Software Engineering and Applications 软件工程与应用, 2022, 11(3), 504-515
Published Online June 2022 in Hans. http://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2022.113053

Hans汉斯

基于NTRU密文域图像可逆双水印算法的研究

张腾鲛，李子臣

北京印刷学院数字版权保护技术研究中心，北京

收稿日期：2022年4月3日；录用日期：2022年6月8日；发布日期：2022年6月15日

摘　要

本文基于NTRU密码算法对数字图像和字符串信息进行加密处理，利用NTRU密码算法的同态特性，实现不同用户在不同阶段对同一数字作品信息进行两次密文域水印信息嵌入；接收者对含水印的密文图像进行NTRU解密算法处理，能够恢复出原始作品信息和两次嵌入的水印信息。通过对比发现该算法能够完全恢复原始作品信息和嵌入的水印信息，能够达到预期效果。同时该算法基于后量子密码算法，可以对抗量子计算机的攻击，而且水印信息的嵌入量更大，能嵌入双方水印信息，嵌入和提取相互不受干扰和影响。

关键词

密文域水印算法，双方数字水印，NTRU同态密码算法，数字版权保护

Research on Image Reversible Double Watermarking Algorithm in Ciphertext Domain Based on NTRU

Tengjiao Zhang, Zichen Li

Digital Rights Management Research Center, Beijing Institute of Graphic Communication, Beijing

Received: Apr. 3rd, 2022; accepted: Jun. 8th, 2022; published: Jun. 15th, 2022

Abstract

In this paper, the digital image and string information are encrypted based on NTRU cryptographic algorithm. Using the homomorphic characteristics of NTRU cryptographic algorithm, different users can embed the watermark information in the ciphertext domain twice in different stages; the receiver can recover the original work information and the watermark information embedded

文章引用: 张腾鲛, 李子臣. 基于 NTRU 密文域图像可逆双水印算法的研究[J]. 软件工程与应用, 2022, 11(3): 504-515.
DOI: 10.12677/sea.2022.113053

twice by processing the ciphertext image with NTRU decryption algorithm. Through comparison, it is found that the algorithm can completely restore the original work information and embedded watermark information, and can achieve the expected effect. At the same time, the algorithm is based on post quantum cryptography algorithm, which can resist the attack of quantum computer, and the embedding amount of watermark information is larger. It can embed watermark information of both sides, and the embedding and extraction are not disturbed and affected by each other.

Keywords

Ciphertext Domain Watermarking Algorithm, Bilateral Digital Watermarking, NTRU Homomorphic Cryptographic Algorithm, Digital Copyright Protection

1. 引言

在互联网和数字媒体技术的发展下，我们的生活处处离不开数字技术，我们可以随时随地享有数字技术发展带来的方便。但与此同时也带来了新的问题和风险：数字信息在传播过程中容易被不法分子复制、篡改、恶意传播等，进而侵害个人、企业的合法权益，损害数字信息作品创作氛围，造成大量损失。所以数字信息版权保护问题迫切需要一种方案来解决。

在数字水印方面，传统的数字水印算法通常将载体图像变换到相应的频域空间，将水印信息对应嵌入在图像频域中，其中文献[1]中傅楚君等人提出了一种基于 DCT 变换的数字水印算法。文献[2]中胡坤等人提出了一种基于 BEMD 与 DCT 的彩色图像多重水印鲁棒算法。也有直接在空域直接进行水印信息嵌入操作，如文献[3]中王东东等人对 LSB 数字水印算法进行了研究与实现，其水印嵌入和提取效果也比较好，但算法的安全性不高，因此需要结合其他加密算法对待嵌入水印进行加解密，以此来提高水印信息的安全性。针对上述问题，文献[4]中 Zhang 等人较早地将加密技术和数字水印技术进行结合，设计出了一种在加密域进行数字水印信息嵌入的算法。而近些年得益于同态密码算法的发展，文献[5]中 Chen 等人提出在加密域应用公钥密码体制实现可逆数据隐藏方案，利用 Paillier 同态加密算法的同态性，将 1bit 的数据嵌入到两两一组的加密像素值中，解密方利用同态性质提取秘密信息。文献[6]中柯彦等人提出了一种基于 R-LWE (ring-learning with errors)加密系统的可逆数据隐藏方案，利用多项式环上的冗余空间进行大容量数据嵌入。文献[7]中周能等人使用 NTRU 加密系统实现加密域可逆数据隐藏，其中预处理采用的算法是差值扩展算法，数据隐藏利用了 NTRU 加密系统同态加法的性质，但是该方案在加密域平均嵌入率较低。文献[8]中 Zhou 等人提出了一种经 NTRU 加密后的对密文图像进行数据隐藏的算法，加密前对明文图像进行分组，计算组内参考点与相邻点的差值，通过建立差值直方图的方法确定隐藏像素点，利用 NTRU 加密系统的同态加性完成数据嵌入，可实现解密前和解密后都可以提取数据。文献[9]中项世军等人首次提出同态加密域图像可逆水印算法。

在同态加密算法方面，当前被广泛使用的同态加密算法包括 Paillier 同态加密[10]、BGV 同态加密[11][12]、BFV 同态加密[13]、NTRU 同态加密[14]等。其中 NTRU 同态密码算法相比于其他同态密码算法具有结构简洁、计算速度较快、尺寸较小等优点，因此比较适合应用于数字水印算法。

综合上述分析，将数字水印算法和同态加密算法相结合是当前数字水印研究领域的热点。当前大部

分水印方案是将传统加密技术和数字水印结合，虽然能提高数字水印嵌入提取的安全性，但是由于加密算法本身的特性不便于进行第二次水印的嵌入，且加密和嵌入数据时运算开销较大，导致嵌入大量数据时程序运行时间较长。另外，随着量子计算的发展，传统加密算法能否抵抗量子计算攻击也是加密域可逆数据数字水印领域备受讨论的问题。NTRU 加密系统被认为是可抵抗量子计算攻击的一种同态加密系统，且具有公私钥生成速度快、加解密运算速度快等特点，基于 NTRU 加密系统的可逆数字水印算法运算时间明显优于其它同态加密系统[15]。

本文基于 NTRU 同态密码算法提出了一种可逆双方水印算法，该算法不同于传统的数字水印算法，首先图像信息所有者通过 NTRU 同态密码算法的加密算法对嵌入第一段水印的图像信息进行加密并上传至云端管理员处。云端管理员通过 NTRU 同态密码算法的同态特性进行第二次水印信息嵌入。最后水印信息验证者可以通过 NTRU 解密算法提取原始图像信息和两次嵌入的水印信息。本方案优点在于算法安全性较高，算法运行时间较短，且扩展性也比较好，可根据需要多次嵌入数字水印信息。经过实验证明，该算法解密恢复原始信息的效果比较好，能够完全恢复出原始图像和两次嵌入的水印信息。

本文的整体结构安排如下：

第 2 节：NTRU 算法及同态特性分析；

第 3 节：基于 NTRU 密文域多方水印算法设计；

第 4 节：实验与分析；

第 5 节：总结。

2. NTRU 算法及同态特性分析

2.1. NTRU 算法

NTRU 加密系统最早由三位数学家 Jill Pipher，Jeffrey Hoffstein，Joseph Silverman 提出[14]。这种加密系统的数学核心是多项式环截断环，加密系统的可靠性由格上最短向量问题和最近向量问题保证，这属于 NP 难(non-deterministic polynomial hard)问题。由于加密和解密过程中只运用到简单的模乘与加减运算，在相同安全性等级的前提下，NTRU 比目前现有的公钥密码系统运算更快，效率更高，具有很广阔的应用前景。

2.1.1. NTRU 密码体制及其基本运算操作

NTRU 算法定义在多项式环 $R=\dfrac{\mathbb{Z}[X]}{X^N-1}$ 上，R 上的元素——多项式 $f(x)$ 也可以用向量表达：$f=\sum_{i=0}^{N-1}f_i\cdot x^i=[f_0,f_1,\cdots,f_{N-1}]$。对于环中的任意两个多项式 $f(x)$ 和 $g(x)$ 可以表示为以下的形式：$f=f_0+f_1\cdot x+\cdots+f_{N-1}\cdot x^{N-1}$，$g=g_0+g_1\cdot x+\cdots+g_{N-1}\cdot x^{N-1}$。元素之间存在多种运算，包括：

系数乘法操作：对于任意实数 $k\in R$，满足 $k\cdot f(x)=k\cdot f_0+k\cdot f_1\cdot x+\cdots+k\cdot f_{N-1}\cdot x^{N-1}$

多项式加法操作：对于两个多项式截断环 f 和 g 之间的加法定义如下：

$$f(x)+g(x)=\sum_{i=0}^{N-1}(f_i+g_i)\cdot x^i \tag{2-2}$$

多项式乘法操作：对于两个多项式截断环 f 和 g 之间的乘法(星乘)定义如下：

$$f(x)*g(x)=\sum_{i=0}^{N-1}\left(\sum_{i+j=k(\mathrm{mod}\,N)}f_i\cdot g_j\right)\cdot x^i \tag{2-3}$$

2.1.2. NTRU 加解密参数

NTRU 密码体制由 3 个正整数 (N,p,q) 和 4 个整系数多项式集合 L_f,L_g,L_r 和 L_m 共同决定。其中正整

数 p 和 q 的选取满足 $\gcd(p,q)=1$ 且 q 远大于 p。用“*”乘表示环 R 中的乘法，在整个密码系统中，一部分乘法将在模 q 下运算，另一部分将在模 p 下运算。多项式 L_f, L_g, L_r 和 L_m 的选取应遵循以下原则：明文 m 所选取的集合 L_m 是包括所有模 p 的多项式。这里为了方便讨论，假设 p 是奇数，于是有

$$L_m=\left\{m\in R: m\text{的系数位于}-\frac{p-1}{2}\text{和}\frac{p-1}{2}\text{之间}\right\}。$$

另外 3 个多项式集合均采用如下形式：

$$L(d_1,d_2)=\{F\in R: F\text{中有}d_1\text{个系数等于}1, d_2\text{个系数等于}-1, \text{剩下的系数为}0\}$$

因此，3 个正整数 d_f, d_g 和 d_r 便可确定参数选取集合：$L_f=L(d_f,d_f-1)$，$L_g=L(d_g,d_g)$，$L_r=L(d_r,d_r)$。

2.1.3. NTRU 算法加密解密过程

首先根据参数 d_f 生成多项式 f，其必须满足 f 模 p 的逆 f_p^{-1} 和 f 模 q 的 f_q^{-1} 逆存在，否则重新生成 f。然后计算 f_p^{-1} 和 f_q^{-1}。最后根据参数 d_g 生成多项式 g。根据公式(2-4)计算多项式 h：$h=p\cdot F_q*g\pmod q$。当计算全部完成后，可得到公钥为 $K_{pub}=h$，私钥为 $K_{pri}=(f,f_p)$。

加密过程：是在加密数据信息前需要将数据信息编码为明文多项式，使其每个系数的范围为 $\left[-\frac{p}{2},\frac{p}{2}\right]$，如当 $p=3$ 时，明文多项式 m 的系数范围是 $\{-1,0,1\}$。获取公钥 h 后，即可对明文多项式 $m\in L_m$ 进行加密，随机选取噪声多项式 $r\in L_r$，对明文 m 根据以下公式操作得到密文多项式 e：$e=r*h+m\pmod q$。

解密过程：给定密文多项式 e 和私钥 (f,f_p) 可以解密得到明文多项式 m。首先根据公式 $a=f*e\pmod q$ 计算中间多项式 a。然后根据公式 $c=F_p*a\pmod p$ 计算得到解密后的明文多项式 c。最后再根据明文编码规则进行逆编码即可得到明文数据 data。

2.1.4. NTRU 安全等级

Silverman 等人给出了 NTRU 不同的参数选取方案，以此来获得不同的安全等级。在 NTRU 公钥密码的原始方案中，$N=107$ 规模的参数对应了中等安全性密码系统。表 1 是 NTRU-1998 参数集对应的安全性等级[14]。

Table 1. Recommended parameters for different security levels of NTRU
表 1. NTRU 不同安全性等级的推荐参数

安全等级	N	p	q	d_f	d_g	d_r
中等安全性	107	3	64	15	12	5
高安全性	167	3	128	61	20	18
最高安全性	503	3	256	216	72	55

2.2. NTRU 同态性质

NTRU 存在加法同态性：对于任意的两个明文多项式 m_1 和 m_2，选择两个随机的多项式 r_1 和 r_2，则经过加密之后对应生成的密文为 e_1 和 e_2，其中满足：

密文相加时：$e_1+e_2=(r_1+r_2)*h+m_1+m_2\pmod q$

解密时：$Dec(e_1+e_2)=m_1+m_2\pmod q$

即两个密文多项式的之和在解密后等于对应的两个明文多项式之和：

假设明文 $PT' = \sum_{i=0}^{N-1} pt_i' \cdot x^i = \left[pt_0', pt_1', \cdots, pt_{N-2}', pt_{N-1}'\right]$；

明文 $PT'' = \sum_{i=0}^{N-1} pt_1'' \cdot x^i = \left[pt_0'', pt_1'', \cdots, pt_{N-2}'', pt_{N-1}''\right]$；

经过 NTRU 加密后分别得到：

密文 $CT' = \sum_{i=0}^{N-1} ct_i' \cdot x^i = \left[ct_0', ct_1', \cdots, ct_{N-2}', ct_{N-1}'\right]$；

密文 $CT'' = \sum_{i=0}^{N-1} ct_i'' \cdot x^i = \left[ct_0'', ct_1'', \cdots, ct_{N-2}'', ct_{N-1}''\right]$；

同态加操作：$CT^* = \sum_{i=0}^{N-1} \left(ct_i' + ct_i''\right) \cdot x^i = \left[ct_0' + ct_0'', ct_1' + ct_1'', \cdots, ct_{N-2}' + ct_{N-2}'', ct_{N-1}' + ct_{N-1}''\right]$；

对密文 CT^* 解密后得到明文结果如下：

$$PT^* = \sum_{i=0}^{N-1} \left(pt_i' + pt_i''\right) \cdot x^i = \left[pt_0' + pt_0'', pt_1' + pt_1'', \cdots, pt_{N-2}' + pt_{N-2}'', pt_{N-1}' + pt_{N-1}''\right]$$

3. 双水印算法设计

本文提出的方案充分利用 NTRU 加密系统的多项式空间冗余性以及 NTRU 加密的同态性。原始信息所有者将原始信息加密后将得到一些密文多项式，其他用户可以在不同阶段将密态信息嵌入到密文多项式中。掌握私钥的用户则可以对密文解密，解密后将获取原始信息和其他用户嵌入的信息。

3.1. 算法流程

本文提出了一种基于 NTRU 的密文域双方数字水印算法，该算法主要由四部分构成：原始图像信息和字符串水印信息加密、图像水印信息加密、第二段水印信息嵌入、解密提取原始图像和双水印信息。

本算法包括图像作品拥有者 A、云端管理者 B 和水印信息验证者 C 三种用户。

第一步：图像作品拥有者 A 嵌入字符串水印信息并加密图像，得到含水印密文图像 P_1；

第二步：云端管理员 B 加密水印图像，得到密文水印图像 P_2；

第三步：云端管理员 B 向含水印密文图像 P_1 嵌入第二段水印信息 P_2；

第四步：水印信息验证者 C 双水印验证者 C 解密密文图像并提取原始图像和先后嵌入的两段水印信息。

方案流程图如图 1 所示。

3.2. 信息编码与加密解密

3.2.1. 字符串信息编码

对于字符串类型的数据，要将其每一个字符都编码成 8 比特(1 个字节)的二进制形式，然后按顺序依次填充到多项式对应的系数上，构造出相应的明文多项式。

3.2.2. 图像信息编码

在数字图像中，一个点通常用像素来表示，一个字节包含 8 个比特，每个比特可以表示为 1 或者 0。在简单的二值图像中一个像素点由一个字节来表示。而复杂一些的图像(例如 24 位真彩色 BMP)，一个像素由三个字节构成，每个字节分别表示 256 种状态的红、绿、蓝。本算法针对彩色图像进行信息加密，因此在编码明文多项式时，需要将像素点转化为二进制字符串并填充到明文多项式对应系数上。

3.2.3. 加密明文多项式

图片或字符串信息经过编码后得到若干个明文多项式，对每一段明文多项式执行 NTRU 加密算法后将得到对应的密文多项式。

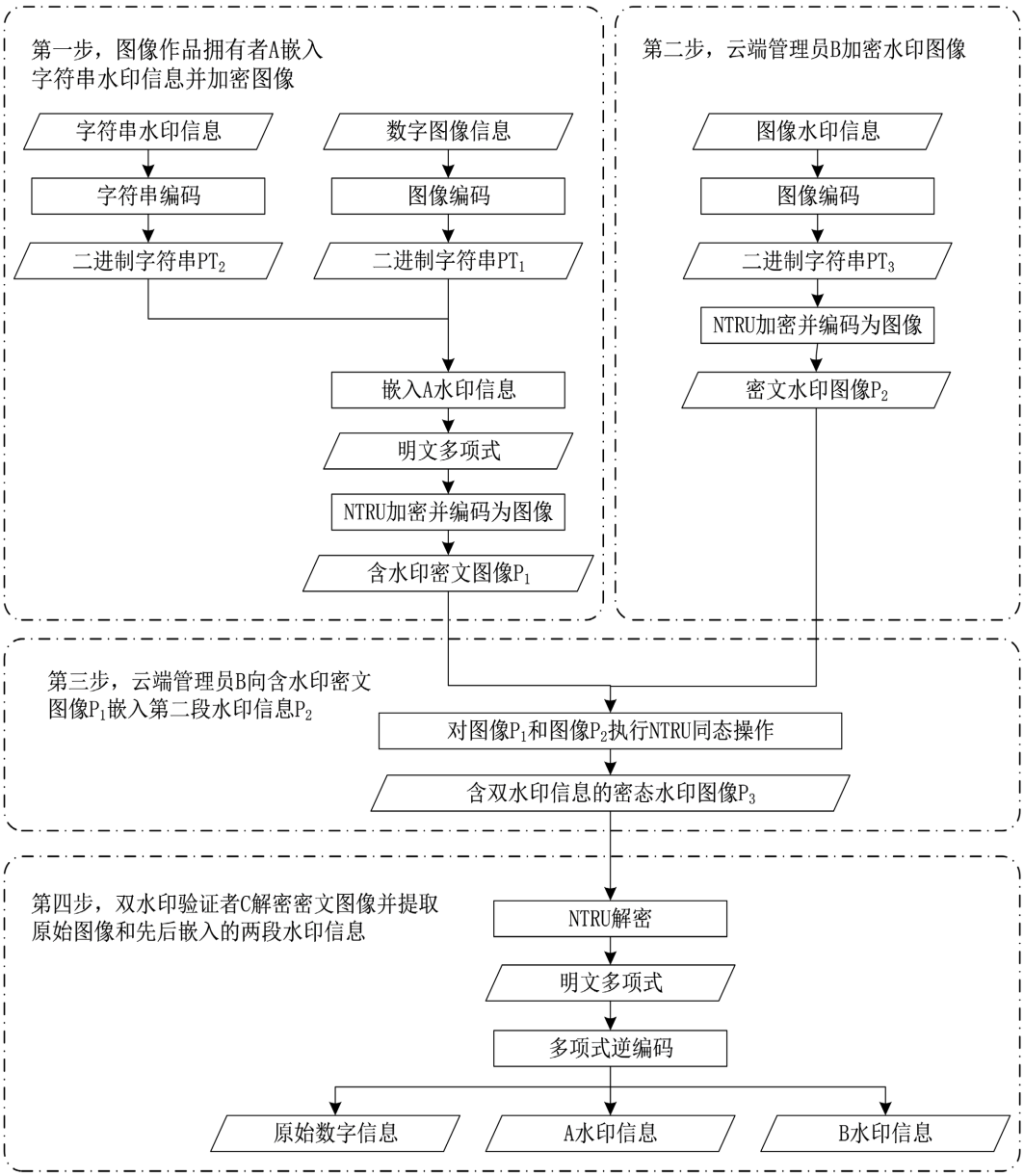


Figure 1. Flowchart of double watermarking algorithm in ciphertext domain based on NTRU
图 1. 基于 NTRU 密文域双水印算法的流程图

3.2.4. 解密密文多项式

解密方得到密文多项式后，使用私钥对其执行 NTRU 解密算法。以中等安全系数($N = 167$)为例，对于解密后得到的每一段明文多项式，都由三部分组成：前 96 个系数代表原始数字图像的 4 个像素信息、中间 32 个系数代表第一段水印信息(字符串)、之后的 24 个系数代表第二段水印信息(图像)的 1 个像素信息。将这些信息按照 3.2.1 节中的编码格式进行还原可以得到原始图像信息和水印信息(包括字符串和图像水印信息)。

3.3. 具体过程

以中等安全等级($N = 167$)为例，每个多项式有 167 个系数可以嵌入数据。

3.3.1. 图像作品拥有者 A 嵌入字符串水印信息并加密图像

首先图像作品拥有者 A 对原始数字图像信息进行编码，每 4 个像素点为一组，构造出长度为 96 的二进制字符串。从多项式的第 1 个系数开始，将 96 个二进制数依次置入明文多项式(不足 4 个像素点则需要填充 0)。经过处理后，每四个像素点信息都将产生一个多项式形式的明文。然后将字符串水印信息也编码为二进制字符串，每 4 个字符(32 比特)为一组，从明文多项式的第 97 个系数到第 128 个系数依次置入二进制字符串信息。其他字符串信息以同样的方式依次置入下一个明文多项式。鉴于原始图像的像素信息比较多，因此能够构造出多个明文多项式，对于每个明文多项式具体填充形式如图 2 所示。

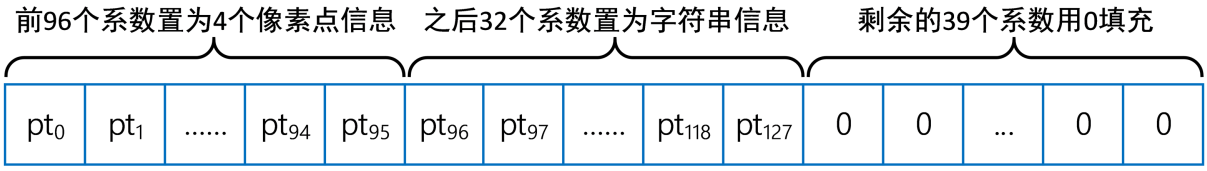


Figure 2. Schematic diagram of encoding original image and string watermark information
图 2. 对原始图像和字符串水印信息编码示意图

之后对每个明文 PT_i 都经过 NTRU 密码算法加密，每个明文 PT_i 都将产生对应的密文 CT_i，每个密文也是以多项式的形式表达，如图 3 所示。最后将得到的密文编码为图像信息并发送给云端管理员 B。

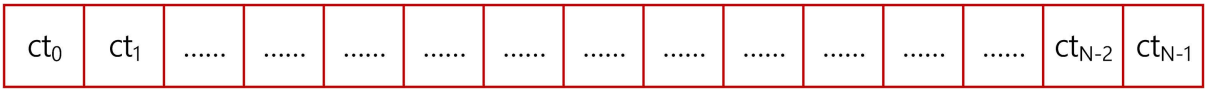


Figure 3. Schematic diagram of ciphertext polynomial
图 3. 密文多项式示意图

每个多项式除前 128 位外，剩余的位置均未置入其他有效信息，多项式系数具有一定的冗余度。云端管理员 B 将在冗余的系数上嵌入第二段水印信息(图像水印)。

3.3.2. 云端管理员 B 加密水印图像

云端管理员需要将每个明文多项式的前 128 位置为 0，水印图像的信息将嵌入在多项式中剩余的位置上。将水印图像的每个像素点信息(24 位)编码成以二进制形式表示的字符串，每个明文多项式从第 129 位开始置入像素信息。对图片的所有像素信息采用同样的处理后将构造出多个多项式形式的明文。对于一个具体的明文，其填充方式如图 4 所示。

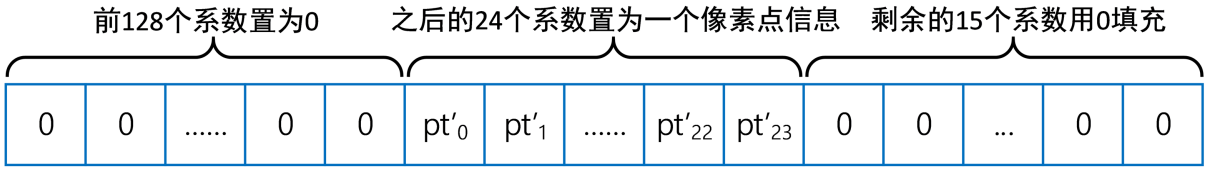


Figure 4. Constructing plaintext polynomial of watermark image in cloud
图 4. 云端构造水印图像的明文多项式

之后对每组明文执行 NTRU 密码算法加密，每个明文都将产生对应的密文 CT_i'。最后将得到的密文编码为图像信息。

3.3.3. 云端管理员 B 嵌入第二段水印信息

云端管理员 B 此时持有来自双方的密文图像信息，下一步将同态地处理密文图像信息，进而计算得

到带有原始图像、字符串水印和图片水印的密文图像，如图 5。具体操作是将密文多项式进行同态加法运算，即 $CT_i^* = CT_i + CT_i'$ 。

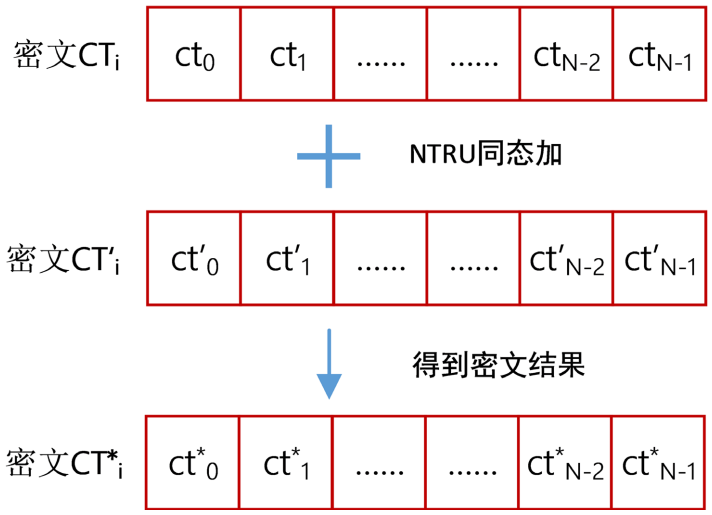


Figure 5. The cloud administrator performs homomorphic addition on ciphertext
图 5. 云端管理员对密文执行同态相加操作

3.3.4. 水印信息验证者 C 解密提取原始图像和双水印信息

水印信息验证者 C 从密文图像中提取密文并进行解密后，将得到对应的明文，每个明文多项式系数的前 24 位为原始图像像素信息，第 25 位到第 72 位为字符串水印信息，剩余的系数为云端管理员嵌入的图像水印信息(每 24 比特表示一个像素信息)，具体结构如图 6。根据原来的编码方式进行逆编码，我们将还原出原始图像信息、字符串水印信息和图像水印信息。

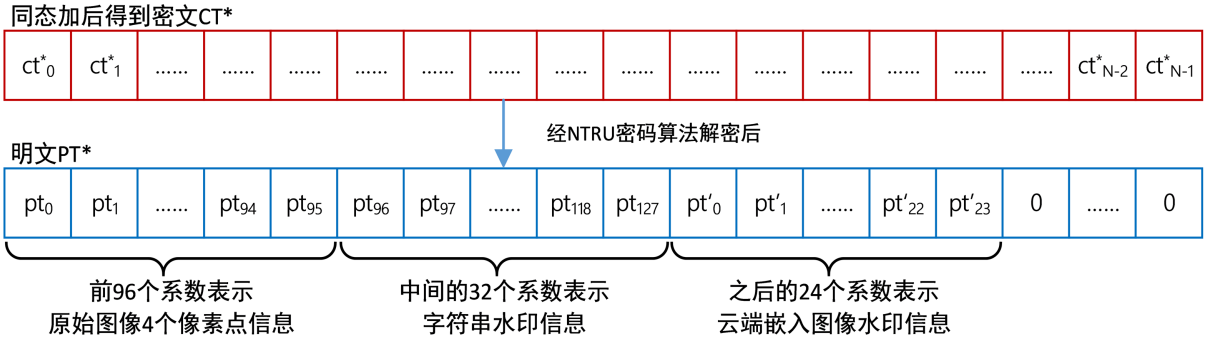


Figure 6. The decryptor provides the private key for decryption
图 6. 解密方提供私钥进行解密

4. 实验与分析

4.1. 实验过程

本文首先以彩色 Lena 图像(如图 7 所示)作为原始图像、原始图像的摘要值(MD5)作为字符串水印和彩色“数字水印”图像(如图 8 所示)作为水印图像进行实验。其中彩色 Lena 图像的像素大小为 256 * 256；字符串水印信息为该 Lena 图像的 MD5 值：27bf9f58bd64ad14c76345c5ec771b19，彩色 BIGC 图像的像素大小为 50 * 50。

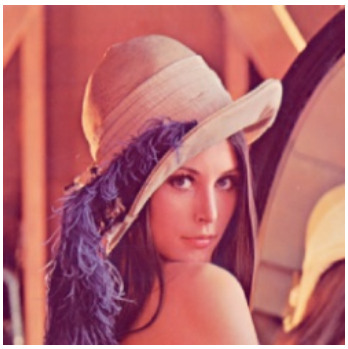
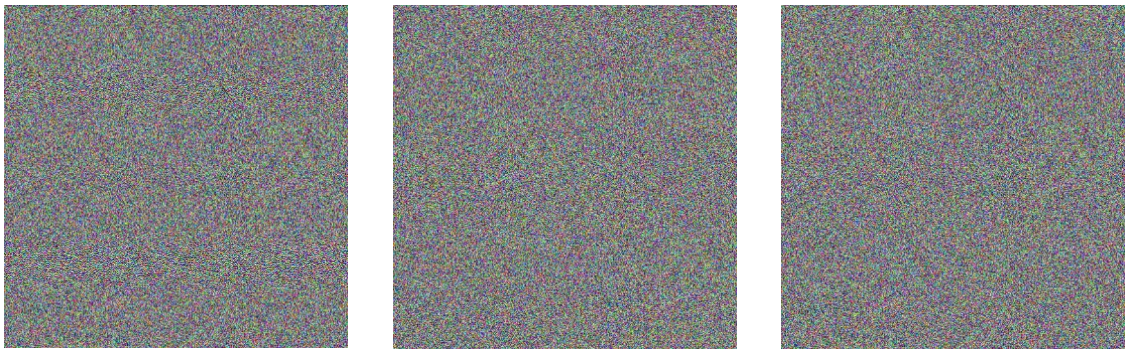


Figure 7. Original image information
图 7. 原始图像信息

Figure 8. Image watermark information
图 8. 图像水印信息

实验中采取最高安全性等级(N = 503)参数进行实验，实验中原始图像信息经 NTRU 加密算法，产生了 3450 组密文多项式，将这些密文多项式编码为数字图像信息后得到含字符串水印的密文图像 P_1 (如图 9(a))。云端管理员加密数字水印图像信息产生了 2500 组密文多项式。同样地将这些密文多项式编码为数字图像信息后得到图像水印的密文图像 P_2 (如图 9(b))。对这两个密文图像进行 NTRU 同态相加操作，得到含双水印信息的密文图像 P_3 (如图 9(c))。



(a) (b) (c)

Figure 9. (a) Ciphertext Image P_1; Ciphertext Image P_2; Ciphertext Image P_3
图 9. (a) 密文图像 P_1；(b) 密文图像 P_2；(c) 密文图像 P_3

对经过同态求和算法得到的含有双方水印信息的密文图像 P_3 进行直方图统计(如图 10)可以看出每个像素点的分布服从较好的随机分布，因此该算法具有较好的安全性。

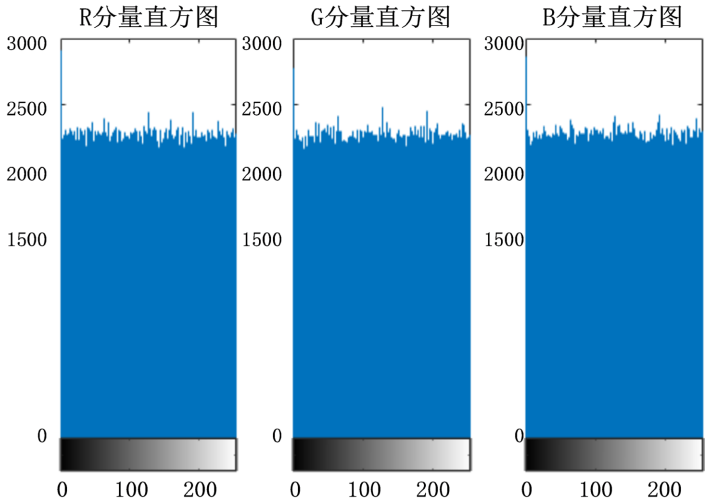


Figure 10. Histogram statistical results of watermark image containing both watermark information
图 10. 含双方水印信息的水印图像的直方图统计结果

密文信息解密和信息提取阶段：

解密时，需要先将密文图像编码为相应的密文多项式。对这些密文多项式执行 NTRU 解密算法，最终得到 3450 组包含原始图像信息、字符串水印信息、图像水印信息的明文多项式。再对其进行逆编码，将恢复出原始图像信息(如图 11 所示)、字符串水印信息(27bf9f58bd64ad14c76345c5ec771b19)、图像水印信息(如图 12 所示)。

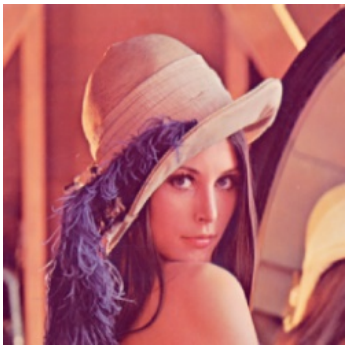


Figure 11. Recover the original image information after decryption
图 11. 解密后还原得到的原始图像信息

Figure 12. Recover the image watermark information after decryption
图 12. 解密后还原得到的图像水印信息

经比较，解密恢复得到的字符串水印信息与原字符串水印信息一致，解密恢复得到的图像信息和图像水印信息与原始图像一致。对原始图像和解密恢复得到的图像进行 PSNR 对比，结果显示经过该算法并解密后得到图像信息与原来的图像信息完全一致，因此该算法能够完全恢复原始图像和水印信息。

4.2. 运行效率

经实验测试得到对编码后的 2048 个明文多项式执行 2048 次 NTRU 加密运行时间、解密运算时间、同时执行加解密和文件编码解码所需要总的时间开销如表 2 所示：

Table 2. Time cost of encrypting and decrypting 2048 polynomials under different security levels of NTRU
表 2. NTRU 不同安全性等级下对 2048 个多项式进行加解密时间开销

安全等级	N	加密时间(秒)	解密时间(秒)	总时间(秒)
中等安全性	107	68.07	51.01	136.14
高安全性	167	126.10	95.54	264.46
最高安全性	503	343.55	335.23	743.20

通过实验分析可以看出，进行合理的参数选择和多项式系数分配将有效利用明文多项式的系数，进而减少因构造多项式过多带来空间和时间上的开销，提高运行效率。当选择最高安全性等级时，虽然单次加解密时间是最长的，但是一次可以填充多个系数，加解密所需要的空间开销和时间开销是最低的。

4.3. 安全性分析

本方案是基于 NTRU 加密算法实现的，文献[15]证明了 NTRU 算法的正确性和安全性，其安全性可规约到格上 SVP (Shortest Vector Problem)问题[16]和 BDD (Bounded Distance Decoding)问题[17]。同时在标准模型下是 IND-CPA(选择明文攻击下的不可区性)安全的[18]。

原始图像所有者和云管理员都需要对嵌入信息进行 NTRU 加密算法加密，任意阶段产生的密态水印信息——密文多项式都需要 NTRU 私钥进行解密后才能提取原始信息，因此该方案具有等价于 NTRU 加密系统的安全性。通过对比 NTRU、RSA 和 ECC 三种公钥密码体制之间的安全级别[14]，NTRU 在相同安全性等级下密钥都短于另外两种公钥密码体制，同时其加解密速度也优于另外两种公钥密码体制。进行暴力破解攻击时，随着 N 的增大，因花费时间太长而基本不能破解[14]。因此，NTRU 加密体制能够提供足够的安全性能。

5. 总结

本文提出了一种基于 NTRU 密文域图像可逆双水印算法，该算法不同于传统的水印嵌算法嵌入提取以及密文的存储形式都是在多项式上进行。图像作品拥有者加密图像和字符串水印信息后，云端管理员可以随时将图片水印信息加密后嵌入到用户上传的密文多项式中，持有私钥的双水印信息验证者在对密文多项式解密后将得到原始图像、字符串水印信息、图片水印信息。同时，本方案可以根据不同环境需要，对明文多项式信息嵌入位置进行进一步设计，可以嵌入更多次水印信息，具有很好的扩展性。

与传统的水印信息嵌入提取算法相比，该算法综合嵌入率较高，并且多项式系数位嵌入时具有较高的灵活性。相比于其他后量子密码算法具有密钥长度短、执行速度快、安全强度高等优点。

但由于 NTRU 加密系统本身固有的小概率解密失败的问题，可能会造成图像水印信息中个别像素点不能正确恢复的情况发生。因此需要进一步研究 NTRU 解密算法的准确性问题，以提高本方案的准确性。

基金项目

国家自然科学基金(61370188)；北京市教委科研计划(KM202010015009)；北京市教委科研计划资助(No. KM202110015004)；北京印刷学院博士启动金项目(27170120003/020)；北京印刷学院科研创新团队项目(Eb202101)；北京印刷学院校内学科建设项目(21090121021)；北京印刷学院重点教改项目(22150121033/009)；北京印刷学院科研基础研究一般项目(Ec202201)。

参考文献

[1] 傅楚君, 兰胜坤. 基于 DCT 变换的数字水印算法[J]. 网络安全技术与应用, 2020(7): 49-51.

[2] 胡坤, 李聪, 胡建平, 王小超, 杜玲, 王红飞. 基于 BEMD 与 DCT 的彩色图像多重水印鲁棒算法[J/OL]. 北京航空航天大学学报, 1-16. https://doi.org/10.13700/j.bh.1001-5965.2021.0214

[3] 王东东, 王福明. 基于 LSB 数字水印算法的研究与实现[J]. 山西电子技术, 2014(5): 76-77.

[4] Zhang, X. (2011) Reversible Data Hiding in Encrypted Image. *IEEE Signal Processing Letters*, **18**, 255-258. https://doi.org/10.1109/LSP.2011.2114651

[5] Chen, Y.C., Shiu, C.W. and Horng, G. (2014) Encrypted Signal-Based Reversible Data Hiding with Public Key Cryptosystem. *Journal of Visual Communication and Image Representation*, **25**, 1164-1170. https://doi.org/10.1016/j.jvcir.2014.04.003

[6] Ke, Y., Zhang, M. and Su, T. (2016) A Novel Multiple Bits Reversible Data Hiding in Encrypted Domain Based on R-LWE. *Journal of Computer Research & Development*, **53**, 2307-2322.

[7] Zhou, N., Zhang, M.Q., Zhou, H.N., *et al*. (2020) Reversible Data Hiding Algorithm in Encrypted Domain Based on NTRU. *Science Technology and Engineering*, **20**, 13285-13294. (in Chinese)

[8] Zhou, N., Zhang, M., Wang, H., *et al*. (2020) Separable Reversible Data Hiding Scheme in Homomorphic Encrypted Domain Based on NTRU. *IEEE Access*, **8**, 81412-81424.

[9] 项世军, 罗欣荣, 石书协. 一种同态加密域图像可逆水印算法[J]. 计算机学报, 2016, 39(3): 571-581.

[10] Paillier, P. (1999) Public-Key Cryptosystems Based on Discrete Logarithms Residues. *Advances in Cryptology-Eurocrypt'99*, *International Conference on the Theory and Application of Cryptographic Techniques*, *Prague*, *Czech Republic*, 2-6 May 1999, 223-238.

[11] Brakerski, Z. and Vaikuntanathan, V. (2014) Efficient Fully Homomorphic Encryption from (Standard) Lwe. 2011 *IEEE 52nd Annual Symposium on Foundations of Computer Science*, pp. 97-106.

[12] Gentry, C. (2009) Fully Homomorphic Encryption Using Ideal Lattices. *STOC*, **9**, 169-178. https://doi.org/10.1145/1536414.1536440

[13] Fan, J. and Vercauteren, F. (2012) Somewhat Practical Fully Homomorphic Encryption. *Iacr Cryptology ePrint Archive*, **2012**, 144.

[14] Hoffstein, J., Pipher, J. and Silverman, J.H. (1998) NTRU: A Ring-Based Public Key Cryptosystem. In: Buhler, J.P., (Ed.), *Algorithmic Number Theory*, Springer, Heidelberg. https://doi.org/10.1007/BFb0054868

[15] Wu, H.T., Cheung, Y., Yang, Z., *et al*. (2019) A High-Capacity Reversible Data Hiding Method for Homomorphic Encrypted Images. *Journal of Visual Communication and Image Representation*, **62**, 87-96. https://doi.org/10.1016/j.jvcir.2019.04.015

[16] Ajtai, M. (1996) Generating Hard Instances of Lattice Problems. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, Philadelphia, 1996, 99-108. https://doi.org/10.1145/237814.237838

[17] Regev, O. (2009) On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *Journal of the ACM*, **56**, 1-40. https://doi.org/10.1145/1568318.1568324

[18] Li, Z.C., Zhang, J.M., Yang, Y.T., *et al*. (2018) A Fully Homomorphic Encryption Scheme Based on NTRU. *Agta Electronica Sinca*, **46**, 938-944. (in Chinese)