计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2021,30(11):164−171 [doi: 10.15888/j.cnki.csa.008198]

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

基于 DWT 密文域图像双水印算法①

张爱娈[1], 李子臣[2]

[1](北京印刷学院 信息工程学院, 北京 102600)
[2](北京印刷学院 数字版权保护技术研究中心, 北京 102600)
通讯作者: 张爱娈, E-mail: ailzhang@163.com

摘　要: 数字水印是保护数字版权的关键技术, 本文首先给出双水印算法形式化的定义, 然后基于小波变换(DWT)、SM4 分组密码算法和 Paillier 同态密码, 设计了一个密文域双水印算法. 在嵌入水印时, 将载体图像进行三重 DWT 变换, 将频带集分为加密部分、水平高频 LH3 水印部分和垂直高频 HL3 水印部分. 利用 SM4 分组密码和 Paillier 公钥密码分别对加密部分和水印部分频带系数加密, 同时利用 Paillier 公钥密码体制对数字水印信息进行加密, 利用最低有效位 (LSB) 方法, 分别在 LH3 和 HL3 的密文域嵌入两个用户水印信息. 最后 DWT 小波逆变换后生成含水印的密文图像. 在水印提取时, 由于 Paillier 具有同态特性, 实现了在解密后的明文提取水印. 实验结果表明, 该算法具有加解密速度快, 水印的不可见性好等特性.

关键词: 三重 DWT; SM4 加密算法; Paillier 同态密码; LSB 嵌入方法

引用格式: 张爱娈,李子臣.基于 DWT 密文域图像双水印算法.计算机系统应用,2021,30(11):164–171. http://www.c-s-a.org.cn/1003-3254/8198.html

DWT-Based Double Watermarking in Ciphertext Domain

ZHANG Ai-Luan[1], LI Zi-Chen[2]

[1](Information and Engineering Academy, Beijing Institute of Graphic Communication, Beijing 102600, China)
[2](Digital Copyright Protection Technology Research Center, Beijing Institute of Graphic Communication, Beijing 102600, China)

Abstract: Digital watermarking is the key technology to protect digital copyright. In this paper, the formal definition of the double watermarking algorithm is given firstly. Then, based on the Discrete Wavelet Transform (DWT), the SM4 block cipher algorithm, and the Paillier homomorphic cipher, a double watermarking algorithm in the ciphertext field is designed. When watermarking is embedded, the carrier image is transformed by triple DWT, and the band set is divided into the encryption part, the horizontal high-frequency LH3 watermarking part, and the vertical high-frequency HL3 watermarking part. The SM4 block cipher and Paillier public-key cipher are used to encrypt the frequency band coefficients of the encryption part and the watermark part, respectively. At the same time, the Paillier public-key cipher scheme is employed to encrypt the digital watermark information, and two user watermarks are embedded in the LH3 and HL3 ciphertext fields with the Least Significant Bit (LSB) method. Finally, a watermark ciphertext image is generated after the inverse wavelet transform of DWT. In the process of watermark extraction, due to the homomorphism of Paillier, the watermark can be extracted from the plaintext after decryption. Experimental results show that the algorithm is capable of fast encryption and decryption and good invisibility of watermarks.

Key words: triple DWT; SM4 encryption algorithm; Paillier homomorphic encryption; LSB embedding method

① 基金项目: 国家自然科学基金 (61370188); 北京市教委科研计划一般项目 (KM202010015009); 北京市教委科研计划 (KM202110015004); 北京印刷学院博士启动金 (27170120003/020); BIGC Project (Ec202007)
Foundation item: National Natural Science Foundation of China (61370188); General Project of Scientific Research Program of Beijing Municipal Education Commission (KM202010015009); Scientific Research Program of Beijing Municipal Education Commission (KM202110015004); Scientific Research Start-Up Fund for Doctorate of Beijing Institute of Graphic Communication (27170120003/020); BIGC Project (Ec202007)
收稿时间: 2021-01-21; 修改时间: 2021-02-23, 2021-03-16; 采用时间: 2021-03-26; csa 在线出版时间: 2021-10-22

1 引言

随着信息社会的不断发展, 双水印[1] 应用非常广泛, 比如多方验证, 为了保证一个数字合同的有效性与不可否认性, 需要同时嵌入甲方、乙方的水印信息, 只有提取并验证通过双方的水印信息才能确定该合同为有效合同, 同时合同中嵌入了双方的水印信息, 可以防止任何一方否认合同. 网络安全交易[2] 中, 为了防止 Buyer 恶意的传输拷贝购买的数字内容, 以及防止当 Buyer 发现数字内容的质量问题追溯到 Seller 时, Seller 否认交易的现象发生, 交易过程中选择将 Seller 和 Buyer 的 ID 信息同时嵌入到数字内容中, 一旦发现交易中任何一方的不法行为都可以定位到双方的身份并进行仲裁处理.

数字水印研究的历史过程中, 单水印算法[3,4] 是主要研究内容, 单水印算法功能明确, 但同时也存在功能单一的不足, 无法满足用户的多功能需求. 双水印算法[5] 因此产生. 另外变换域水印算法是水印算法中研究重点之一, 嵌入水印时并不是直接对载体图像的像素值进行操作, 而是利用选定的变换方法, 对变换后的系数进行操作. 因此, 变换域双水印[6] 是数字水印算法的研究热点, 在现实中应用广泛.

2016 年 Frattolillo 提出了基于云计算平台多方水印算法[7], 文章中设计了一个安全的交易流程, 将水印嵌入的工作交由云计算平台来完成, 云平台利用公钥密码体制的加法同态性质对密文操作来嵌入水印, 这样可以防止半可信的第三方恶意的篡改载体信息与水印信息, 保障了数字内容的安全. 但是公钥密码体制对数字内容加密解密, 效率不高, 影响交易效率.

基于小波变换的数字水印算法, 在嵌入水印之前, 首先对载体图像进行小波变换, 小波变换之后图像的小波系数集分为低频系数与高频系数. 其中, 低频信息[8] 是图片的主要信息, 低频系数的改变对图像的影响很大; 高频信息[9] 是图片的细节信息. 小波系数一般较小, 水印在这部分嵌入会很大程度地改变图像的小波系数, 因此会影响嵌入水印后的图像质量.

基于以上的问题, 本文利用 SM4 分组密码[10]、Paillier 公钥密码[11,12] 以及 DWT 数字水印算法[13], 设计了一个新的数字图像双水印算法. 首先将载体图像进行三层小波变换, 根据频带系数特性将各个频带系数集分为加密部分和水印部分, 加密部分利用 SM4 进行加密, 水印部分利用 Paillier 同态性质进行加密与水印嵌入, 与以往的完全用同态密码[7] 进行加密的水印算法相比, 很好地规避了公钥密码算法低速性的缺点.

在水印嵌入时, 本文的算法将第一个用户的水印信息嵌入到第 3 层的 *HL*3 位置, 另一个用户的水印信息嵌入到 *LH*3 位置. 嵌入水印时利用 Paillier 密码对 *LH*3、*HL*3 以及水印信息进行加密, 利用 LSB 水印算法[14] 来嵌入水印, 将加密后的密文重组输出含双水印的密文图像. 本文中将水印信息嵌入到中高频 *HL*3 和 *LH*3 的位置可以减少水印嵌入后对载体图像质量的影响, 同时结合 LSB 水印算法可以增加水印的不可见性.

在水印提取时, 可以在密文中分别提取第 1 个水印和第 2 个水印, 由于 Paillier 具有加法同态特性, 也可以在解密后的明文中分别提取第 1 个水印和第 2 个水印, 实现了解密和提取水印的交换.

实验结果表明, 相比其他双水印算法, 本文提出的算法在保证提取水印信息正确的前提下, 加解密速度快, 嵌入水印后的图像对水印的不可见性好.

2 双水印算法的分析研究

2.1 双水印概念

双水印的应用场景广泛, 下面根据双水印在本方案中的应用对其进行定义. 本方案中双水印是在保证载体信息安全的前提下, 用户双方各自嵌入不同的水印信息到载体图像中. 嵌入水印相当于在载体中设下标识, 用来表示载体的归属.

如图 1 所示, 在双水印嵌入模型中, 两个用户分两次嵌入水印信息 *w*1 和 *w*2, 得到嵌入水印的图像. 对嵌入水印的图像提取水印, 得到水印信息 *w*1 和 *w*2.

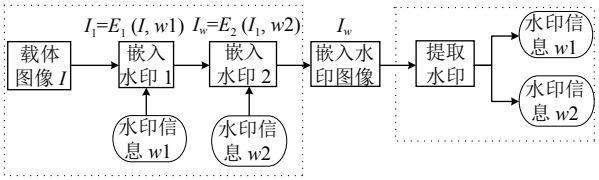


图 1 双水印模型

其中 E 为加密函数, I 表示载体图像, $w1$ 与 $w2$ 表示两个水印信息. 用户 1 在密文中向载体图像 I 嵌入水印信息 $w1$, 得到 $I_1=E_1(I,w1)$, 用户 2 在密文中向载体图像 I_1 中嵌入水印信息 $w2$, 得到 $I_w=E_2(I_1,w2)$. 双水印模型可以形式化表示为:

$$\text{水印嵌入过程}: I_w = E_2(E_1(I,w1),w2) \quad (1)$$

水印提取过程: $w=(w1,w2)=D(I_w)$ (2)

该模型中, 水印嵌入过程是对载体图像的密文信息操作的, 用户不能有目的性的篡改载体图像的信息, 保证了载体图像的安全.

2.2 Paillier 同态加密算法

密钥生成: 首先选取两个大素数 p 和 q, 计算 $n=p\times q$. 然后随机选取参数 g, 其中 g 满足 $g\in Z_{n^2}^*$ 且 $n|ord_{n^2}(g)$. 最后生成公钥为: (n,g), 私钥为: λ 或者 (p,q).

加密算法: 对任意的明文 $m(m\in Z_n)$ 加密后得到密文:

$$C=E(m)=g^m\times r^n \bmod n^2 \tag{3}$$

解密算法: 利用上述私钥对密文 C 解密得到明文:

$$m=\frac{L(C^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \tag{4}$$

对载体信息 $m1$ 与水印信息 $w1$, 分别加密后可得:

$$\begin{cases} E(w1)=g^{w1}\times r_2^n \bmod n^2 \\ E(m1)=g^{m1}\times r_1^n \bmod n^2 \end{cases} \tag{5}$$

对加密后的两个密文信息 $E(m1)$、$E(w1)$ 相乘得到:

$$E(m1)E(w1)=g^{m1+w1}\times(r_1r_2)^n \bmod n^2 \tag{6}$$

由式 (6), 两个密文相乘再解密可以得到: $D(E(m1)E(w1) \bmod n^2)=(m1+w1) \bmod n$.

由此可得, Paillier 密码算法具有加法同态性质, 即明文相加对应密文的相乘, 本文利用 Paillier 的同态性质来嵌入水印.

3 密文域双水印算法的设计

本方案中, 首先对图像进行小波分解, 小波分解后, 根据不同频带系数的特性将各个频带系数块划分成加密部分 X 与水印部分 Y, 其中加密部分 X 利用 SM4 密码算法进行加密得到 $E_{k_4}(X)$, 水印部分 Y 利用 Paillier 同态性质进行水印嵌入得到 $E_{pk_B}(Y^*)$. 将分块加密的密文和嵌入水印的密文进行重组以及小波逆变换即可得到嵌入双水印的密文图像 $E_{pk_B,k_4}(I^*)$. 用户利用 SM4 的密钥 k_4 与 Paillier 的私钥 sk_B 对图像进行解密, 得到嵌入双水印的图像 I^*. 第三方机构根据水印算法特性通过盲提取得到水印信息.

3.1 数据预处理及加密

本方案中, 需要对载体图像以及水印图像进行预处理之后再嵌入水印, 下面介绍图像预处理的流程.

3.1.1 初始化并生成密钥

初始化 SM4 密码算法的参数和 Paillier 密码算法的参数. 其中 k_4 为对称加密算法 SM4 的密钥, 是一个 128 位二进制的随机密钥; Paillier 密码算法的公私钥对为 (pk_B,sk_B), 其中公钥 pk_B 用于加密水印部分 Y 以及水印信息 $w1$ 和 $w2$, 私钥 sk_B 用于解密嵌入水印的密文信息. 每次事务中生成一套固有的公私钥, 将生成的密钥保存到文件里, 每次用到密钥时直接从文件中读取, 这样保证了一次事务中加解密共用一套公私钥.

3.1.2 分块加密

首先对图像进行如图 2 的三层小波变换, 得到 10 个频带系数集 {*LL*3, *LH*3, *HL*3, *HH*3, *LH*2, *HL*2, *HH*2, *LH*1, *HL*1, *HH*1}, 根据不同频带系数集的频带特性, 将子频带划分为两个部分: 图片中灰色的部分为加密部分记为 X, 白色部分为水印部分记为 $Y=\{Y1, Y2\}$. 其中水印部分 $Y1$ 为水平高频, 水印部分 $Y2$ 为垂直高频. 利用分组密码 SM4 的高速加密性对 X 进行加密, 利用 Paillier 密码算法对水印部分 Y 加密. 分块加密的细节流程如下:

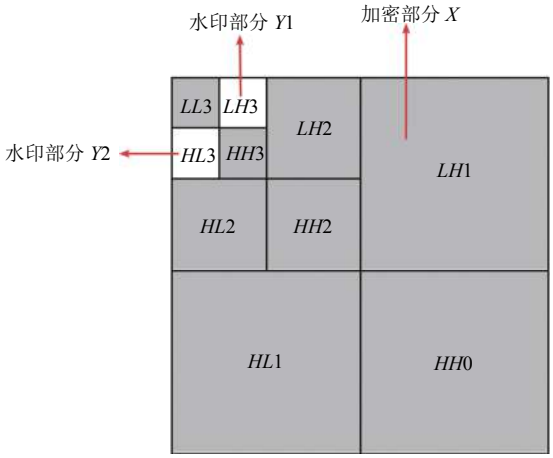


图 2 三层小波分解

(1) 将图像进行三重小波分解, 得到系数集合 {*LL*3, *LH*3, *HL*3, *HH*3, *LH*2, *HL*2, *HH*2, *LH*1, *HL*1, *HH*1}.

(2) 由上图可以得知, 加密部分 X 的频带集为 {*LL*3, *HH*3, *LH*2, *HL*2, *HH*2, *LH*1, *HL*1, *HH*1}.

1) 将频带系数集 {*LL*3, *HH*3, *LH*2, *HL*2, *HH*2, *LH*1, *HL*1, *HH*1} 拼接成为一个向量 X.

2) (SM4 加密) 使用密钥 k_4 对向量 X 进行加密, 得到密文 $E_{k_4}(X)$.

(3) 加密水印部分 $Y1$(*LH*3).

1) 将子频带系数集 $LH3$ 拼接成一个向量 $V=\{v_1,v_2,\cdots,v_n\}$.

2) 对向量 V 中的元素进行预处理. 由于 Paillier 密码算法只能对正整数进行加密解密, 然而进行小波分解后的频带系数为浮点型小数. 为了加密小波系数, 本方案中需要对各个频带系数预处理成正整数, 过程如下:

① 遍历向量集 V 中的元素, 将集合中的每一个元素进行四舍五入保留小数点后 a 位 (其中 a 的取值不同得出的水印效果不同, 在实验阶段进行了分析). 通过这样的操作, 集合 V 中的元素, 都统一成为小数点后位数相同的元素.

② 将集合中元素的正负情况保存到集合 $pnflag1$ 中.

如果 $v_i<0$,那么 $pnflag1(i)=-1$;

如果 $v_i>0$,那么 $pnflag1(i)=1$.

③将向量 V 中的系数处理成正整数向量 Pre_LH3, 对于每一个元素 $Pre\_LH3(i)$, 计算 $Pre\_LH3(i)=pnflag1(i)\times v_i\times 10^a$, 将元素 v_i 乘以 $pnflag1(i)\times 10^a$ 后, 得到的每一个 $Pre\_LH3(i)$ 元素变成正整数.

④ 遍历向量集 Pre_LH3 中的元素, 将 Pre_LH3 中的元素处理成偶数.

如果 $Pre\_LH3(i)$ 为奇数, $Pre\_LH3(i)=Pre\_LH3(i)-1$.

如果 $Pre\_LH3(i)$ 为偶数, $Pre\_LH3(i)=Pre\_LH3(i)$.

3) 使用 Paillier 算法, 利用公钥 pk_B, 对预处理后的水印部分 Pre_LH3 进行加密, 得到密文 $E_{pk_B}(Pre\_LH3)$.

(4) 加密水印部分 $Y2$. 最后得到加密后的密文 $E_{pk_B}(Pre\_HL3)$ 和系数集 $pnflag2$ (处理过程与步骤 (3) 相同).

(5) 加密水印信息: 利用密钥 pk_B, 对水印信息 $w1$、$w2$ 加密得到 $E_{pk_B}(w1)$、$E_{pk_B}(w2)$.

(6) 输出: $\{E_{k_4}(X), E_{pk_B}(Pre\_LH3), E_{pk_B}(Pre\_HL3), pnflag1, pnflag2, E_{pk_B}(w1), E_{pk_B}(w2), a\}$.

3.2 水印嵌入

对数据预处理以及加密完成后, 用户 A 得到 $\{E_{pk_B}(w1), E_{pk_B}(Pre\_LH3)\}$, 并利用 Paillier 同态性质将水印信息 $w1$ 嵌入到 $LH3$ 中. 用户 B 得到 $E_{pk_B}(w2)$、$E_{pk_B}(Pre\_HL3)$ 后将水印信息 $w2$ 嵌入到 $HL3$ 中. 整体的水印嵌入过程如图 3 所示.

(1) 用户 A 嵌水印

加密后载体图像的密文:

$$E_{pk_B}(Pre\_LH3)=\{E_{pk_B}(Pre\_LH3(1)), E_{pk_B}(Pre\_LH3(2)), \cdots, E_{pk_B}(Pre\_LH3(n))\} \tag{7}$$

密文水印信息:

$$E_{pk_B}(w1)=\{E_{pk_B}(w1(1)), E_{pk_B}(w1(2)), \cdots, E_{pk_B}(w1(n))\} \tag{8}$$

水印嵌入的过程如下:

$$\begin{aligned}&E_{pk_B}(Eem\_LH3(i))\\&=E_{pk_B}(Pre\_LH3(i))\times E_{pk_B}(w1(i)),\ 其中 i\in[1,n]\\&=E_{pk_B}(Pre\_LH3(i)+w1(i))\end{aligned} \tag{9}$$

其中, 将载体图像的密文 $E_{pk_B}(Pre\_LH3(i))$ 与水印信息的密文 $E_{pk_B}(w1(i))$ 对应相乘得到的结果相当于载体明文 $Pre\_LH3(i)$ 与水印信息 $w1(i)$ 相加再加密, 最终可以得到嵌入水印的密文图像 $E_{pk_B}(Eem\_LH3)$. 在 3.1 节中, 对频带系数进行预处理后, 每一个载体明文 $Pre\_LH3(i)$ 都为偶数, 因此嵌入水印后, 有如下规律:

① 如果 $Eem\_LH3(i)$ 为奇数, 则嵌入水印 $w1(i)$=1.

② 如果 $Eem\_LH3(i)$ 为偶数, 则嵌入水印 $w1(i)$=0.

(2) 用户 B 嵌水印

嵌入过程同上, 水印嵌入过程:

$$\begin{aligned}&E_{pk_B}(Eem\_HL3(i))\\&=E_{pk_B}(Pre\_HL3(i))\times E_{pk_B}(w2(i)),\ 其中 i\in[1,n]\\&=E_{pk_B}(Pre\_HL3(i)+w2(i))\end{aligned} \tag{10}$$

其中, 将载体图像的密文 $E_{pk_B}(Pre\_HL3(i))$ 与水印信息的密文 $E_{pk_B}(w2(i))$ 对应相乘得到的结果相当于对载体明文 $Pre\_HL3(i)$ 与水印信息 $w2(i)$ 相加再加密, 最终可以得到嵌入水印的密文图像 $E_{pk_B}(Eem\_HL3)$.

(3) 输出嵌入水印后的图像

得到密文 $E_{k4}(X)$、$E_{pk_B}(Eem\_LH3)$、$E_{pk_B}(Eem\_HL3)$ 后分别使用密钥进行解密, 得到嵌入水印后的明文图像 I^*. 具体过程如下:

① 解密 $E_{k4}(X)$: 使用 SM4 的密钥 $k4$ 对 $E_{k4}(X)$ 解密, 得到明文系数向量 U, 将向量 U 还原成小波系数集合 $\{LL3, HH3, LH2, HL2, HH2, LH1, HL1, HH1\}$.

② 解密 $E_{pk_B}(Eem\_LH3)$: 利用私钥 sk_B 对 $E_{pk_B}(Eem\_LH3)$ 进行解密可以得到明文信息: $D_{sk_B}\left(E_{pk_B}(Eem\_LH3)\right)=Eem\_LH3$.

③ 将嵌入水印后的频带集 Eem_LH3 恢复到原来的量级: $Eem\_LH3(i)=pnflag1(i)\times Eem\_LH3(i)\times(1/10)^a$.

④ 解密 $E_{pk_B}(Eem\_HL3)$: 利用私钥 sk_B 对 $E_{pk_B}(Eem\_HL3)$ 进行解密可以得到明文信息: $D_{sk_B}\left(E_{pk_B}(Eem\_HL3)\right)=Eem\_HL3$.

⑤ 将嵌入水印后的频带集 Eem_HL3 恢复到原来

的量级: $Eem\_HL3(i)=pnflag2(i)\times Eem\_HL3(i)\times(1/10)^{a}$.

⑥ 将{X, Eem_LH3, Eem_HL3}小波系数按照原来的顺序格式组合在一起, 然后使用离散小波逆变换(IDWT)将其还原成嵌入双水印的图像I^{*}.

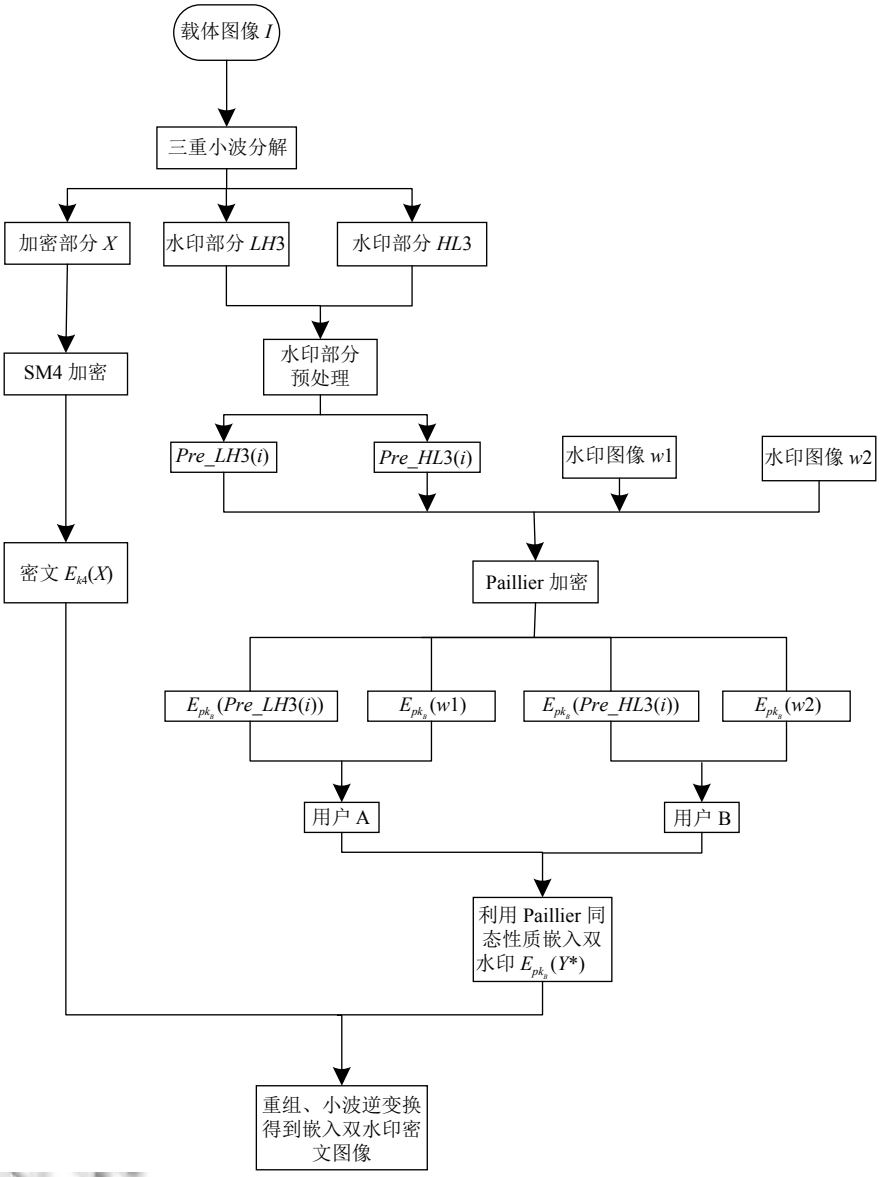


图 3 水印嵌入过程

3.3 水印提取

由上述的水印嵌入算法可以看出, 本文的水印嵌入过程在密文中进行, 而水印提取是对明文进行操作, 因此本文的水印算法具有可交换性. 水印提取的过程如下:

(1) 对I^{*}进行三层小波分解 (只需要对嵌入水印的部分: Eem_LH3、Eem_HL3 操作提取水印即可).

(2) 对 Eem_LH3 部分进行水印提取:

1) 遍历系数集合 Eem_LH3 中的元素, 将每一个元素进行四舍五入保留小数点后 a 位;

2) 对 Eem_LH3 中的每个元素操作完之后, 对每个元素 $Eem\_LH3(i)$ 进行奇偶性判断:

① 若 $Eem\_LH3(i)$ 为奇数, 则水印信息为: $w1(i)=1$, $i\in[1,n]$;

② 若 $Eem\_LH3(i)$ 为偶数, 则水印信息为: $w1(i)=0$, $i\in[1,n]$;

3) 输出水印图像 $w1$.

(3) 对 Eem_HL3 部分进行水印提取 (过程同上), 输出水印图像 $w2$.

4 实验结果与分析

本算法在 Matlab R2020a[15,16], IntelliJ IDEA 2017.3.2, Windows 10 操作系统下进行仿真测试. 实验过程中使用经典的灰度图进行测试, 并从加密参数、不可见性、时间负载的角度来说明算法的性能.

4.1 参数测试

嵌入率用来衡量水印嵌入比例, 其计算公式如下:

$$\text{嵌入率} = \frac{\text{嵌入的bit数}}{\text{载体图像像素个数}} \tag{11}$$

选取 3 幅经典的灰度图 Lena、Baboon、Camera, 在嵌入容量为 0.031 25 bpp 时, 对尺度参数 a 进行测试. 选取 6 个不同的参数 a 时, 嵌入水印后, 含水印图像的 PSNR 值见表 1.

表 1 不同 a 时含水印图像 PSNR 值

a	Lena	Baboon	Camera
−2	24.60	25.13	24.67
−1	45.43	45.43	45.21
0	65.37	65.43	65.40
1	85.27	85.31	85.33
6	184.50	184.50	184.50
12	302.41	302.19	302.42
13	306.58	306.36	306.28
15	306.68	306.488	306.34

表 1 中展示了 3 个不同的载体图像, 在 a 的取值不同时, PSNR 值的变化规律. 从表中可以发现在 a 值相同的情况下, 3 个不同的载体图像 Lena, Baboon, Camera 的 PSNR 值相差很小; 对于同一副载体图像, a 的值越大, 嵌入水印后图像的 PSNR 值越高.

实验数据分析: 本方案中参数 a, 用于预处理过程中对频带系数的倍数扩张, a 的取值越大, 水印的不可见性越好.

表 2 为在 a 的取值不同时, 提取出的两个水印信息的 NC 值变换规律. 表中的每个数据代表提取出的两个水印信息的 NC 值. 从数据中可以看出, 随着参数 a 增大, 提取的水印的 NC 值起初比较稳定, 但是当 a 取 13 时, NC 值大幅下降.

实验数据分析: 小波变换后, 小波系数为浮点型, 并且小数点后的位置并不能确定, 当 a 值超越大部分小波系数的小数位数时, 提取水印时容易将水印信息过滤掉, 因此当 a 值过大时, 不能很好地提取出水印图像.

表 2 不同 a 时提取水印图像的 NC 值

a	Lena	Baboon	Camera
−2	1/1	1/1	1/1
−1	1/1	1/1	1/1
0	1/1	1/1	1/1
1	1/1	1/1	1/1
6	0.977/0.976	0.982 /0.982	0.970/0.971
12	0.963/0.96	0.966/0.963	0.959/0.95
13	0.644/0.666	0.614/0.645	0.661/0.68
15	0.355/0.483	0.239/0.392	0.505/0.48

经过表 1 与表 2 中的数据, a 在 [−1,12] 区间内的值 PSNR 值与 NC 值都比较高. 实际应用中可根据应用需求选择具体的 a 值.

与其他的密文域双水印算法[17,18] 的性能进行比较, 结果见表 3. 下面各项性能数据是在参数 a=1, 嵌入容量为 0.031 25 bpp 时取得的.

表 3 本文算法与其他算法的性能比较

水印算法	载体图像	水印形式	嵌入水印 (PSNR)	提取水印 (NC)
文献[17]	Lena	二值图像	46.47	1/1
文献[18]	Lena	二值图像	52.95	1/1
本文算法	Lena	二值图像	85.27	1/1

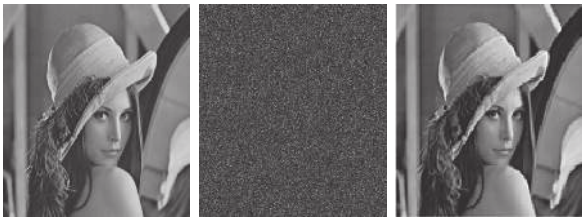
从表 3 中可以看出, 本文的 PSNR 值明显优于文献 [17,18] 的算法, 原因分析, 本文的水印嵌入算法是利用 LSB 思想对小波变换后的系数进行操作来嵌入水印, 嵌入水印信息后对载体图像的影响很小, 因此 PSNR 值较高. 由此可见, 本文算法更加适用于对数字内容质量要求较高的应用场景中.

4.2 实验结果

上述的实验结果为载体图像为 512×512 的 Lena 图, 水印图像为 2 个 64×64 的二值图像, 且参数 a=1 时的实验结果. 其中在密文中嵌入水印的实验结果见图 4, 明文中提取水印的实验结果见图 5. 此水印算法满足一定的交换性, 即在密文中嵌入水印, 明文中提取水印.

4.3 时间负载

本文的实验使用的环境是在 Matlab R2020a, IntelliJ IDEA 2017.3.2, Windows 10 操作系统下进行仿真测试, 在商业环境中为了增加方案的执行效率, 会将部分计算任务交由云计算平台[19] 来完成, 从而提高执行效率. 下面对本文算法的时间负载特性进行分析.



(a) 原始图像 (b) 嵌入水印后密文图像 (c) 嵌入水印后明文图像

图 4 密文域水印实验结果

(a) 原水印图像 1 (b) 提取水印信息 1

(c) 原水印信息 2 (d) 提取水印信息 2

图 5 双水印提取实验结果

从图 6 中可以看出, 同一个载体图像的总消耗时间随着嵌入水印的增大而增大; 同一水印图像的总消耗的时间随着载体图像的增大而增大. 但是从图中可以发现同一大小的水印图像嵌入到不同大小的载体图像的时间消耗差别很小, 而同一载体图像嵌入不同大小的水印图像时间消耗的变化幅度很大. 因此可以得出, 嵌入的水印图像的大小是影响总消耗时间的主要因素, 即利用公钥密码 Paillier 加密以及嵌入水印的时间消耗大, 而利用 SM4 分组密码加密的时间消耗非常小.

图 7 为本文算法与文献 [7] 中的加密域水印算法的时间负载对比图. 图中的实验结果为嵌入水印图像大小是 64×64 时, 不同大小的载体图像对应的加密以及嵌入水印的总时间消耗. 由图 7 可以看出, 在嵌入水印图像大小固定的情况下, 本方案中不同的载体图像的大小, 对加密以及嵌入水印的时间影响较小, 而文献 [7] 中的水印算法的总时间消耗随着载体图像大小的增加而大幅增加. 从图中可以看出, 在嵌入水印大小固定时, 本方案的水印算法相较于方案[7], 时间消耗更少.

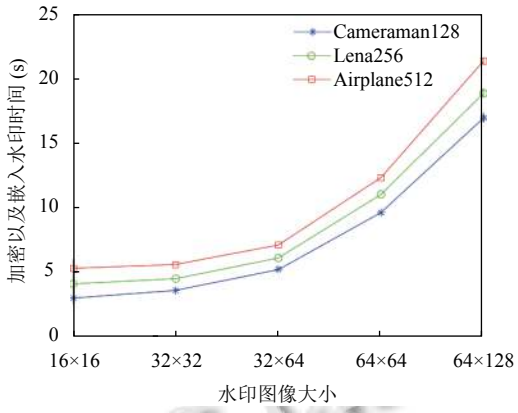


图 6 时间消耗

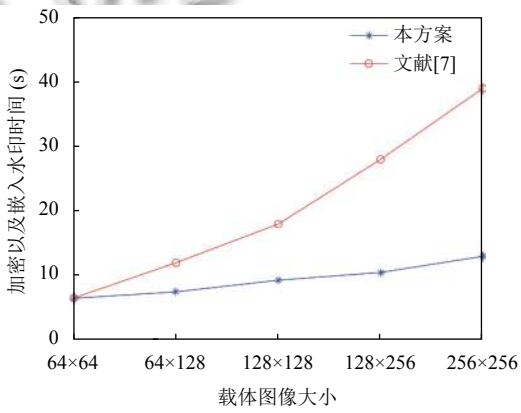


图 7 本算法与文献 [7] 算法时间消耗比较

原因分析, 文献 [7] 中的水印嵌入方法是对整幅图像利用公钥密码的同态性质嵌入水印, 在水印嵌入的过程中, 需要对整幅图像用同态密码进行加密. 而本方案将图像分为加密部分与水印部分, 只有水印部分需要利用同态性质嵌入水印, 加密部分利用对称密码 SM4 进行加密. 对称密码的加解密速度高于公钥密码, 因此本方案的效率更高.

5 结束语

本文基于 Paillier 同态加密算法、SM4 加密算法以及 DWT 小波变换水印算法, 构造了一种新的密文域双水印算法. 与其他水印算法相比, 本文的水印算法既可以保障嵌入水印后的图片质量高, 水印信息提取正确, 也可以保证高效的计算速率. 实验数据表明, 本方案中的水印嵌入方法具有较高的峰值信噪比, 提取出的水印质量好, 以及时间消耗少, 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一种更高效的水印嵌入方

法, 来提高密文域双水印算法的鲁棒性, 从而进一步改善算法的性能.

参考文献

1 叶天语, 钮心忻, 杨义先. 多功能双水印算法. 电子与信息学报, 2009, 31(3): 546–551.

2 Frattolillo F. Watermarking protocols: An excursus to motivate a new approach. International Journal of Information Security, 2018, 17(5): 587–601. [doi: 10.1007/s10207-017-0386-9]

3 Shannon CE. Communication theory of secrecy systems. The Bell System Technical Journal, 1949, 28(4): 656–715. [doi: 10.1002/j.1538-7305.1949.tb00928.x]

4 Lu ZM, Pan JS, Sun SH. VQ-based digital image watermarking method. Electronics Letters, 2000, 36(14): 1201–1202. [doi: 10.1049/el:20000876]

5 Wu KX, Yan WW, Du J. A robust dual digital-image watermarking technique. 2007 International Conference on Computational Intelligence and Security Workshops (CISW 2007). Harbin: IEEE, 2007. 668–671.

6 段加姣. 变换域双水印算法研究 [硕士学位论文]. 哈尔滨: 哈尔滨工业大学, 2015.

7 Frattolillo F. A multiparty watermarking protocol for cloud environments. Journal of Information Security and Applications, 2019, 47: 246–257. [doi: 10.1016/j.jisa.2019.05.011]

8 黄达人, 刘九芬, 黄继武. 小波变换域图像水印嵌入对策和算法. 软件学报, 2002, 13(7): 1290–1297.

9 王吉林. 一种基于离散小波变换的数字水印算法. 盐城工学院学报 (自然科学版), 2010, 23(2): 35–39.

10 陈佳哲. 几个分组密码算法的安全性分析 [博士学位论文]. 济南: 山东大学, 2012.

11 陈志伟, 杜敏, 杨亚涛, 等. 基于 RSA 和 Paillier 的同态云计算方案. 计算机工程, 2013, 39(7): 35–39. [doi: 10.3969/j.issn.1000-3428.2013.07.008]

12 夏超. 同态加密技术及其应用研究 [硕士学位论文]. 合肥: 安徽大学, 2013.

13 杨福生. 小波变换的工程分析与应用. 北京: 科学出版社, 1999.

14 李翔, 丁文霞. 基于小波变换的文本不可见水印算法. 通信技术, 2012, 45(4): 31–33, 37. [doi: 10.3969/j.issn.1002-0802.2012.04.010]

15 周伟. 基于 MATLAB 的小波分析应用. 西安: 西安电子科技大学出版社, 2010.

16 李涛. Matlab 工具箱应用指南. 北京: 电子工业出版社, 2000.

17 申丽平. 基于离散小波变换的数字图像双水印算法. 计算机工程, 2011, 37(S1): 128–130.

18 刘庆亮, 杨树国. 基于小波变换的图像双水印算法. 电脑与电信, 2017, (10): 1–5.

19 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]