像加密算法[D]. 南昌: 南昌大学, 2017.