Computer Science and Application 计算机科学与应用, 2026, 16(11), 130-141
Published Online November 2026 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2026.1611331

Hans汉斯

Kyber密文域DWT图像双水印算法设计

蒋　雪[1]，张若箐[2]，袁艺林[1]，高　博[1]，李子臣[1*]

[1]北京印刷学院信息工程学院，北京
[2]香港高等教育科技学院酒店及商业管理系，香港

收稿日期：2026年10月6日；录用日期：2026年11月5日；发布日期：2026年11月12日

摘　要

随着云存储与隐私计算的发展，密文域数字水印逐渐成为图像版权保护的重要研究方向，同时在后量子密码学逐步迈入标准化进程的背景下，面向后量子安全的双水印也成为研究热点。本文提出一种基于Kyber后量子公钥加密的密文域双水印算法，该算法将两个独立的版权水印分别嵌入三级小波变换后的HL3与LH3子带，为多主体版权验证提供技术基础。嵌入步骤为首先将图像进行小波变换，对小波系数预处理后进行Kyber加密，随后利用其加法同态性质在密文域完成双水印嵌入；在提取阶段，既可在密文域中直接提取，完成版权验证，也可利用同态性质在解密后于明文域中提取水印，从而提高算法的灵活性与隐私保护能力。实验结果表明，方案在保持高保真度的前提下，两个水印能抵抗噪声、JPEG压缩等常见攻击，且相互干扰低，在数字版权保护与隐私内容分发等领域具有一定应用价值。

关键词

同态加密，Kyber算法，密文域水印，多水印

Kyber Ciphertext-Domain DWT Image Double Watermarking Algorithm Design

Xue Jiang[1], Ruoqing Zhang[2], Yilin Yuan[1], Bo Gao[1], Zichen Li[1*]

[1]School of Information Engineering, Beijing Institute of Graphic Communication, Beijing
[2]Department of Hospitality and Business Management, Technological and Higher Education Institute of Hong Kong, Hong Kong

Received: October 6, 2026; accepted: November 5, 2026; published: November 12, 2026

Abstract

With the development of cloud storage and privacy computing, ciphertext-domain digital water-

*通讯作者。

文章引用: 蒋雪, 张若箐, 袁艺林, 高博, 李子臣. Kyber 密文域 DWT 图像双水印算法设计[J]. 计算机科学与应用, 2026, 16(11): 130-141. DOI: 10.12677/csa.2026.1611331

marking has gradually become an important research direction for image copyright protection. At the same time, with post-quantum cryptography gradually moving toward standardization, post-quantum secure double watermarking has also become a research hotspot. This paper proposes a ciphertext-domain double watermarking algorithm based on Kyber post-quantum public-key encryption. The algorithm embeds two independent copyright watermarks into the HL3 and LH3 subbands of a three-level wavelet transform, providing a technical foundation for multi-party copyright verification. The embedding steps involve first applying a wavelet transform to the image, preprocessing the wavelet coefficients, then encrypting them with Kyber, and finally using its additive homomorphic property to embed the double watermark in the ciphertext domain. During extraction, the watermark can be directly extracted in the ciphertext domain to complete copyright verification, or it can be extracted in the plaintext domain after decryption using the homomorphic property, enhancing the algorithm's flexibility and privacy protection. Experimental results show that the scheme maintains high fidelity while the two watermarks can resist common attacks like noise and JPEG compression, with low mutual interference, making it valuable for digital copyright protection and privacy content distribution.

Keywords

Homomorphic Encryption, Kyber Algorithm, Cipher Field Watermark, Multiple Watermark

Copyright © 2026 by author(s) and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

随着数字内容交易的迅速发展，越来越多的图像、视频及模型文件需要通过第三方云平台进行托管与分发。这些平台往往不可信，存在数据泄露、内容篡改及非法复制的风险[1]。在典型的多方交易场景下，如版权方与购买方共同参与，单一水印仅能标记一方身份，难以同时实现版权所有权认证与交易溯源的独立需求[2]；在嵌入水印的过程中还要保证嵌入过程不向平台泄露载体内容，这对隐私保护提出了严格要求[3]。密文域水印技术借助同态加密，可在加密图像上直接完成水印嵌入与验证，为解决上述矛盾提供了可行路径[4]。但如何在密文域中完成多水印独立嵌入，并兼顾后量子安全性，仍是该领域面临的挑战。多水印嵌入且具备后量子安全性的密文域水印方法，具有重要的理论和应用价值。

在密文域水印领域，早期工作多采用 RSA 或 Paillier 等传统公钥密码，利用其乘法[5]或加法[6]同态性质实现水印的嵌入与提取，验证了密文域版权保护的可行性。随着发展，这些方案显现两方面关键局限。其一，水印数量受限[7]。现有的密文域水印设计大多为单一水印嵌入，若想在密文域中嵌入两个相互独立的水印，通常会面临两个水印嵌入过程相互干扰的问题，难以直接扩展为多水印嵌入[8]。其二，安全基础面临威胁且计算开销大。Paillier 和 RSA 等算法依赖的整数分解与离散对数难题，在 Shor 量子算法面前理论上可被高效破解[9]，因而不具备后量子安全性[10]。此外，这类算法涉及大整数模幂运算，计算效率低，在处理高维度图像数据时尤为明显[11]。综上，现有密文域水印方法在多水印嵌入与后量子安全方面存在明显不足，亟需一种基于后量子密码的密文域多水印方案。

上述传统公钥加密在 Shor 算法等量子攻击模型下不再可靠。为应对这一威胁，NIST 推动了后量子密码的标准化进程，其中基于格问题的 Kyber 算法因其较高的安全性与运算效率受到广泛关注[12]。基于 Kyber 密文结构的线性可加性，可构造有限整数加法同态运算[13]，能够支持密文域数据运算，为密文域数字水印嵌入与提取提供了新的实现方式。因此，将 Kyber 与数字水印技术相结合，能够在保证隐私保

护的同时，实现密文域多版权认证。

此外，双水印框架本身的设计对多主体版权保护同样重要。现有的双水印方案大致可分为两类[14]。第一类是功能耦合法，典型代表如 Zermi 等人[15]和 Ahmadi 等人[16]的工作，它们分别在医学图像中嵌入鲁棒水印与脆弱水印，前者承担版权标识功能，后者承担内容完整性认证功能。这类方案本质上仍服务于单一方版权保护，两个水印之间的职能绑定使其难以用于多主体认证场景。第二类是明文域多水印，如段等人[17]提出的频域双水印方案虽已开始关注隐私保护，但其所依赖的加密或置乱仍属于传统预处理手段，水印的嵌入与提取仍在明文域完成，无法避免不可信平台泄露隐私。正是密文域嵌入与后量子安全缺失的双重空白，使得现有双水印方案无法直接应用于密文域多版权认证场景中，为本文设计 Kyber 同态加密的密文域双水印算法提供了必要性。

针对现有密文域水印算法多以单水印为主、现有双水印算法缺少密文域多主体版权认证等问题，本文提出一种基于 Kyber 加法同态性质的 DWT 密文域双水印算法。首先，对载体图像进行三级离散小波变换，并选取 HL3 与 LH3 子带作为双水印嵌入的子带；随后，使用 Kyber 加密算法对小波系数进行加密，利用加法同态性质在密文域完成双水印嵌入。本方案涉及三类实体：版权方、不可信平台、验证方。在上传到平台前对图片和水印信息完成加密，嵌入水印在平台中密文域完成，保证不泄露图片原始信息。

本文嵌入的两个水印均用于版权认证，具有相同的鲁棒性，以实现多主体版权验证与责任追溯。此外，所提算法既支持在密文域中直接提取水印，也支持解密后在明文域中进行版权认证，从而提高了算法在隐私场景下的应用灵活性。

2. 理论基础

本部分将介绍同态水印算法、三层小波变换嵌入水印以及 Kyber 加密所具有的加法同态特性。

2.1. 同态水印算法

同态加密是密码学的范畴，主要是指在密文域中进行的加法运算和乘法运算等操作，可以映射到对明文的运算，因此，在明文数据嵌入水印信息可以通过在密文域中嵌入来实现，同样的，在密文域中嵌入水印可以通过在明文域中操作来实现。

在一个密码系统中，E 是加密算法，D 是对应的解密算法。明文域 $M=(a_1,a_2,\cdots,a_t)$，密文域 $C=(E(a_1),E(a_2),\cdots,E(a_t))$，有两个代数系统分别为 $V1=(M,※1,※2,\cdots,※n)$ 和 $V2=(C,\odot 1,\odot 2,\cdots,\odot n)$。代数系统中的两套运算为 $※i(a_1,a_2,\cdots,a_t)$ 和 $\odot i(E(a_1),E(a_2),\cdots,E(a_t))$，$i=1,2,\cdots,n$，$t\in Z$，分别代表明文域和密文域数字水印算法。

若对任意的运算 $※i$ 和 $\odot i$，都满足：$※i(a_1,a_2,\cdots,a_t)=D(\odot i(E(a_1),E(a_2),\cdots,E(a_t)))$，$i=1,2,\cdots,n$，$t\in Z$，称 $\odot i$ 为密文域全同态水印算法。

若水印嵌入与提取过程满足密文域运算与明文域运算之间的同态映射关系，则称其为同态水印算法。

同态密码的同态属性允许对加密域进行某些操作，解密后，在明文域中执行相同操作可以实现同样的效果。因此，使用同态密码算法来设计同态水印方案，是一种水印技术和密码技术相互融合的有效途径。本文使用 Kyber 加法同态加密图像来实现同态数字水印。

2.2. 三层离散小波变换

离散小波变换(Discrete Wavelet Transform, DWT)具有良好的时频局部化分析能力和多分辨率特性，能够将图像分解为不同尺度与方向的频率子带，被广泛应用于数字水印领域。在水印算法中，DWT 能够有效分离图像的低频结构信息与高频纹理信息，从而为水印嵌入区域的选择提供依据。

对原始图像进行三级离散小波分解后，可得到 LL3、HL3、LH3 和 HH3 等多个子带。其中，LL3 子带包含图像的大部分低频能量，虽然稳定性较高，但在该区域嵌入水印容易对图像视觉质量产生明显影响：HH3 子带主要包含高频细节信息，对压缩和噪声攻击较为敏感，鲁棒性较差。相比之下，HL3 与 LH3 子带能够保证图像不可感知性，而且保留一定的结构信息与能量分布，可以较好地平衡水印的鲁棒性与图像保真性，适合作为水印嵌入区域。

此外，多层小波分解能够在不同频率层级提供独立的嵌入空间，为多重水印的嵌入提供基础。

本文将两个版权水印分别嵌入 HL3 与 LH3 子带。图 1 为三级离散小波分解结构示意图。

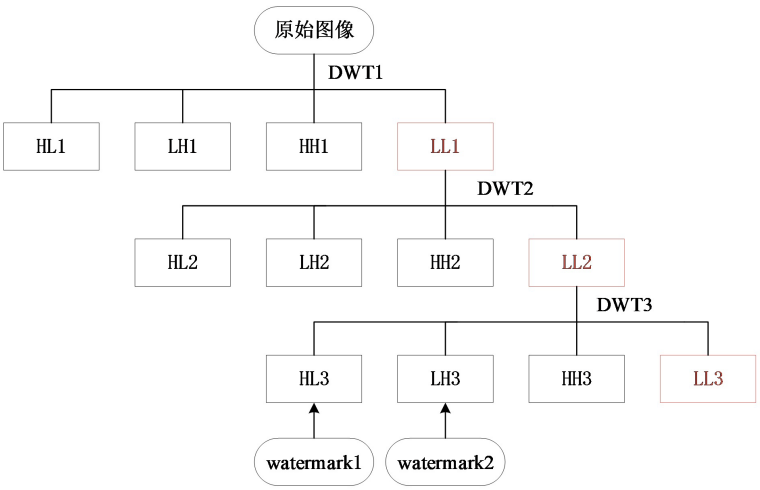


Figure 1. Three-level wavelet transform diagram
图 1. 三层小波变换图

2.3. Kyber 加法同态加密算法

为了实现在密文域上的加法操作，在 Kyber 公钥加密的基础上，引入了整数编码技术[18]，具体而言，算法通过编码过程将待加密明文映射到整数多项式上，随后进行加密、同态运算和解密等操作，保证了密文运算和明文运算的结果一致。

2.3.1. Kyber 算法整体流程

Kyber 加解密算法的整体流程如算法 1 表 1 所示。其中，KeyGen()函数用于生成公私钥对 pk 和 sk; Encode()函数将输入的明文整数 m 转换为多项式向量 M; Enc()函数在 Kyber 体系下完成加密运算，生成密文 c，密文 c 由(u, v)组成；Dec()函数负责将密文 c 解密还原为多项式 M，之后由 Decode()函数将多项式 M 解码为明文整数 m; Add()函数实现密文域上的加法同态操作。通过上述步骤，可以在保持数据机密性的同时，实现整数加法的安全计算。

2.3.2. Kyber 的加法同态

Kyber.PKE 的安全性建立在模容错学习问题(Module Learning with Errors, MLWE)之上，Kyber.PKE 的密文形如 $c=(u,v)$，其中 $u=A^{\mathrm{T}}r+e_1$，$v=t^{\mathrm{T}}r+e_2+\mathrm{Decompress}(\mathrm{Encode}(m),dp)$，公钥 $t=As+e$，r,e_1,e_2 为加密时取样的小噪声，不考虑压缩和解压缩过程，另明文 $m=v-s^{\mathrm{T}}u$，对于两组相同公钥加密 m_1 和 m_2 得到的密文 $c_1=(u_1,v_1)$，$c_2=(u_2,v_2)$，在明文中 $m_1+m_2=m_3$，$(v_1-s^{\mathrm{T}}u_1)+(v_2-s^{\mathrm{T}}u_2)=(v_1+v_2)-s^{\mathrm{T}}(u_1+u_2)$，且 $m_3=(v_3-s^{\mathrm{T}}u_3)$，可得 $(v_1+v_2)-s^{\mathrm{T}}(u_1+u_2)=v_3-s^{\mathrm{T}}u_3$，因此在密文上满足加法同态。其依赖密文结构的线性可加性。

Table 1. Kyber algorithm process
表 1. Kyber 算法流程

算法 1　Kyber 加法同态加密算法
输入待加密的明文 m，示例密文 $(u_1,v_1),(u_2,v_2)$。
输出密文 (u,v)，同态加法结果密文 $(u_{\text{add}},v_{\text{add}})$。
1) 生成密钥对 $(pk,sk)\leftarrow \text{KeyGen}(\text{parameters})$；
2) 对明文执行整数编码 $M\leftarrow \text{Encode}(m)$；
3) 使用公钥加密 $(u,v)\leftarrow \text{Enc}(pk,M)$；
4) 同态加法 $(u_{\text{add}},v_{\text{add}})\leftarrow \text{Add}((u_1,v_1),(u_2,v_2))$；
5) 解密加法结果 $M\leftarrow \text{Dec}(sk,(u,v))$；
6) 对多项式 M 解码 $m\leftarrow \text{Decode}(M)$；

将整数明文编码到明文空间中，并且把编码后的向量作为多项式的系数，本文参考吕[18]的文章中的整数编码思想，在此基础上进行整理与适配，使其更适用于本文的同态加法框架。

编码算法的核心是通过固定长度的二进制分段与添加 0 前缀的思想，将任意整数编码为长度为 n 的多项式向量，n 为环 R_q 上多项式的次数。

需要加密的明文整数为 m，首先将其转化为二进制表示 $bin(m)$。之后进行分段，每段长度为 $dp-1$，dp 为 Kyber 压缩参数，得到 $\{bin_1,bin_2,\cdots,bin_l\}$，在每段最高位添加一个“0”，此时每段长度为 dp，得到新序列，之后将添加“0”后的每段二进制数转化为十进制表示，得到整数向量：

$$v=(v_1,v_2,\cdots,v_l) \tag{1}$$

若 v 的向量长度 $l<n$，则在向量前端补零，使其长度达到 n，最终得到多项式向量：

$$M=\left(\underbrace{0,\cdots,0}_{n-l\text{个}},v_1,v_2,\cdots,v_l\right) \tag{2}$$

使用公钥对多项式向量 M 加密，解密后同样得到多项式向量 M，之后解码，解码过程为逆操作，给定多项式向量 $M=(0,\cdots,0,v_1,v_2,\cdots,v_l)$，对 M 采用逆序重构的方式，取逆序 $M_{\text{reverse}}=(v_l,\cdots,v_1,0,\cdots,0)$ 之后计算：

$$\text{Decode}(M)=\sum_{i=0}^{n-1}M_{\text{reverse}}[i]\cdot\left(2^{dp-1}\right)^i \tag{3}$$

本方案采取单次加法控制噪声增长，每个嵌入位置只做一次同态加法，噪声只累加一次，不涉及多次同态运算导致的逐次噪声放大。

3. 密文域同态图像双水印算法

本小节介绍基于 Kyber 密文域同态双水印算法的实现，具体包括图像加密的流程以及水印的嵌入和提取。该算法充分利用 Kyber 公钥加密算法所具备的加法同态特性，将水印信息嵌入至离散小波变换域的高频子带中，在保障图像内容安全性的同时，提高水印的鲁棒性与不可见性。

3.1. 技术架构

首先将载体图像进行三层离散小波变换，将图像分解得到 1 个低频子带与 9 个高频子带，选择 LH3

和 HL3 作为水印嵌入区域。为了确保密文域中水印嵌入过程的可控性与可逆性，先对其小波系数进行预处理，将每个系数都变为整数，预处理完成后使用 Kyber 加密算法进行加密，加密完成后在特定子带嵌入水印，得到含有双水印的密文图像，解密后再对其进行三层小波逆变换得到含水印的明文。提取水印时可在明文中处理。算法总体流程如图 2。

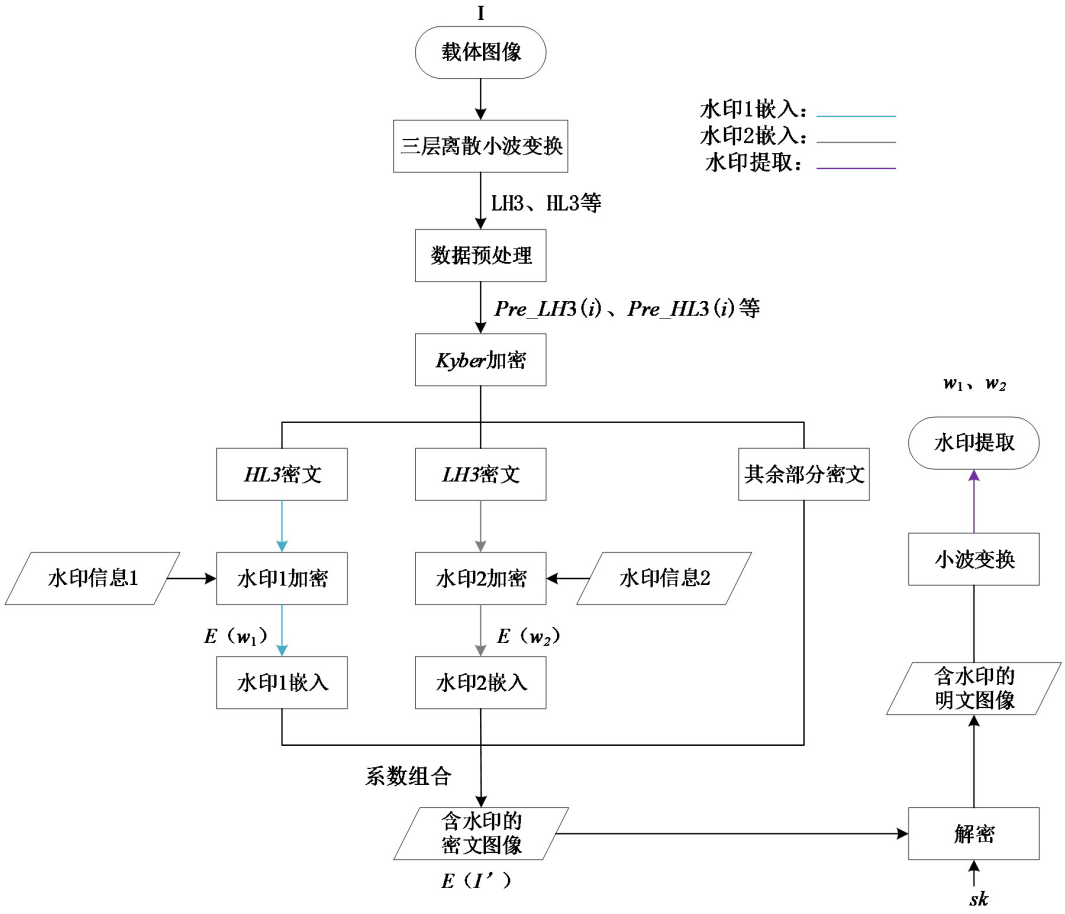


Figure 2. Overall algorithm structure diagram
图 2. 算法总体结构图

3.2. 图像加密

三层小波变换完成后，要对得到的频带系数进行处理以便于加密和后期提取水印。

对于需要嵌入水印部分，在加密之前，要将系数进行预处理，预处理将每个小波系数 x 量化为正整数，在保留两位小数取整数时，其引入的舍入误差满足小于等于 0.005，即每个系数至多损失半个最低有效位，该误差对所有子带一致，且与图像内容无关。嵌入所引起的峰值信噪比远高于嵌入水印所造成的峰值信噪比，说明 2 位小数的量化对图像质量的影响可以忽略不计。

预处理过程为：将频带系数变为正整数，使其能够进行 Kyber 加密。以 LH3 部分加密为例，将 LH3 部分中的 1024 个频带系数按矩阵保存，对矩阵中的每个小数保留小数点后第 d 位，本文中经实验对比选择 d 为 2，之后取绝对值将其转化为整数，记转化后的整数为 x_i，对 x_i 进行编码和加密：

$$C_1 = \mathrm{Enc}\left(pk, \mathrm{Encode}\left(x_i\right)\right) = \left(u_i, v_i\right) \tag{4}$$

C_1 是 LH3 子带加密后不含水印的密文。使用相同的方法对 HL3 部分进行处理后加密，得到 C_2。

对于未嵌入水印的频带系数，在加密前也需对其进行处理，将各部分频带系数分别保存，并利用 Kyber 算法进行加密，具体过程同加密 LH3，得到密文 C_j。

将以上加密完成后的系数拼接，得到密文不含水印的图像。

对于加密过程中 n 和 dp 参数的选择，$n=256$，$dp=4$，选择依据为对 512 × 512 的 8 bit 灰度图像，三层 Haar 小波后 HL3/LH3 系数绝对值一般不超过几十，放大 100 倍后仅需十余个比特即可表示，故 $n=256$ 提供的编码空间绰绰有余。dp 为每个系数分段的位宽，本方案每个嵌入位置只做一次加法，$dp=4$ 提供的保护位余量充足，是明文容量与噪声容限之间的合适折中。

3.3. 双水印嵌入与提取

嵌入水印时加性扩频方式嵌入，嵌入增量为：

$$\delta = 2\alpha \cdot W \tag{5}$$

其中 $W \in \{0,1\}$ 为要嵌入的水印比特，α 为嵌入强度，使用 Kyber 算法对 δ 加密，先将 δ 用整数编码方式编码为 $n=256$ 维多项式向量，再用相同的公钥 pk 加密，得到 $E(\delta)$，由于 x_i 与 δ 都编码到同一个 n 维系数空间、且使用同一公钥，二者的密文具有相同的结构，所以满足同态加法，嵌入过程以 LH3 子带为例，对于密文 C_1：

$$C_1' = C_1 + E(\delta) \tag{6}$$

其中 C_1' 为嵌入水印后的密文，其是由密文 C_1 和密文 $E(\delta)$ 进行同态加法的结果。

嵌入水印时在密文域中进行嵌入，根据 Kyber 的同态性质，提取水印时既可在密文域提取，也可在明文域中提取。具体而言，将嵌入水印后的密文频带系数与未嵌入水印的密文频带系数重新排列组合，构造得到含水印的密文图像。在此基础上，执行与嵌入相反的操作可以实现在密文域提取水印；也可先利用私钥对含水印的密文图像进行解密，并在解密完成后对图像进行小波逆变换，从而得到嵌入水印的明文图像 I'。

下面主要介绍在明文域提取水印。

以提取 LH3 自带为例，首先对图像 I' 进行三层离散小波变换，提取第三层分解中的 LH3 子带系数。随后，对上述高频系数保留小数点后第 d 位，并将其转换为正整数形式，得到含水印量化系数 x_i'；同时利用原始载体图像按相同方式得到原始量化系数 x_i。二者作差后，通过阈值 α 判决水印比特：

$$\begin{cases} W = 1, x_i' - x_i > \alpha \\ W = 0, \text{others} \end{cases} \tag{7}$$

嵌入时 $W=1$ 的位置叠加了 2α，$W=0$ 的位置叠加了 0，理想情况下差值分别为 2α 与 0；取中点 α 作为判决阈值，只要攻击噪声引起的差值波动不超过$\pm\alpha$，即可正确恢复水印比特。α 越大，判决容错能力越强、鲁棒性越好，但同时不可见性下降，二者通过 α 折中。

4. 实验

4.1. 实验设置

本次实验选取经典灰度测试图像 Lena、Baboon、Peppers 进行验证，这些图像来自公开的图像测试库，图像尺寸均为 512 × 512，实验平台为 Windows 11、Matlab2016b 和 Pycharm2024，版本为 Python3.8；嵌入的水印信息一为图 3 左图，水印信息二为图 3 右图，使用 DWT 和 Kyber 算法对图片进行加密并嵌入水印，采用峰值信噪比(PSNR)衡量不可见性、归一化相关系数(NC)和比特容错率(BER)衡量提取水印

的准确性和不可见性，PSNR 值越大、NC 越接近 1、BER 越小，说明方案的性能越好。在鲁棒性测试中，对含水印图像施加高斯噪声、椒盐噪声、模糊和 JPEG 压缩等常见攻击，并分别计算攻击后图像的 PSNR 值及水印的 NC 值，以验证所提方法在不同攻击条件下的性能。

本方案两个水印各占一个 64 × 64 子带，为进一步提高鲁棒性，另设 4 × 冗余配置：将 32 × 32 的水印按 2 × 2 平铺扩展为 64 × 64 后嵌入，提取时对每个 2 × 2 块做多数表决还原。



Figure 3. Watermark image
图 3. 水印图像

4.2. 实验结果分析

嵌入率 = 嵌入的 bit 数/载体图像像素个数，本方案的嵌入率为 0.03125。

首先小波变换后选取保留的小数位数为 2，加密图像并嵌入双水印，图 4 分别是原图、使用 Kyber 加密后的密文图像；图 5 分别是密文带水印图像和嵌入水印后的明文图像，图 6 是提取出来的水印图像，由于 Kyber 加密后会使密文膨胀，文中仅展示部分典型密文结构。图 4 中的密文图像上半部分为选取 HL3 4 × 32 加密过后的数据，下半部分为选取 LH3 4 × 32 加密过后的数据，重构形成完整的 u_1，u_2 和 v，其中 $u=(u_1,u_2)$，对于含水印的密文图像同理，上半部为水印 1 嵌入后的 HL3 部分，下半部分为水印 2 嵌入后的 HL3 部分。

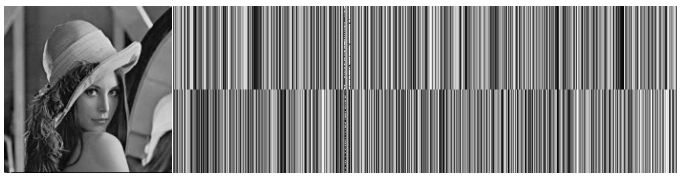


Figure 4. Plain image and encrypted image
图 4. 明文图像和密文图像

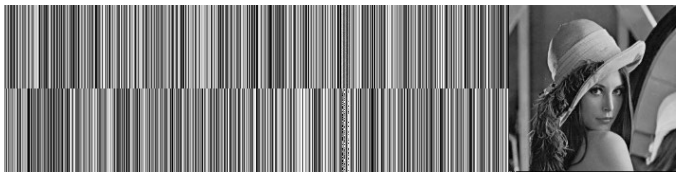


Figure 5. Cipher image with embedded watermark and the original image
图 5. 嵌入水印后的密文图像和明文图像



Figure 6. Extracted watermark image
图 6. 提取出的水印图像

4.3. 水印算法的性能测试

4.3.1. 水印性能与攻击测试

嵌入水印后图像的 PSNR 和 NC 值主要由嵌入强度 α 决定，在无攻击时 NC 值恒为 1，不受嵌入强度的影响。表 2 展示了同一幅图像，不同的 α 值对应的 PSNR 值以及两种典型攻击下提取的 NC。测试发现：当嵌入容量选取为 0.03125 时，α 值增大，图像的 PSNR 值呈现下降趋势，原因在于嵌入强度增大，对于载体系数引入的修改量也随之增大，从而导致图像质量下降。但 α 过小又会使图像受到攻击判决阈值低于攻击噪声，导致鲁棒性不足。

Table 2. PSNR (dB) and NC of different α values (Lena)
表 2. 不同 α 值的 PSNR (dB)和 NC (Lena)

α	PSNR	高斯 $\sigma = 10$ 的 NC1/NC2	椒盐 0.01 的 NC1/NC2
800	47.79	0.494/0.524	0.491/0.539
1200	44.27	0.734/0.734	0.584/0.621
1600	41.77	0.871/0.876	0.710/0.737

综合表 2 选取 $\alpha = 1200$，此时 PSNR 为 44.27 dB，显著高于 40 dB 的常规可接受阈值，含水印图像肉眼不可察觉；而高斯 $\sigma = 10$ 与椒盐 0.01 下的 NC 分别提升至 0.72 与 0.58 以上，较 $\alpha = 800$ 有大幅改善；继续增大 α 到 1600 所换取的鲁棒性增量已较有限，且以 PSNR 下降约 2.5 dB 为代价。因此本文选取 $\alpha = 1200$。

在 $\alpha = 1200$ 下，对含水印图像进行攻击并提取水印。实验结果如表 3 所示。

Table 3. Regular attack test
表 3. 常规攻击测试

攻击类型	冗余前 BER1/%	冗余前 BER2/%	冗余后 BER1/%	冗余后 BER2/%	NC1/NC2
无攻击	0.0	0.0	0.0	0.0	1/1
高斯 $\sigma = 5$	0.9	0.9	0.0	0.0	0.982/0.982
高斯 $\sigma = 10$	13.9	13.9	1.7	2.6	0.723/0.723
椒盐 0.01	20.8	19.0	5.2	4.5	0.584/0.621
椒盐 0.03	38.5	34.9	20.6	18.2	0.230/0.303
JPEG 70	0.0	0.0	0.0	0.0	1/1
JPEG 30	1.4	1.2	0.2	0.1	0.973/0.975
中值滤波 3 × 3	2.0	2.3	1.2	2.1	0.960/0.954
高斯模糊 3 × 3	1.4	1.7	1.4	2.1	0.972/ 0.966
缩放 0.5	2.8	3.7	2.9	3.5	0.945/0.927

从整体来看，在 JPEG 压缩下方案表现出很强的鲁棒性，即使质量因子降至 30，冗余后 BER 仍不超过 0.2%，NC 高于 0.97；对高斯噪声 $\sigma = 5$、中值滤波、高斯模糊和缩放攻击，冗余后 BER 均控制在 2% 以内、NC 不低于 0.94，两个水印之间无明显相互干扰。唯一明显的短板出现在高密度椒盐噪声(0.03)下，冗余后 BER 仍达 18%~20%，这是脉冲噪声对高频子带系数造成大范围翻转所致。

为验证方案鲁棒性与载体内容无关，在 $\alpha = 1200$ 下对四幅载体分别嵌入双水印并施加相同攻击，结

果如表 4 所示。

Table 4. Robustness under different carriers when $\alpha = 1200$
表 4. $\alpha = 1200$ 时不同载体下的鲁棒性

载体	Lena	Cameraman	Peppers
PSNR/dB	44.27	44.27	44.27
高斯 $\sigma = 10$ 冗余 BER1/%	1.7	2.2	2.0
椒盐 0.01 冗余 BER1/%	5.2	4.4	4.0
JPEG 30BER1/%	0.2	0.2	0.1
中值滤波 3 × 3BER1/%	2.0	0.6	1.5
高斯模糊 3 × 3BER1/%	1.4	2.1	1.5
缩放 0.5BER1/%	2.8	3.4	2.9

四幅载体的 PSNR 均为 44.27 dB，说明嵌入强度相同、不可见性一致。Lena、Cameraman、Peppers 三幅载体在各攻击下的 BER 与 NC 高度接近，表明方案鲁棒性基本与载体内容无关，具备较好的通用性。

4.3.2. 算法性能对比与局限性讨论

与其他加密域的水印算法文献[19]-[21]进行比较结果见表 5。文献[19]为双水印安全增强方向，本质上还是明文域水印；文献[20]为视频双水印，也属于明文域水印；文献[21]为密文域双水印文献，但是不能抵抗量子攻击。由表 5 可见，在无水印攻击时，以 512 × 512 的 Lena 灰度图像为例，选取保留小数位数为 2，α 为 1200，与文献[19]-[21]中的算法比较，本文水印算法的 PSNR 值为 44.27 dB，文献[19]和[20]的 PSNR 值分别为 36.71 dB，45.71 dB，本文算法求得的 PSNR 值，与其他算法相差较小，说明嵌入水印后的图像与原始图像差异较小，相较文献[21]，本文算法具有更高的鲁棒性。由此可见，本文算法的整体性能得到了改善。

Table 5. Comparison of this paper's algorithm with algorithms from other papers
表 5. 本文算法与其他文献算法比较

水印算法	含水印图像 PSNR (dB)	水印形式	提取水印(NC)
文献[19]	36.71	彩色图片	0.99
文献[20]	45.71	二值图像	0.98
文献[21]	85.27	二值图像	1/1
本文算法	44.27	0/1	1/1

5. 结论与展望

本文针对传统单水印算法在多方版权验证与量子计算下的不足，提出了一种基于 Kyber 同态加密与三层离散小波变换相结合的密文域同态双水印算法。该方法充分利用 Kyber 算法的加法同态特性，在图像变换域的高频子带中嵌入双水印信息，实现了在加密域内的水印嵌入，兼顾了图像加密安全性与水印的不可见性，并在遭受一定攻击后还能提取到水印。基于已完成的多水印算法，后续可将载体图像扩大，嵌入更多水印信息。

尽管本文所提出的算法在双水印嵌入与抗量子攻击方面取得了良好效果，但仍存在一些值得进一步研究和优化的方向，如后续工作应着重于提高水印嵌入的容量。

基金项目

国家自然科学基金(62472040)；北京市自然科学基金(L251065)；中国版权保护中心版权研究课题(BQ2024017)；2025 年京港澳高校交流项目。

参考文献

[1] Goswami, P., Faujdar, N., Debnath, S., Khan, A. and Singh, G. (2024) Investigation on Storage Level Data Integrity Strategies in Cloud Computing: Classification, Security Obstructions, Challenges and Vulnerability. *Journal of Cloud Computing*, **13**, Article No. 45. https://doi.org/10.1186/s13677-024-00605-z

[2] Kadian, P., Arora, S.M. and Arora, N. (2021) Robust Digital Watermarking Techniques for Copyright Protection of Digital Data: A Survey. *Wireless Personal Communications*, **118**, 3225-3249. https://doi.org/10.1007/s11277-021-08177-w

[3] Cheng, H., Huang, Q., Chen, F., Wang, M. and Yan, W. (2022) Privacy-Preserving Image Watermark Embedding Method Based on Edge Computing. *IEEE Access*, **10**, 18570-18582. https://doi.org/10.1109/access.2022.3151115

[4] Zhang, C., Ou, B., Peng, F., Zhao, Y. and Li, K. (2024) A Survey on Reversible Data Hiding for Uncompressed Images. *ACM Computing Surveys*, **56**, 1-33. https://doi.org/10.1145/3645105

[5] Jain, J., Jain, A., Srivastava, S.K., Verma, C., Raboaca, M.S. and Illés, Z. (2022) Improved Security of e-Healthcare Images Using Hybridized Robust Zero-Watermarking and Hyper-Chaotic System along with RSA. *Mathematics*, **10**, Article No. 1071. https://doi.org/10.3390/math10071071

[6] Kabir, F., Araghi, T.K. and Megías, D. (2024) Privacy-Preserving Protocol for High-Frequency Smart Meters Using Reversible Watermarking and Paillier Encryption. *Computers and Electrical Engineering*, **119**, Article ID: 109497. https://doi.org/10.1016/j.compeleceng.2024.109497

[7] Hernández-Joaquín, A., Melendez-Melendez, G. and Cumplido, R. (2023) A Secure DWT-Based Dual Watermarking Scheme for Image Authentication and Copyright Protection. *Multimedia Tools and Applications*, **82**, 42739-42761. https://doi.org/10.1007/s11042-023-14974-1

[8] Hu, Y., Jiang, X., Zhu, C., Ren, N., Guo, S., Duan, J., *et al*. (2024) A Dual Watermarking Algorithm for Trajectory Data Based on Robust Watermarking and Fragile Watermarking. *Computers & Geosciences*, **191**, Article ID: 105655. https://doi.org/10.1016/j.cageo.2024.105655

[9] Shor, P.W. (1994) Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *Proceedings* 35*th Annual Symposium on Foundations of Computer Science*, Santa Fe, 20-22 November 1994, 124-134. https://doi.org/10.1109/sfcs.1994.365700

[10] Li, S., Chen, Y., Chen, L., Liao, J., Kuang, C., Li, K., *et al*. (2023) Post-Quantum Security: Opportunities and Challenges. *Sensors*, **23**, Article No. 8744. https://doi.org/10.3390/s23218744

[11] Rivest, R.L. and Kaliski, B. (2025) RSA Problem. In: Jajodia, S., *et al*., Eds., *Encyclopedia of Cryptography, Security and Privacy*, Springer, 2144-2148. https://doi.org/10.1007/978-3-030-71522-9_475

[12] Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., *et al*. (2018) CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM. 2018 *IEEE European Symposium on Security and Privacy* (*EuroS&P*), London, 24-26 April 2018, 353-367. https://doi.org/10.1109/eurosp.2018.00032

[13] Chen, A.C.H. (2023) Homomorphic Encryption Based on Post-Quantum Cryptography. 2023 *IEEE International Conference on Machine Learning and Applied Network Technologies* (*ICMLANT*), 14-15 December 2023, 1-5. https://doi.org/10.1109/icmlant59547.2023.10372974

[14] Naem, S.A.S. and Hameed, S.M. (2025) Digital Watermarking Techniques, Challenges, and Applications: A Review. *Mesopotamian Journal of CyberSecurity*, **5**, 453-476.

[15] Zermi, N., Khaldi, A., Kafi, R., Kahlessenane, F. and Euschi, S. (2021) A DWT-SVD Based Robust Digital Watermarking for Medical Image Security. *Forensic Science International*, **320**, Article ID: 110691. https://doi.org/10.1016/j.forsciint.2021.110691

[16] Ahmadi, S.B.B., Zhang, G., Rabbani, M., Boukela, L. and Jelodar, H. (2021) An Intelligent and Blind Dual Color Image Watermarking for Authentication and Copyright Protection. *Applied Intelligence*, **51**, 1701-1732. https://doi.org/10.1007/s10489-020-01903-0

[17] 段昀霞, 李燕. 基于频域双水印的彩色医学影像隐私保护研究[J/OL]. 计算机应用与软件, 1-11. https://link.cnki.net/urlid/31.1260.tp.20250403.1552.002, 2025-12-11.

[18] 吕经浪, 李子臣. 基于 Kyber 的小数加法同态密码体制的研究[J]. 计算机技术与发展, 2024, 34(11): 101-108.

[19] Ma, J.Z., Yang, Y.G., Jiang, D.H. and Liao, X. (2024) Robust Double Encryption and Watermarking Algorithms for Color Watermark Images. *Physica Scripta*, **99**, Article ID: 125263. https://doi.org/10.1088/1402-4896/ad9183

[20] Zheng, J., Teng, S., Li, P., Ou, W., Zhou, D. and Ye, J. (2021) A Novel Video Copyright Protection Scheme Based on Blockchain and Double Watermarking. *Security and Communication Networks*, **2021**, Article ID: 6493306. https://doi.org/10.1155/2021/6493306

[21] 张爱娈, 李子臣. 基于 DWT 密文域图像双水印算法[J]. 计算机系统应用, 2021, 30(11): 164-171.