**引 用 格 式**：Wang Xiucheng, Zhang Liming. A Digital Fingerprinting Scheme for Remote Sensing Images based on the Homomorphic Public Key Encryption Algorithm[J]. Remote Sensing Technology and Application, 2022, 37(2): 532-538.[王修成，张黎明. 一种基于同态公钥加密的遥感影像数字指纹方案[J]. 遥感技术与应用，2022，37(2)：532-538.]

DOI：10.11873/j.issn.1004-0323.2022.2.0532

# 一种基于同态公钥加密的遥感影像数字指纹方案

王修成[1,2,3]，张黎明[1,2,3]

（1.兰州交通大学 测绘与地理信息学院，甘肃 兰州 730070；
2.地理国情监测技术应用国家地方联合工程研究中心，甘肃 兰州 730070；
3.甘肃省地理国情监测工程实验室，甘肃 兰州 730070）

**摘要**：针对非对称指纹计算复杂性高以及带宽效率低的问题，提出了一种基于同态公钥加密的遥感影像非对称指纹方案。在该方案中，内容提供商通过DCT扩频置乱方法加密遥感影像，运用Bresson同态公钥加密来实现解密密钥的非对称分发，通过客户端解密含指纹的遥感影像拷贝，使不同的解密密钥能够生成不同的含指纹拷贝。方案中公钥加密算法并未直接加密遥感影像，由此降低了计算复杂性并提高了加密效率；同时因为内容提供商只需为多个消费者生成相同的指纹拷贝，通过多播传输将其分发给不同的消费者，因此降低了带宽需求。实验表明：在用户数量较大的情况下，该方案可以有效提高带宽效率及加密效率，能够显著降低数据服务器的计算负载，减少用户等待时间。

**关 键 词**：非对称指纹；同态公钥加密；遥感影像；多播传输；带宽效率

**中图分类号**：TP79 **文献标志码**：A **文章编号**：1004-0323(2022)02-0532-07

## 1 引 言

随着遥感技术的快速发展，遥感影像在国防军事建设，现代化建设，科学研究等领域中应用广泛，其经济价值、社会价值日益凸显[1]。然而伴随遥感影像的广泛应用，泄密、侵权及盗版等问题也日益突出，解决该问题成为信息安全领域研究的热点。

目前有关遥感影像的安全保护技术，从保护方式上可分为事后追究与事先防范两大类。数字水印和数字指纹技术都属于事后追究技术，它们通过在遥感影像中嵌入版权信息或用户标识信息等，必要的时候提取出嵌入的水印信息，可以有效解决遥感影像的版权保护问题。数字水印和数字指纹技术已经发展成为测绘成果版权认证、使用跟踪、内容认证等方面的一种有效手段[2]。与数字水印技术相比，数字指纹技术能够从盗版的数字拷贝中追踪到原始的购买者（盗版者），因此，数字指纹技术在数字产品版权保护中更具优势。

数字指纹方案可以分为3种基本类型：对称指纹方案，非对称指纹方案及匿名指纹方案[3]。区别对称指纹方案与非对称指纹方案的主要依据是判断指纹拷贝的生成过程中是否需要消费者的参与。匿名指纹方案是在非对称指纹的基础上实现了消费者的匿名性，因此，可以把匿名指纹方案归属到非对称指纹方案中。在对称指纹方案中，指纹的生成和嵌入由内容提供商单方面完成，内容提供商及消费者都保有相应的指纹拷贝，因此不诚实的内容提供商可能恶意多次分发含用户指纹的拷贝来诬

**收稿日期**：2021-04-14；**修订日期**：2022-02-21

**基金项目**：国家自然科学基金项目“面向内容的矢量地图数据认证与版权保护方法研究”(41761080)，甘肃省高等学校产业支撑引导项目“地理空间数据数字指纹系统集成及应用示范”(2019C-04)。

**作者简介**：王修成(1994-)，男，甘肃兰州人，硕士研究生，主要从事遥感数据版权保护方面的研究。E-mail: 0218750@stu.lzjtu.edu.cn

**通讯作者**：张黎明(1975-)，男，甘肃天水人，教授，主要从事空间数据指纹和水印方面的研究。E-mail: zlm@lzjtu.edu.cn

陷消费者;同理,不诚实的消费者可以通过辩解盗版的数字拷贝来自内容提供商的恶意分发来抵赖。为了克服对称指纹方案存在的缺陷,非对称指纹方案逐渐被采用。在非对称指纹方案中,数字产品的交易通过各参与者的一个交互协议(指纹协议)来完成。当协议正常执行完成后,消费者得到了其所购买的含有指纹的数字拷贝,而内容提供商得到了对应消费者的一些秘密信息。内容提供商可以根据盗版的数字拷贝中提取的指纹信息以及在交易过程中所得到的有关消费者的秘密信息有效追踪到盗版者,而指纹方案的非对称属性可以防止无辜的消费者受到诬陷。已有的非对称指纹方案实用性不强,主要原因如下:首先,内容提供商必须为每个不同的消费者生成不同的指纹拷贝,指纹拷贝的分发通过单播的方式一对一地发送给相应的消费者。指纹拷贝的唯一性不但加重了内容提供商的负担,也给指纹拷贝的分发提出了严峻的考验,随着消费者数量的增加,内容提供商的负担以及带宽需求也会呈现指数型增长;其次,实现非对称属性的效率较低。Pfitzmann等[4-5]实现非对称属性的核心方法是比特承诺方案,而由于安全原因,其加密率应大于$1/10^3$,即要加密1MB的数据,通信数据量将超过1GB。Kuribayashi等[6]实现非对称属性的核心方法是同态公钥加密,但存在计算复杂度高,加密速度慢以及加密后数据量激增等问题在。张新鹏等[7-8]通过公钥加密随机变量的方法实现了非对称属性,但同时也使用公钥加密多媒体图像。遥感影像相较于普通多媒体图像,数据量大,精度高,光谱特征丰富,若采用公钥加密遥感影像并生成含指纹的影像,计算量巨大;同时含指纹的影像质量会下降。所以目前已有的非对称指纹方案无法直接运用于遥感影像。

设计出安全使用的非对称指纹方案是数字指纹技术走向应用与普及的前提。非对称指纹技术已经成为一个热点研究问题,得到了研究人员的广泛专注。近年来,研究人员提出了许多种非对称指纹方案。Pfitzmann等[4-5]基于比特承诺方案提出一种非对称指纹方案,而由于安全原因,比特承诺方案的加密率应大于$1/10^3$,即要加密1MB的数据,通信数据量将超过1GB,带宽效率随着原始拷贝的增大而快速降低。Kuribayashi等[6]实现非对称属性的核心方法是同态公钥加密,同态公钥加密算法(Homomorphic Public Key Encryption Algorithm)是指具有同态属性的公钥加密算法,其同态属性可以将加密的数字水印或数字指纹直接嵌入到加密的数字产品中而无需提前解密,从而实现交易协议的非对称性,但其存在计算复杂度高,加密速度慢以及加密后数据量激增等问题。张新鹏等[7-8]通过公钥加密随机变量的方法实现了非对称属性,但同时也使用公钥加密多媒体图像,计算复杂度高。Hu等[9]提出了一种带宽高效的非对称指纹方案,通过将同态公钥加密算法用于密钥交换而不是直接加密影像数据来降低计算复杂度,同时采用多播传输[10-11]的方式提高带宽效率。在文献[9]的基础上,结合遥感影像的特点,提出了基于Bresson同态公钥加密算法的遥感影像数字水印方案。

现有的非对称指纹方案适用于多媒体图像,在遥感影像上鲜有应用,同时存在带宽需求高,加密效率低等问题。因此,研究提出一种基于Bresson同态公钥加密算法非对称指纹方案,并将其应用于遥感影像中。

## 2　Bresson同态公钥加密算法

一个公钥加密算法$E(\cdot)$如果对于任意的加密密钥$k$以及其加(乘)法操作满足以下条件,则称该公钥加密算法为加(乘)同态的,其中$x$, $y$为明文空间$M$中的任意两条消息:

$$E_k(x+y)=E_k(x)\oplus E_k(y) \tag{1}$$

加同态与乘同态称之为部分同态。如果一个公钥加密算法既满足加同态性质,又满足乘同态性质,则称其为全同态的。目前已知的公钥密码中,RSA[12]、EIGamel[13]具有乘同态性质,而Paillier[14],Goldwasser-Micali[15]、Okamoto-Uchiyama[16]以及Bresson[17]具有加同态性质,2009年Gentry[18]提出了第一个全同态加密算法。

同态公钥加密算法[19-21]被广泛用于设计非对称指纹方案。同态属性使得内容提供商能够把消费者提供的、加密的指纹信息直接嵌入到加密的数字内容中去而无需预先解密,从而可以实现指纹方案的非对称属性。研究以Bresson公钥密码为例介绍同态公钥加密算法。

设$N=pq$,其实$p$和$q$为素数,同时满足$p=2p_0+1$,$q=2q_0+1$,$p_0$以及$q_0$也为素数,$G$为模$N^2$的二次剩余循环群组。在生成密钥过程中,随机选择$\alpha\in Z^*_{N^2}$和A$\in[1, ord(G)]$,且满足$g=\alpha^2 mod N^2$,$h=g^a mod N^2$,则生成的公钥为$(N, g, h)$,对应的私钥

为A。在加密过程中，对于明文$m\in Z_N$，在$Z_{N^2}$中选择随机数$r$，密文对(A，$B$)可以用以下公式表示：

$$A=g^r \bmod N^2 \tag{2}$$

$$B=h^r(1+mN) \bmod N^2 \tag{3}$$

则解密时可以按以下公式计算明文：

$$m=\frac{\frac{B}{A^a}-1 \bmod N^2}{N} \tag{4}$$

对于明文$m_1$和$m_2$，在进行Bresson加密后，可以得到其密文分别为$E(m_1)=(A_1, B_1)$和$E(m_2)=(A_2, B_2)$，其中：

$$A_1=g^{r_1} \bmod N^2 \tag{5}$$

$$B_1=h^{r_1}(1+m_1N) \bmod N^2 \tag{6}$$

$$A_2=g^{r_2} \bmod N^2 \tag{7}$$

$$B_2=h^{r_2}(1+m_2N) \bmod N^2 \tag{8}$$

若定义⊗为两个向量对应的分量乘积，即：

$$E(m_1)\otimes E(m_2)=(A_1A_2, B_1B_2) \tag{9}$$

而：

$$A_1A_2=g^{r_1+r_2} \bmod N^2 \tag{10}$$

$$B_1B_2=h^{r_1+r_2}[1+(m_1+m_2)N] \bmod N^2 \tag{11}$$

因此可以得到式(12)：

$$E(m_1)\otimes E(m_2)=E(m_1+m_2) \tag{12}$$

由此可见其具有加同态特性。

## 3 非对称指纹方案

### 3.1 基本思想

内容提供商加密原始影像后通过多播传输给多个消费者，使用该遥感影像需要进行解密，在解密密钥的生成过程中使用了Bresson加密的同态属性，生成解密密钥后分发给消费者，指纹拷贝的生成通过客户端的解密完成，不同的解密密钥将产生不同的指纹拷贝。在整个过程中，同态公钥加密算法没有用于加密遥感影像。由于解密密钥构造过程中步骤较多，将具体流程分为遥感影像加密及解密过程与解密密钥的构造过程，如图1所示。

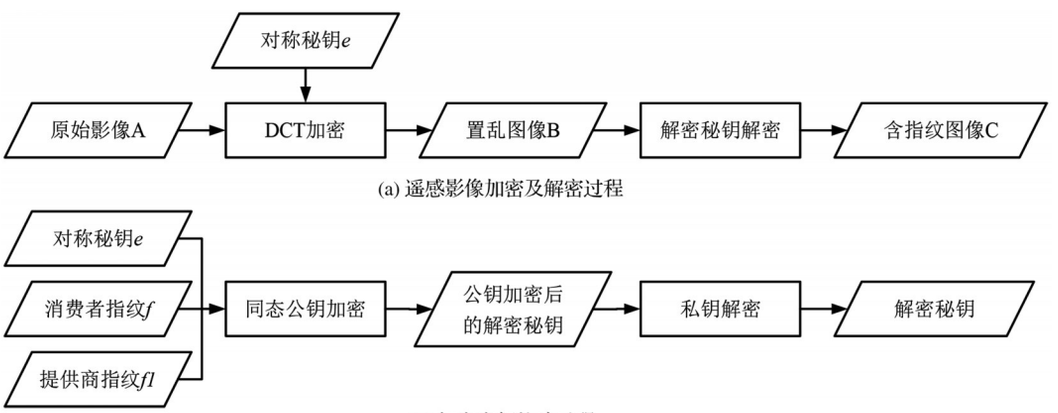


**图1 基于同态公钥加密的数字指纹流程图**

**Fig.1 Flow chart of digital fingerprint based on homomorphic public key encryption**

### 3.2 加密遥感影像

选取大小为512像素×512像素TIFF格式灰度遥感影像为例，采用目前研究最多的离散余弦变换(Discrete Cosine Transform，DCT)[22]对其做8×8分块DCT变换后转化为频率域系数，根据人眼视觉系统(Human Visual System，HVS)，人眼一般对图像的低频部分较为敏感，只需修改低频系数就可以使图像置乱，失真。因此，选取低频系数实现遥感影像的置乱。

设该影像为$P$，将其表示为长度$N$的实数向量$\boldsymbol{P}=(\boldsymbol{p}_1, \boldsymbol{p}_2, \cdots, \boldsymbol{p}_N)$，该向量的每一个元素表示一个DCT系数。内容提供商选择一个相同长度的实数向量$\boldsymbol{E}_k=(\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_N)$作为对称加密密钥。其中的第$j$位元素按如下方式生成：

$$e_i=\alpha\sum_{k=1}^{M}u_k^j(j=1,2,...,N) \tag{13}$$

其中：$\alpha$是一个实数，$\alpha$的值越大，则加密强度越大，该加密过程可以视为水印的扩频嵌入过程。加密完成后得到一份严重置乱的拷贝：

$$\begin{aligned}c&=(c_1,c_2,...,c_N)\\&=(p_1+e_1,p_2+e_2,...,p_N+e_N)\end{aligned} \tag{14}$$

内容提供商将这份拷贝采用多波发送给所有消费者。

### 3.3 解密密钥的生成及分发

解密密钥的分发过程是一个内容提供商$A$与第$i$个消费者$B$的双方协议，为了简单起见，以下省略了相应的签名及验证过程。

(1)为了从$A$处获得解密密钥,$B$首先与$A$协商建立一个双方密钥协议AGR,其中规定了双方的权利与义务,同时其也限定了解密密钥的生成过程:解密密钥由内容提供商与消费者共同生成以便识别消费者并防止内容提供商的恶意诬陷。由于遥感影像存在高精度,光谱特征丰富等特点,为了保持嵌入指纹后遥感影像的较高质量,$A$需要根据HVS为$B$的每个解密密钥元素的取值给定一个适当的区间。

(2)$B$通过同态公钥加密算法生成一个公钥-私钥对$(pk_b, sk_b)$以及他的指纹$f_b$,$f_b$是长度为$N$的实数向量,其中前$N_1$个元素皆为0,以便传输至$A$共同生成解密密钥,后$N_2=N-N_1$为一组实数向量,用于表示$B$的身份。然后$B$用公钥$pk_b$加密$f_b$,将同态运算符记为$\ominus$,并将公钥$pk_b$,密钥协议$AGR$,有关加密函数$E$的信息以及用公钥加密完成的指纹$E_{pk}(f_b)$发送给$A$。

(3)$A$在接受到$B$发送的请求后,生成一组长度为$N$的实数向量$f_i$,其中后$N_2=N-N_1$为空,前$N_1$个元素为一组实数向量,用于表示$A$的身份,然后$A$通过以下方法生成解密密钥$dk_i=(dk_1^i, dk_2^i, \cdots, dk_n^i)$:

$$\begin{aligned} E_{pkb}(dk_i)&=E_{pkb}(ek)\ominus E_{pkb}(fi)\ominus E_{pkb}(fb)\\ &=E_{pkb}(ek\ominus fi\ominus fb)\\ &=E_{pkb}(ek\ominus(fi\ominus fb))\\ &=E_{pkb}(ek\ominus\gamma_i) \end{aligned} \tag{15}$$

此处的$\boldsymbol{\gamma}_i=(\gamma_1^i, \gamma_2^i, \cdots, \gamma_N^i)$为内容提供商$A$以及消费者$B$共同生成的指纹,然后$A$将$E_{pk_b}(dk_i)$发送给$B$。

### 3.4　解密遥感影像

在接收到$A$发送的$E_{pk_b}(dk_i)$后,$B$用自己的私钥$sk_b$对其进行解密,得到解密密钥$dk_i$,然后$B$用解密密钥$dk_i$解密置乱拷贝$C$,解密操作可以表示为:

$$\begin{aligned} y_i^j&=c_i-dk_i^j\\ &=(p_j+e_j)-(e_j-r_i^j)\\ &=p_j+r_i^j \end{aligned} \tag{16}$$

由以上步骤可以看出,当解密操作完成后,一个由$f_b$和$f_i$共同组成的唯一向量$\gamma_i$留在了解密拷贝$Y_i$中,不同的解密密钥中的可能含有相同的$f_b$,但$f_i$彼此不同。指纹$f_i$可以用来识别相应的消费者,指纹$f_b$可以被消费者用来防止内容提供商的诬陷。

## 4　实验与分析

为验证该方案的安全性与加密效率,以MATLAB R2016a为平台,选取原始大小336 KB的512×512 TIFF格式灰度遥感影像进行实验,原始图像如图2(a)所示。

### 4.1　安全性分析

安全性分析主要包括三部分:数字内容本身的安全性,内容提供商的安全性以及消费者的安全性,后两者也可以统称为交易协议的安全性。数字内容本身的安全性是指数字拷贝加密后的置乱程度,其视觉质量应该是不可接受的,以防止未授权的访问与分发。这里首先必须指出的是,交易协议的安全性取决于所使用的密码学原语的安全性,即解密密钥分发协议中所采用的加密算法。

(1)数字内容加密后的置乱程度取决于嵌入到数字媒体中的水印强度,水印强度越大,数字内容加密后的视觉质量越差,可感知性越低。由公式(9)可知,参数$\alpha$用于调节水印强度,$\alpha$值越大,加密后的影像置乱程度就越高,图2(b)~图2(d)给出了不同$\alpha$值下的加密遥感影像。

(2)该方案对于对消费者$B$来说是安全的。首先,在交易过程中,内容提供商$A$不知道最终所获得的指纹拷贝,因此不能够通过直接重分发的指纹拷贝的方式来诬陷$B$。其次,虽然$A$知道相应的指纹$f_i$以及用于加密数字内容的加密密钥$E_k$,但是由于它不知道指纹$f_b$以及$B$的私钥$sk_b$,因此$A$无法够构造出相应的组合指纹$\gamma_i$。在不知道$\gamma_i$的情况下,$A$无法伪造出的$B$指纹拷贝,从而不能够通过伪造出$B$的指纹拷贝来诬陷$B$。

(3)该方案对于对内容提供商$A$来说也是安全的。首先,当$A$在某处找到一份未授权的数字拷贝时,他能通过运行叛逆者追踪算法识别出相应的盗版者。其次,只有消费者$B$知道相应的指纹$f_b$,除$B$之外,任何人都不能够伪造出$B$的指纹拷贝,因此,当$B$被认定是盗版的来源时,$B$无法够推脱由其盗版行为所引起的责任。

### 4.2　带宽效率

在本文的非对称指纹方案中,通信开销由两部分组成:①以多播方式传输一份加密的遥感影像$C$给消费者数目为$M$的多播组;②由密钥分发协议产生的通信开销。以上两部分可以通过与普通单播传输方案的通信开销进行对比的方式来分析所提出的非对称指纹方案的带宽效率。

令$C_m$表示多播传输方案的通信开销,$C_u$表示普通单播传输方案中每个用户的平均通信开销,根据文献[19]中的结论,$C_m$与$C_u$有如下关系:

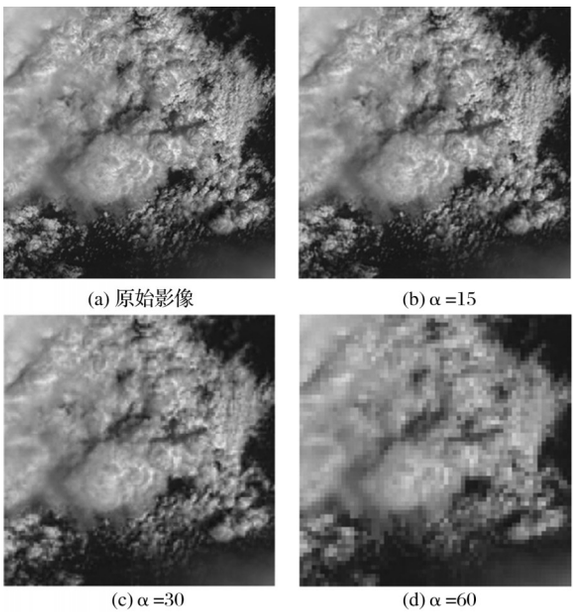


**图 2 原始影像及不同 $\alpha$ 值下影像加密效果**

**Fig.2 Original image and image encryption effect under different $\alpha$ values**

$$\frac{C_m}{C_u} \approx M^{0.66} \tag{17}$$

假设每个解密密钥由 10 240 个元素，每个元素长度为 32 比特（4 字节），则每个消费者获得的解密密钥大小为 40 KB。令 $T_0$ 表示所提出的方案的总通信开销，$T_u$ 表示单播方案的总通信开销，令 $R=T_0/T_u$，由式（14）可以得出：

$$R=\frac{40\times M+ds\times M^{0.66}}{M\times ds} \tag{18}$$

其中：$ds$ 表示加密的数字拷贝 $C$ 的大小。在上式中，对于给定的 $ds$，$R$ 随着 $M$ 的增大而减小。表 1 给出了不同消费者数目时的带宽效率比。

**表 1 消费者数目增长时的带宽效率统计**

**Table 1 Bandwidth efficiency statistics when the number of consumers grows**

| 消费者数目 | 带宽效率 |
|---|---|
| 5 | 0.619 |
| 100 | 0.214 |
| 500 | 0.161 |

由表 1 可以看出，在消费者数量增长时，采用多播这一有效的一对多数据传输方式，可以很大程度上降低通信开销。同时由于采用了基于数字水印的加密方法，加密后的遥感影像大小与原始遥感影像相近，进一步降低了通信开销。

### 4.3 加密效率

由于加密过程是由内容提供商统一完成，解密过程由用户收到解密密钥后独立完成，在消费者较多时，对内容提供商的加密效率分析更有参考价值，故本文模拟了多消费者购买情况下的加密效率。

加密实验模拟采用 OpenSSL 中密码算法库大数操作函数编写了 1024 bit 的 Bresson 算法。实验环境为：Intel core i5-9300H 四核 CPU，DDR4 2666MHZ 16GB 双通道内存。模拟文中 DCT 扩频置乱算法与 1 024 bit Bresson 算法加密原始大小 336 KB 的 512×512 遥感影像，实验次数设置为 100 次，表 2 给出了二者计算耗时的统计。

**表 2 加密算法计算耗时统计**

**Table 2 Encryption algorithm calculation time-consuming statistics**

| 算法 | 计算耗时/s |
|---|---|
| DCT 扩频置乱算法 | 2.17 |
| Bresson 加密算法 | 45.23 |

由上表可以看出，使用同态公钥加密算法直接加密影像数据的耗时要远远长于基于数字水印算法的扩频置乱算法。而目前的遥感影像数据量正在迅速增长，随着原始影像数据大小的增长，使用同态公钥加密算法直接加密影像数据的计算耗时也会以几何倍数增长，这是十分低效的。

## 5 结 语

针对遥感影像提出了一种基于同态公钥加密算法的数字指纹方案。与已有相关方案相比，所提出的方案有着较低的计算复杂性、较小的带宽需求以及较强的实用性。首先，在提出的方案中，同态公钥加密算法只用于分发解密密钥，而不是用于加密遥感影像数据。因此，降低了计算复杂性，提高了加密效率。其次，多播通信被用于传输一份相同的加密拷贝给多个消费者，够降低了通信开销，提高了带宽效率。再次，由于加密遥感影像时采用了基于数字水印的 DCT 加密方法，加密后的遥感影像与原始影像大小相近，不会出现同态公钥加密算法加密遥感影像后加密后数据量激增的问题，可以进一步降低通信开销。另外，内容提供商只需要为多个消费者生成一份相同的加密拷贝，这极大地降低了内容提供商的负担。

在设计数字指纹方案时，多个用户之间的合谋攻击问题有所疏漏。当然，这个问题将会涉及到数字指纹的抗合谋编码设计，即根据合谋攻击的过程

对数字指纹进行编码,防止被多个用户合谋攻击。这将在未来对其进行研究,并证实可用性。

**参考文献(References):**


[1] Ding Kaimeng, Zhu Changqing, Luo Wen, *et al*. Perceptual hash algorithm based on adaptive PCNN and PCA for remote sensing image authentication[J]. Journal of Nanjing Normal University(Natural Science Edition),2019,42(2):17-22.[丁凯孟,朱长青,罗文,等.基于自适应PCNN与PCA的遥感影像感知哈希认证算法[J].南京师大学报(自然科学版),2019,42(2):17-22.]

[2] Zhu Changqing, Fu Haojun, Yang Chengsong, *et al*. Watermarking algorithm for digital grid map based on integer wavelet transformation[J]. Geomatics and Information Science of Wuhan University,2009,34(5):619-621.[朱长青,符浩军,杨成松,等.基于整数小波变换的栅格数字地图数字水印算法[J].武汉大学学报(信息科学版),2009,34(5):619-621.]

[3] Pfitzmann B, Waidner M. Anonymous Fingerprinting, Berlin, Heidelberg,1997[C]//Springer Berlin Heidelberg,1997.

[4] Pfitzmann B, Schunter M. Asymmetric Fingerprinting, Berlin, Heidelberg,1996[C]// Springer Berlin Heidelberg,1996.

[5] Biehl I, Meyer B. Cryptographic methods for collusion-secure fingerprinting of digital data[J]. Computers & Electrical Engineering, 2002,28(1):59-75.

[6] Kuribayashi M, Tanaka H. Fingerprinting protocol for images based on additive homomorphic property[J]. IEEE Transactions on Image Processing, 2005,14(12):2129-2139

[7] Zhang Xinpeng, Wang Shuozhong, Chen Chao. Asymmetric fingerprint scheme without authoritative third party[C]// The Sixth National Symposium on information hiding and multimedia information security, Harbin.[张新鹏, 王朔中, 陈超. 不需权威第三方的非对称指纹方案[C]// 第六届全国信息隐藏暨多媒体信息安全学术研讨会, 哈尔滨.]

[8] Xie Jianquan, Huang Dazu, Xie Qing. Asymmetric fingerprinting protocol based on RSA public key system[J]. Journal of Chinese Computer Systems, 2013,34(11):2542-2545.[谢建全,黄大足,谢勍.基于RSA公钥体制的非对称数字指纹协议[J].小型微型计算机系统,2013,34(11):2542-2545.]

[9] Hu D, Li Q. Bandwidth efficient asymmetric fingerprinting scheme[J]. International Journal of Communication Systems, 2012,25(2):84-91.

[10] Paul S. Multicasting on the internet and its applications[M]. Unised states: Springer science & Business media,1998.

[11] Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169-180.

[12] T. E. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985,31(4):469-472.

[13] Paillier P. Public-key cryptosystems based on composite degree residuosity classes, 1999[C]// International conference on the theory and applications of cryptographic techniques. Berlin, Heidelberg: Springer, 1999.

[14] Goldwasser S, Micali S. Probabilistic encryption & how to play mental poker keeping secret all partial information[M]. Providing sound foundations for cryptography: on the work of Shafi Goldwasser and Silvio Micali. United States: ACM Books, 2019.

[15] Okamoto T, Uchiyama S. A new public-key cryptosystem as secure as factoring, 1998[C]// International conference on the theory and applications of cryptographic techniques. Berlin, Heidelberg: Springer, 1998.

[16] Bresson E, Catalano D, Pointcheval D. A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications, 2003[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Heidelberg: Springer, 2003.

[17] Gentry C. Fully homomorphic encryption using ideal lattices[C]//Proceedings of the forty-first annual ACM symposium on Theory of computing. United States: Association for Computing Machinery, 2009.

[18] Qin Sixian, Yu Yongsheng, Zhang Xiaohui, *et al*. Comparison and analysis of invisible digital watermark algorithms for remote sensing[J]. Journal of Geomatics, 2017, 42(5): 59-62.[秦思娴, 余咏胜, 张小惠, 等. 遥感影像不可见数字水印算法比较与分析[J]. 测绘地理信息,2017,42(5):59-62.]

[19] Diao Yiqing, Ye Ayong, Zhang Jiaomei, *et al*. A dual privacy protection method based on group signature and homomorphic encryption for alliance blockchain[J]. Journal of Computer Research and Development, 2022, 59(1): 172-181.[刁一晴,叶阿勇,张娇美,等.基于群签名和同态加密的联盟链双重隐私保护方法[J].计算机研究与发展, 2022, 59(1): 172-181.]

[20] Tu Hang. Secure multi-party computation protocol based on fully homomorphic encryption[J]. Communications Technology, 2021, 54(12): 2674-2678.[涂航. 基于全同态加密的安全多方计算协议[J]. 通信技术, 2021, 54(12): 2674-2678.]

[21] Zhong Yang, Bi Renwan, Yan Xishan, *et al*. Efficient homomorphic neural network supporting privacy-preserving training [J/OL]. Journal of Computer Applications: 1-11 [2022-03-12].[钟洋, 毕仁万, 颜西山, 等. 支持隐私保护训练的高效同态神经网络[J/OL]. 计算机应用: 1-11 [2022-03-12].

http://kns.cnki.net/kcms/detail/51.1307.TP.20220302.1536.004.html]

[22] Chalmers R C, Almeroth K C. Modeling the branching characteristics and efficiency gains in global multicast trees:[C]// Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society. United States: IEEE, 2001.

# A Digital Fingerprinting Scheme for Remote Sensing Images based on the Homomorphic Public Key Encryption Algorithm

Wang Xiucheng[1,2,3], Zhang Liming[1,2,3]

(1.*Faculty of Geomatics, Lanzhou Jiaotong University, Lanzhou* 730070, *China*;
2.*National -Local Joint Engineering Research Center of Technologies and Applications for National Geographic State Monitoring, Lanzhou* 730070, *China*;
3.*Gansu Provincial Engineering Laboratory for National Geographic State Monitoring, Lanzhou* 730070, *China*)

**Abstract**: An asymmetric fingerprinting scheme for remote sensing images based on the homomorphic public key encryption algorithm is proposed for solving the problems of high computational complexity and low bandwidth efficiency in asymmetric digital fingerprinting. In this scheme, the data provider encrypts the remote sensing images via the DCT spread spectrum scrambling method, and the Bresson homomorphic public key encryption algorithm is used to realize asymmetric distribution of the decryption key. The copies of remote sensing images with the fingerprint are decrypted by the client, and different copies with the fingerprint come from different decryption keys. The remote sensing images are not directly encrypted by the public key encryption algorithm, so the complexity of the algorithm is greatly reduced and the encryption efficiency is dramatically improved. Meanwhile, the demand of bandwidth will be reduced and the efficiency of bandwidth will be improved, because data owners not only need to generate one copy with the fingerprint for different users, but also data copies are distributed to different users via multicast transmission. The experiments have shown that the scheme can effectively improve the efficiency of bandwidth and the efficiency of encryption when the number of users is relatively large, which can greatly reduce the computing load of the data server and reduce the waiting time of the users.

**Key words**: Asymmetric fingerprint; Homomorphic public key encryption; Remote sensing images; Multicast transmission; The efficiency of bandwidth