计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2021,30(5):234−240 [doi: 10.15888/j.cnki.csa.007936]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于 ElGamal 的同态交换加密水印算法①

方立娇, 李子臣, 丁海洋

(北京印刷学院 信息工程学院, 北京 102600)
通讯作者: 方立娇, E-mail: jao_flj@163.com

摘　要: 针对多媒体信息安全与版权保护的需求, 本文将 ElGamal 公钥密码体制与 Patchwork 数字水印算法相结合, 提出一种新的同态密文域交换加密水印算法. 算法利用 ElGamal 乘法同态的特性, 将明文域嵌入水印的运算映射到密文域中, 实现了加密与嵌入水印操作的交换, 在水印提取时, 既可以在密文域提取水印, 也可以解密后提取出水印. 实验结果表明, 该算法嵌入水印和数据加密的顺序不影响含水印信息密文数据的产生和在密文和明文中水印信息的提取, 保证了水印嵌入操作的机密性和多媒体数据在分发管理过程中的安全性, 同时, 水印算法的综合性能也得到了改善.

关键词: ElGamal 密码算法; 同态加密; 数字水印; 信息安全; 交换加密水印算法

引用格式: 方立娇,李子臣,丁海洋.基于 ElGamal 的同态交换加密水印算法.计算机系统应用,2021,30(5):234–240. http://www.c-s-a.org.cn/1003-3254/7936.html

Homomorphic Commutative Watermarking Encryption Algorithm Based on ElGamal

FANG Li-Jiao, LI Zi-Chen, DING Hai-Yang

(School Information and Engineering, Beijing Institute of Graphic Communication, Beijing 102600, China)

Abstract: Aiming at the needs of multimedia information security and copyright protection, this study combines the ElGamal public key crypto system with Patchwork digital watermarking algorithms to propose a new homomorphic ciphertext domain-commutative watermarking encryption algorithm. The algorithm maps the operation of embedding the watermark in the plaintext domain to the ciphertext domain based on the multiplicative homomorphism of ElGamal, swapping the operations of encryption and embedding watermark. The watermark can be extracted in the ciphertext domain or in the plaintext domain. The experimental results show that the order of embedding watermarks and encrypting data does not affect the generation of ciphertext data containing watermarks and the extraction of watermarks from ciphertext and plaintext, which ensures the confidentiality of embedding watermarks and the security of multimedia data in distribution management. Also, the comprehensive performance of watermarking algorithms is improved.

Key words: ElGamal cryptographic algorithm; homomorphic encryption; digital watermarking; information security; commutative watermarking encryption algorithm

随着互联网技术、云计算技术的进一步发展和普及, 用户可以将海量的数据上传到云来进行存储, 需要时也很方便再下载下来使用[1]. 但是, 云技术在给人们带来便捷的同时, 人们也不得不考虑数据在传输和存

① 基金项目: 北京市教委科研计划一般项目 (KM201610015002, KM201510015009); 北京市教委科研计划重点项目 (KZ201510015015, KZ201710015010); 国家自然科学基金 (61370188)
Foundation item: General Project of Science and Technology Plan of Beijing Municipal Education Commission (KM201610015002, KM201510015009); Key Project of Science and Technology Plan of Beijing Municipal Education Commission (KZ201510015015, KZ201710015010); National Natural Science Foundation of China (61370188)
收稿时间: 2020-09-22; 修改时间: 2020-10-21, 2020-10-27, 2020-11-04; 采用时间: 2020-11-09; csa 在线出版时间: 2021-04-28

储过程中遇到的安全问题[2]. 为了避免未经授权的非法修改和非法使用, 以及恶意攻击等, 需要对多媒体数据进行加密保护或者嵌入水印. 此外, 在一些特殊领域, 如网上匿名投票, 医疗军事等, 人们希望不泄露原始数据就能够进行数据认证. 此时, 不仅需要传输和访问过程中的安全保护, 还需要考虑使用过程中的安全保护. 所以需要将加密技术与水印技术结合起来对多媒体数据进行保护[3].

近年来, 人们发现同态密码算法所特有的同态特性, 使得加密前后的明文数据与密文数据之间具有一定的代数关系[4–6], 这种特性为加密与水印的结合提供了一种有效的方法. 在文献 [7] 中 Chen 等提出基于公钥加密域的数字水印算法, 该算法利用 Paillier 同态公钥加密系统[4] 对载体图像进行加密, 数据隐藏者将秘密消息嵌入其中, 以生成加密图像, 并将嵌入的秘密消息发送给接收者, 最后, 接收者可以不解密就提取信息并恢复原始图像. 文献 [8–10] 基于时域水印算法, 将水印与同态加密算法结合, 提出将明文水印映射到密文域, 可以直接修改载体的原始信号值来嵌入水印. 其中文献 [8] 中, Zhang 等针对公钥密码体制加密的密文图像, 提出了一种具有概率和同态特性的无损、可逆和组合数据隐藏方案, 将密文像素替换为新值, 通过多层湿纸编码将附加数据嵌入到密文像素的多个 LSB 平面中. 实现了数据嵌入操作不会影响原始明文图像的解密, 可以在解密前提取一部分嵌入数据, 解密后提取另一部分嵌入数据并恢复原始明文图像. 并且对图像进行预处理, 预防了像素溢出的问题. 文献 [9] 中, 提出了一种新的加密图像的可逆数据隐藏方案. 该方法无需对原始图像进行任何预处理, 即可将附加数据直接嵌入到加密图像中. 但是必须解密后才能恢复原始图像和提取水印信息. 在文献 [10] 中 Xiang 利用 Paillier 密码体制的同态和概率特性, 提出了一种新的加密图像的可逆数据隐藏方案, 嵌入的数据可以直接从加密域中提取出来, 方案具有更低的计算复杂度、更高的安全性能和更好的嵌入性能. 文献 [11] 提出了一种同态加密域的离散小波变换 (DWT) 和多分辨率分析 (MRA) 的方法, 利用模乘法逆元的方法解决了量化带来的数据扩展问题. 尽管如此, 仍可改善加密域中水印方案的性能. 文献 [12] 结合离散小波变换和离散余弦变换 (DCT) 的方法提高了加密域水印方案的鲁棒性能. 水印提取可以在明文域和加密域上执行. 文献 [13] 中提出了一种同态加密域图像可逆水印算法, 大大降低了数据扩展, 提高了嵌入容量. 人们虽然提出了许多加密技术与水印技术相结合的水印算法, 但是仍存在一些关键问题需要研究. 比如, 先对多媒体数据进行加密然后再在多媒体密文中嵌入水印, 则可能导致密文无法解密. 另一方面, 先嵌入水印, 然后再加密, 那么不能直接在密文域提取出水印信息, 只有在解密后才能提取水印信息. 这样使得水印提取的解密步骤冗余, 更会使明文数据暴露于检测环境中, 大大降低了多媒体数据分发过程中的安全性.

利用交换加密水印 (Commutative Encryption Watermarking, CEW) 方案, 可以实现在明文或密文域嵌入水印, 提取水印时, 不仅在密文域能提取出数字水印, 而且在解密后的明文域也可以提取水印, 实现加密和水印嵌入顺序的交换. 人们通常选择基于独立操作数的 CEW[14], 文献 [15] 中的方案基于树形结构的 Haar 变换, 在变换系数的子集中执行水印嵌入, 并对其余部分进行加密. 但是部分加密的 CWE 方案面临暴露明文媒体数据的风险. 文献 [16] 借助 Paillier 密码算法的同态特性, 实现相同操作数的加密和水印相结合, 在不解密的情况下也能提取出水印, 提高了多媒体信息的安全性, 但是该方案忽略了像素溢出的问题. 随后, 文献 [17] 提出了一种基于模运算 CEW 方案, 但是该方案的加密算法并不安全. 目前人们提出了许多加密域水印方案和 CEW 方案, 但是对同态加密域的 CEW 技术的研究还很少还不成熟, 仍有许多可以改进的地方.

基于上述问题, 本文利用 ElGamal 密码算法的乘法同态特性, 同时, 结合 Patchwork 水印算法[18], 提出一种更方便的基于同态操作的 CEW 方案, 将明文水印算法通过同态映射到密文域, 实现密文水印的嵌入以及明文水印在密文域中嵌入. 解决了加密和数字水印相互影响的问题, 保证了数据加密、水印嵌入操作不受先后顺序的限制, 实现数据在密文状态下的直接检测水印以及解密后水印仍可提取的功能, 以确保算法具有更高的安全性.

1 理论基础

本节将介绍 CEW[16], ElGamal 密码体制[5] 的同态特性、Patchwork 水印算法[18], 以及本文提出的基于 ElGamal 同态交换加密水印算法的基本原理.

1.1 交换加密水印

CEW 是实现加密与水印结合的有效途径. 利用

CEW 方案, 可以实现加密和水印操作顺序的交换. 下图 1 是交换加密水印算法的流程图.

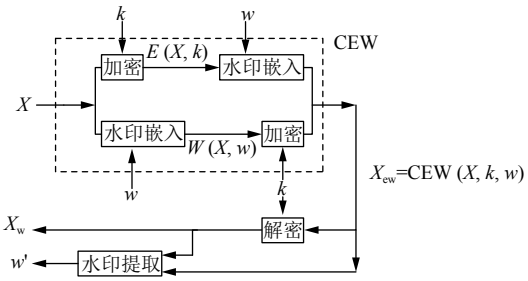


图 1 交换加密水印算法流程图

图 1 中, E 为加密函数, W 是数字水印函数, CEW 是交换加密水印算法, k 是加密密钥, X 是明文多媒体载体, w 是嵌入的数字水印, X_{ew} 是经过交换加密水印运算后的多媒体信息, X_w 是解密后含水印明文多媒体载体, w'是提取的数字水印.

目前, 为了避免加密与水印之间相互干扰, 大多数 CEW 算法都是通过操作的独立性来完成. 这意味着水印的操作数对用户是透明的, 因为没有加密, 降低了多媒体信息数据的安全性. 为此, 人们将正交分解引入到基于独立操作的 CEW (CEWod)[19] 中, 以提高多媒体信息的安全性. 然而, CEWod 也是一种基于独立操作的 CEW, 并不是解决 CEW 安全问题的根本出路. 本文利用同态加密来削弱对特定加密算法和水印算法的限制, 并提高水印方案的安全性.

1.2 ElGamal 同态加密算法

ElGamal 算法[5], 是国际公认的公钥密码体制, 算法的安全性依赖于计算有限域上离散对数这一难题. ElGamal 密码算法由参数产生、密钥生成、加密和解密 4 部分组成.

参数产生: 设 G 为有限域 Z_p 的乘法群, p 是一个素数, g 是 Z_p 上的一个生成元, 且$g \in Z_P^*$.

密钥生成: 选取 $x \in [1, p-1]$, 计算$y = g^x (\bmod p)$, 那么 x 为私钥, y 为公钥.

加密过程: 对消息 m, 可以任意的选取随机数 $r \in [1, p-1]$, 利用公钥 y 和系统参数计算$c_1 = g^r (\bmod p)$和$c_2 = mg^r (\bmod p)$, 可以得到密文为$E(m) = (c_1, c_2)$, 其中, $E(\cdot)$表示加密算法.

解密过程: 接收者接收到密文消息$c = (c_1, c_2)$后, 利用私钥 x, 计算$m = D(E(m)) = c_2 (c_1{}^x)^{-1} \mod p$, 其中, $D(\cdot)$表示解密算法.

对两个明文m_1、m_2, 对其分别进行加密, 得到$E(m_1) = (g^{r_1} \mod p, m_1 y_1^{r_1} \mod p)$, $E(m_2) = (g^{r_2} \mod p, m_2 y_1^{r_2} \mod p)$, 则$E(m_1)E(m_2) = (g^{r_1+r_2} \mod p, m_1 m_2 y_1^{r_1+r_2} \mod p)$ $D(E(m_1)E(m_2)) = m_1 m_2 y_1^{r_1+r_2} [(g^{r_1+r_2})^x]^{-1} (\bmod p) = m_1 m_2$.

因此, ElGamal 密码体制具有乘法同态特性[5].

1.3 Patchwork 水印算法

Patchwork 算法是根据数据统计特性而设计的一种数字水印算法. 在水印信息嵌入之前, 先从原始载体数据中选择一些数据, 然后将这些数据按照一定的关系组成两个集合, 通过修改这两个集合的关系来嵌入水印, 两个集合间的关系可以是大小/能量/奇偶性关系, 提取水印时根据对应关系提取水印信息. 一般 Patchwork 水印算法[18] 的步骤可以描述如下:

(1) 数据集合选取: 从载体数据中选择两组数据, 将这些数据按照一定关系组成两个集合$A = \{a_{i,j}\}$, $B = \{b_{i,j}\}$, $i \in [1, n]$, $j \in [1, n]$, 其中 A, B 的图像的像素值相近.

(2) 水印嵌入: 将集合 A 中所有的像素点增加 d, 将集合 B 中所有的像素点减少 d.

(3) 水印提取: 通过计算均值 s 提取水印信息: $s = Ext\left(a_{i.i}^w\right) - Ext\left(b_{i.i}^w\right)$[18].

即:

$$s = \frac{1}{N^2} \sum_{i=1}^{N} \sum_{j=1}^{N} \left(a_{i,j}^w - b_{i,j}^w\right) \tag{1}$$

其中, $Ext(x_{i,j}) = \frac{1}{N^2} \sum_{i=1}^{N} \sum_{j=1}^{N} x_{i,j}$, $a_{i,j}^w = a_{i,j} + d$, $b_{i,j}^w = b_{i,j} - d$.

以 d=1 为例, 假设原始载体中随机选取 $2N^2$ 个数据对 $(a_{i,j}, b_{i,j})$, 则嵌入水印算法如下:

$$\begin{cases} a_{i,j}^w = a_{i,j} + 1 \\ b_{i,j}^w = b_{i,j} - 1 \end{cases} \tag{2}$$

利用 $a_{i,j}$+1, $b_{i,j}$−1 可以保持载波数据的平均值, 所以水印提取算法为:

$$s = \frac{1}{N^2} \sum_{i}^{N} \sum_{j}^{N} \left(a_{i,j}^w - b_{i,j}^w\right) \tag{3}$$

其中, 当 $s \approx 2$, 表示带水印载波, 水印信息为 1; 若 $s \approx 0$, 表示无水印载波嵌入水印, 水印信息为 0.

2 基于 ElGamal 和 Patchwork 交换加密水印算法

通过将 ElGamal 同态加密算法与 Patchwork 水印

算法相结合, 在嵌入水印时, 可以在明文嵌入水印, 或者在加密后密文嵌入水印. 在水印提取时, 既可以密文域提取水印, 也可以在解密后的明文中提取水印. 实现了加密算法和水印算法先后顺序的交换.

算法总体结构如图 2 所示.

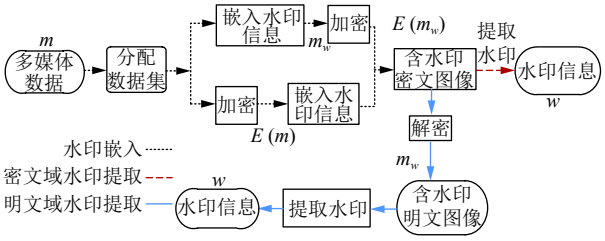


图 2 算法总体结构图

在设计算法的时候, 我们可以由 ElGamal 对消息 m 加密, 计算得到密文为$c_1 = g^r (\bmod p), c_2 = my^r (\bmod p)$. 将 m 的密文记为$E(m) = \bmod [(c_1, c_2), p]$.

$D\{\bmod [(c_1, c_2), p]\} = c_2 / c_1^x (\bmod p)$, 其中 y 是加密时的公钥, x 是解密时的私钥.

2.1 交换加密水印算法基本原理

基于 ElGamal 加密算法与 Patchwork 水印算法的 CEW 算法包括如下步骤:

(1) 数据集合选取: 在载体图像中选择一些数据, 根据像素值下标之和的奇偶性将数据重新组成两个集合$A = \{a_{i,j}\}, B = \{b_{i,j}\}$, $i \in [1, N]$, $j \in [1, N]$, 其中 A, B 集合中的像数值用$a_{i,j}$和$b_{i,j}$代表, 并且在实际图像的像素点下标之和分别为偶数和奇数.

(2) 水印嵌入: 将集合 A 中所有的像素点改变λ倍, 将集合 B 中所有的像素点改变λ^{-1}倍. 此处的λ接近 1. λ值的大小由均衡水印提取率与嵌入水印后图像质量的得到.

(3) 水印提取:

$$s = \frac{1}{N^2} \sum_i^N \sum_j^N \frac{a_{i,j}^w}{b_{i,j}^w} \approx \lambda^2 \tag{4}$$

其中, s 的值将决定是否带有载波水印, 若$s \approx \lambda^2$, 含有带水印载波, 水印信息为 1; 若$s \approx 1$, 表示无水印载波, 水印信息为 0.

2.2 含水印密文载体的生成

首先在原始载体数据中选择一些数据, 然后计算这些像素值下标的值, 再按照下标值的奇偶性分配组成两个集合$\{a_{i,j}\}, \{b_{i,j}\}, i \in [1, N], j \in [1, N]$.

2.2.1 先嵌入水印后加密

在明文中嵌入水印:

$$\begin{cases} a_{i,j}^w = a_{i,j}\lambda (\bmod p) \\ b_{i,j}^w = b_{i,j}\lambda^{-1} \bmod p \end{cases} \tag{5}$$

其中, $a_{i,j}^w$, $b_{i,j}^w$是带水印的明文.

然后对含水印的明文进行加密:

$$\begin{cases} \hat{a}_{i,j}^{ew} = \bmod [(c_{\hat{a}1}, c_{\hat{a}2}), p] \\ \hat{b}_{i,j}^{ew} = \bmod [(c_{\hat{b}1}, c_{\hat{b}2}), p] \end{cases} \tag{6}$$

其中, $c_{\hat{a}1} = g^{r_a} (\bmod p)$, $c_{\hat{a}2} = a_{i,j}^w y^{r_a} (\bmod p)$, $c_{\hat{b}_1} = g^{r_b} (\bmod p)$, $c_{\hat{b}_2} = b_{i,j}^w y^{r_b} (\bmod p)$, r_a、r_b为在 $(1, 1-p)$ 中的随机数.

为了将来能在密文中提取水印, 选取适当随机参数(r_a, r_b)满足:

当水印信息为 1 时, 使得$(c_{\hat{a}_2} \geq c_{\hat{b}_2} (\bmod p))$; 当水印信息为 0 时, 使得$(c_{\hat{a}_2} < c_{\hat{b}_2} (\bmod p))$.

由于, ElGamal 加密算法是一种概率公钥密码体制, 选取适当的随机参数, 满足上述不等式是可行的.

2.2.2 先加密后嵌入水印

对每个像素值加密, 加密算法$c_{a_1} = g^{r_a} (\bmod p), c_{a_2} = a_{i,j} g^{r_a} (\bmod p), c_{b_1} = g^{r_b} (\bmod p)$, $c_{b_2} = b_{i,j} g^{r_b} (\bmod p)$, 其中$r_a r_b$ 为在区间 $(1, p-1)$ 中的随机参数.

同理, 将λ加密之后的密文记为$(c_{\lambda 1}, c_{\lambda 2})$, 将$\lambda^{-1}$加密之后的密文记为$(c_{\lambda^{-1}1}, c_{\lambda^{-1}2})$.

在密文中嵌入水印:

$$\begin{cases} \bar{a}_{i,j}^{ew} = \bmod [(c_{\lambda 1} c_{a1}, c_{\lambda 2} c_{a2}), p] \\ \bar{b}_{i,j}^{ew} = \bmod [(c_{\lambda^{-1}1} c_{b1}, c_{\lambda^{-1}2} c_{b2}), p] \end{cases} \tag{7}$$

其中, $\bar{a}_{i,j}^{ew}$, $\bar{b}_{i,j}^{ew}$是密文水印载体.

为了能在密文中提取水印, 选取适当随机参数$(r_a, r_b, r_\lambda, r_{\lambda^{-1}})$满足:

当水印信息为 1 时, 使得$(c_{\lambda 2} c_{a2} \geq c_{\lambda^{-1}2} c_{b2} (\bmod p))$; 当水印信息为 0 时, 使得$(c_{\lambda 2} c_{a2} < c_{\lambda^{-1}2} c_{b2} (\bmod p))$.

2.3 水印信息的提取

2.3.1 在解密后的明文提取水印

首先引入如下的结论.

定理. 对利用上述先嵌入水印后加密与先加密后嵌入水印所得到的含水印的密文进行解密结果是相同的, 即:

$$D\left(\hat{a}_{i,j}^{ew}\right) = D\left(\bar{a}_{i,j}^{ew}\right) = \lambda a_{i,j} \tag{8}$$

$$D\left(\hat{b}_{i,j}^{ew}\right)=D\left(\bar{b}_{i,j}^{ew}\right)=\lambda b_{i,j} \tag{9}$$

其次证明:

$$\begin{aligned}D\left(\hat{a}_{i,j}^{ew}\right)&=D\{\mathrm{mod}[(c_{\hat{a}1},c_{\hat{a}2}),p]\}\\&=\frac{c_{\hat{a}2}}{(c_{\hat{a}1})^{x}}\ \mathrm{mod}\ p=\frac{a_{i,j}^{w}y^{r_a}}{g^{xr_a}}\ \mathrm{mod}\ p\\&=a_{i,j}^{w}\ \mathrm{mod}\ p=\lambda a_{i,j}\end{aligned} \tag{10}$$

$$\begin{aligned}D\left(\bar{a}_{i,j}^{ew}\right)&=D\{\mathrm{mod}[(c_{\lambda1}c_{a1},c_{\lambda2}c_{a2}),p]\}\\&=\frac{c_{\lambda2}c_{a2}}{(c_{\lambda1}c_{a1})^{x}}\ \mathrm{mod}\ p=\frac{\lambda y^{r_\lambda}a_{i,j}y^{r_a}}{g^{xr_\lambda}g^{xr_a}}\ \mathrm{mod}\ p=\lambda a_{i,j}\end{aligned} \tag{11}$$

因此, $D\left(\hat{a}_{i,j}^{ew}\right)=D\left(\bar{a}_{i,j}^{ew}\right)=\lambda a_{i,j}$. 同理可以证明 $D\left(\hat{b}_{i,j}^{ew}\right)=D\left(\bar{b}_{i,j}^{ew}\right)=\lambda b_{i,j}$.

提取水印步骤如下:

然后计算:

$$\begin{aligned}s&=\frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\left[D\left(\bar{a}_{i,j}^{ew},x\right)/D\left(\bar{b}_{i,j}^{ew},x\right)\right]\\&=\frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\left[D\left(\hat{a}_{i,j}^{ew},x\right)/D\left(\hat{b}_{i,j}^{ew},x\right)\right]\end{aligned} \tag{12}$$

最后, 根据 s 的值, 提取水印信息. 若 $s\approx\lambda^2$, 表示有载波水印, 水印信息为 1; 若 $s\approx1$, 表示不含有载波水印, 实际水印信息为 0.

2.3.2 在密文中提取水印

在密文中提取水印的步骤如下:

首先计算:

$$s=\frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\delta\left(\hat{a}_{i,j}^{ew},\hat{b}_{i,j}^{ew}\right) \tag{13}$$

其中, $\delta\left(\vec{a},\vec{b}\right)$为布尔函数, $\delta\left(\vec{a},\vec{b}\right)=\begin{cases}1,a_2\geq b_2\\0,a_2<b_2\end{cases}$, $\vec{a}=(a_1,a_2)$, $\vec{b}=(b_1,b_2)$为二维向量.

然后, 根据 s 的值提取水印信息. 若 s=1, 表示含有载波水印, 水印信息为 1. 若 s=0, 表示未含载波水印, 水印信息为 0.

最后, 通过计算 $s=\frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\delta\left(\bar{a}_{i,j}^{ew},\bar{b}_{i,j}^{ew}\right)$, 也可以提取水印信息.

3 实验分析

3.1 实验设置

在实验时, 为了验证算法的可行性, 实验首选标准 Lena(256×256) 灰度图像来做示例, ElGamal 加密算法中选取大素数 p=257, g=3, 私钥 x=2, 公钥 $y=g^x \bmod p$. 为简单起见, 加密时选取的随机数 r=5.

实验使用水印算法的客观评价标准, 如峰值信噪比 (PSNR)、误码率 (BER) 和嵌入率 (BR) 来测试和衡量设计的水印算法的性能指标. 其中, 峰值信噪比 (PSNR) 的值用来衡量嵌入水印后的图像与原始图像之间的差异, PSNR 值越大, 差异越小, 效果越好. 误码率 BER∈[0, 1], BER 的值越接近 0 说明提取水印准确率越高. 对于相同大小的载体, 当嵌入率 (BR) 越高时, 相应的嵌入容量也越大. 假设原始图像用 $\boldsymbol{I}$ 表示, 解密后含水印的图像记为 $\boldsymbol{I}'$, 使用 (i, j) 表示图像的像素坐标, 其中 h 代表图像的高度, w 表示图像的宽度, M 为嵌入的水印总比特数.

峰值信噪比 (*PSNR*) 的计算公式为:

$$PSNR=10\times\lg\frac{h\times w\times255^2}{\sum_{i=1}^{h}\sum_{j=1}^{w}[I(i,j)-I'(i,j)]^2} \tag{14}$$

误码率 (*BER*) 的计算公式为:

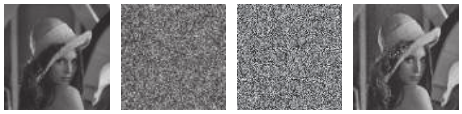
$$BER=\frac{1}{M}\sum_{i=1}^{M-1}X_i,\ X_i=\begin{cases}1,\ I(i,j)=I'(i,j)\\0,\ I(i,j)\neq I'(i,j)\end{cases} \tag{15}$$

另外, 在数字水印图像处理技术领域中, 一般原始载体图像的像素值为 [0, 255], 由于加密域水印算法中的加密操作, 很可能会出现像素值为负数或者像素值超过 255 的现象, 为了减少或者避免像素溢出的问题, 人们会在嵌入水印信息之前对待处理图像进行预处理[20]. 在本算法中, 由于 ElGamal 算法加密操作, 会出现像素值溢出的情况, 为了减少溢出, 在仿真实验过程中, 选取素数 p=257, 这样使得在对像素值进行模运算的时候, 尽可能地使得运算结果的范围为 0~255, 有极小的可能性像素值会上溢. 在实际实验时, 我们可以对所有像素点进行扫描和标记, 在加密后和嵌入水印之前, 预先将大于 255 的像素值修改为 255, 并对修改位进行标识. 然后在解密和提取水印的过程中, 根据标识位将像素值修改为原像素值. 有时候图像预处理比较繁琐, 但是进行图像预处理, 能够保证算法准确无误的进行.

3.2 实验结果分析

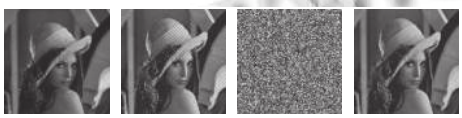
图 3(a) 是原始载体图像, 图 3(b) 是利用 ElGamal 加密系统加密后得到的密文图像, 图 3(c) 是嵌入水印

后的密文水印图像, 以及图 3(d) 是解密后的含水印图像, 计算得到的 *PSNR* 值为 24.71 dB, *BER* 值为 0.0039. 图 4 分别是原始图像, 嵌入水印信息之后的含水印图像和密文含水印图像, 以及解密后的含水印图像, 图 4(b) 的 *PSNR* 值为 51.36 dB, 解密后的含水印图像, *PSNR* 值为 50.38 dB, *BER* 值均为 0, 说明能准确提取水印. 由实验结果可知, 利用本算法无论是在明文域还是在密文域, 都能成功提取水印信息, 并解密得到原始图像, 且解密得到的水印图像质量较高.



(a) 原图 (b) 加密 (c) 加水印 (d) 提取

图 3 加密域下的实验结果图



(a) 原图 (b) 加水印 (c) 加密 (d) 提取

图 4 明文域下的实验结果图

3.3 水印算法的性能测试

为了更进一步评估本算法的试用性和鲁棒性, 接下来对再分别选取 4 幅 256×256 大小的图像 (peppers、cameraman、plane、baboon) 进行性能评估. 根据式 (14), 计算在不同嵌入容量下得到的水印图像的峰值信噪比, 表 1 是密文域不同嵌入容量下的 *PSNR*, 表 2 是明文域不同嵌入容量下的 *PSNR* 值. 由表 1 和表 2, 可见随着嵌入容量的减小, *PSNR* 值越来越大, 并且算法无论是在密文域还是在明文域, 在嵌入容量高达 0.25 bpp (bpp 表示每像素嵌入的比特数[13]) 情况下, 含水印图像解密后也能获得比较清晰的图像. 在明文域下解密得到的 *PSNR* 值达到了 50.38 dB, 很好的恢复了原始图像.

表 1 密文域不同嵌入容量下的 *PSNR* (dB)

原始图像	0.25	0.0625	0.0156	0.0039
Lena	24.71	26.98	33.88	39.80
Peppers	24.39	27.85	28.45	29.27
Cameraman	21.58	24.10	33.79	40.21
Plane	24.28	28.03	36.10	41.98
baboon	21.58	26.81	33.57	39.11

与其他加密域的水印算法文献 [16] 和文献 [13] 进行比较结果见表 3. 由表 3 可见, 在无水印攻击时, 以 256×256 的 Lena 灰度图像为例, 与文献 [16] 和 [13] 中的算法比较, 本文水印算法在明文域的 PSNR 值为 50.38 dB, 文献 [16] 和文献 [13] 的 *PSNR* 值分别为 48.13 dB 和 42.81 dB, 本文算法求得的 *PSNR* 值, 高于其他算法, 说明提取出的水印图像与原始图像差异较小, 水印图像效果较好, 水印图像质量得到了改善, 同时还能实现密文域下水印的提取, 并且本文算法还具有一定的抗攻击性能, 由此可见, 本文算法的整体性能得到了改善.

表 2 明文域不同嵌入容量下的 *PSNR* (dB)

原始图像	0.25	0.0625	0.0156	0.0039
Lena	50.38	63.46	66.38	72.21
Peppers	49.45	61.65	66.64	72.37
Cameraman	49.42	60.17	66.19	72.21
plane	46.03	54.94	60.80	66.71
Baboon	49.04	60.81	66.92	74.17

表 3 本文算法与其他文献算法比较

水印算法	水印图像*PSNR* (dB)	水印形式	鲁棒性测试
文献[16]	48.13	0/1	噪声|压缩
文献[13]	42.82	二值图像	无测试
本文算法	50.38	0/1	噪声|压缩|剪切

4 结论与展望

本文基于同态加密算法 ElGamal 与 Patchwork 水印算法, 构造了一种新的同态密文域交换加密水印算法, 实现了加解密算法和水印算法先后顺序的完全交换. 与以前的水印算法相比, 本文提出的水印算法既可以保证多媒体数据在存储分发过程中的安全性, 也可以保证数据在使用以及认证过程中的安全性. 在算法性能方面, 实验结果表明, 该算法具有较高的嵌入率和峰值信噪比, 提取出的水印图像质量较好, 因此本文的算法具有一定的研究意义和参考性.

下一步的研究可以寻求更高效的方法解决同态加密域像素溢出的问题, 或者提高交换加密域水印算法的鲁棒性, 来进一步改善算法的综合性能.

参考文献

1 冯登国, 张敏, 张妍, 等. 云计算安全研究. 软件学报, 2011, 22(1): 71–83. [doi: 10.3724/SP.J.1001.2011.03958]

2 Otto-von-Guericke University at Magdeburg (GAUSS) (2005) First summary report on hybrid systems, TR: IST-2002–507932. ECRYPT European Network of Excellence in

Cryptology.http://www.ecrypt.eu.org/ecrypt1/documents.htm. [2020-03-25].

3 Kamstra L, Heijmans HJAM. Reversible data embedding into images using wavelet techniques and sorting. IEEE Transactions on Image Processing, 2005, 14(12): 2082–2090. [doi: 10.1109/TIP.2005.859373]

4 Rivest RL, Adleman L, Dertouzos ML. On data banks and privacy homomorphisms. Foundations of Secure Computation, 1978, 4(11): 169–180.

5 Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 1985, 31(4): 469–472. [doi: 10.1109/TIT.1985.1057074]

6 Paillier P. Public-key cryptosystems based on composite degree residuosity classes. Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques. Prague, Czech Republic. 1999. 223–238.

7 Chen YC, Shiu CW, Horng G. Encrypted signal-based reversible data hiding with public key cryptosystem. Journal of Visual Communication and Image Representation, 2014, 25(5): 1164–1170. [doi: 10.1016/j.jvcir.2014.04.003]

8 Zhang XP, Long J, Wang ZC, *et al*. Lossless and reversible data hiding in encrypted images with public-key cryptography. IEEE Transactions on Circuits and Systems for Video Technology, 2016, 26(9): 1622–1631. [doi: 10.1109/TCSVT.2015.2433194]

9 Xiang SJ, Luo XR. Efficient reversible data hiding in encrypted image with public key cryptosystem. EURASIP Journal on Advances in Signal Processing, 2017, 2017: 59. [doi: 10.1186/s13634-017-0496-6]

10 Xiang SJ, Luo XR. Reversible data hiding in homomorphic encrypted domain by mirroring ciphertext group. IEEE Transactions on Circuits and Systems for Video Technology, 2018, 28(11): 3099–3110. [doi: 10.1109/TCSVT.2017.2742023]

11 Zheng PJ, Huang JW. Discrete wavelet transform and data expansion reduction in homomorphic encrypted domain. IEEE Transactions on Image Processing, 2013, 22(6): 2455–2468. [doi: 10.1109/TIP.2013.2253474]

12 Guo JT, Zheng PJ, Huang JW. Secure watermarking scheme against watermark attacks in the encrypted domain. Journal of Visual Communication and Image Representation, 2015, 30: 125–135. [doi: 10.1016/j.jvcir.2015.03.009]

13 项世军, 罗欣荣, 石书协. 一种同态加密域图像可逆水印算法. 计算机学报, 2016, 39(3): 571–581. [doi: 10.11897/SP.J.1016.2016.00571]

14 Park SW, Shin SU. Combined scheme of encryption and watermarking in H. 264/scalable video coding (SVC). In: Tsihrintzis GA, Virvou M, Howlett RJ, *et al*. eds. New Directions in Intelligent Interactive Multimedia. Berlin, Heidelberg: Springer, 2008. 351–361.

15 Cancellaro M, Battisti F, Carli M, *et al*. A commutative digital image watermarking and encryption method in the tree structured haar transform domain. Signal Processing: Image Communication, 2011, 26(1): 1–12. [doi: 10.1016/j.image.2010.11.001]

16 Jiang L. The identical operands commutative encryption and watermarking based on homomorphism. Multimedia Tools and Applications, 2018, 77(23): 30575–30594. [doi: 10.1007/s11042-018-6142-y]

17 南京吉印信息科技有限公司. 一种基于模运算的交换密码水印方法及系统: 中国, 201910728982.9. [2019-11-19].

18 Bender WR, Gruhl D, Morimoto N. Techniques for data hiding. Proceeding of SPIE 2420, Storage and Retrieval for Image and Video Databases III. San Jose, CA, USA. 1995. 164–173.

19 Jiang L, Xu ZQ, Xu YY. Commutative encryption and watermarking based on orthogonal decomposition. Multimedia Tools and Applications, 2014, 70(3): 1617–1635. [doi: 10.1007/s11042-012-1181-2]

20 Wu HT, Mai WQ, Meng SY, *et al*. Reversible data hiding with image contrast enhancement based on two-dimensional histogram modification. IEEE Access, 2019, 7: 83332–83342. [doi: 10.1109/ACCESS.2019.2921407]