Computer Science and Application 计算机科学与应用, 2019, 9(4), 663-673
Published Online April 2019 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2019.94075

Hans汉斯

Adaptive Lifting Wavelet Scheme Based on Homomorphic Encrypted Domain

Yixuan Wu, Xuan Wang

School of Physics and Information Technology, Shaanxi Normal University, Xi'an Shaanxi
Email: wyx_hnu@163.com, wxuan@snnu.edu.cn

Received: Mar. 12th, 2019; accepted: Mar. 20th, 2019; published: Mar. 27th, 2019

Abstract

With the development of information industry, data privacy's protection becomes a necessary issue to face with. Since the valuable signals need to be protected from a malicious device, they must be processed in an encrypted domain. In this paper, we proposed an encrypted adaptive lifting wavelet method by using the homomorphic properties of Paillier's cryptosystem to act wavelet decomposition on pending signal in encrypted domain. In addition, the implementation of encrypted LBP scheme is also proposed to encode detail signal which is prerequisite for classification work. The mentioned works are useful for classification servers to process data without private-key so that the sensitive message will not divulge. We conduct some experiments include reconstruction, simplified watermarking, and palmprint classification experiments in encrypted domain to demonstrate the usefulness and feasibility of our encrypted processing work.

Keywords

Adaptive Lifting Wavelet Scheme, Homomorphic Cryptosystem, Signal Processing in the Encrypted Domain

基于同态加密域的自适应提升小波

吴怡宣，王　晅

陕西师范大学，物理学与信息技术学院，陕西　西安
Email: wyx_hnu@163.com, wxuan@snnu.edu.cn

收稿日期：2019年3月12日；录用日期：2019年3月20日；发布日期：2019年3月27日

文章引用：吴怡宣，王晅. 基于同态加密域的自适应提升小波[J]. 计算机科学与应用, 2019, 9(4): 663-673.
DOI: 10.12677/csa.2019.94075

摘　要

随着信息时代的不断发展，信息安全与隐私保护问题越来越受到人们的重视，由于有价值的信号可能受到恶意攻击，因此它们必须在加密的域中进行处理。本文利用Paillier密码系统的同态特性，对加密域内的待处理信号进行小波分解，提出了一种加密的自适应提升小波方法。此外，还提出了采用加密的LBP方案对细节信号进行编码的方法，这些方法用于服务器在没有私钥的情况下进行数据处理，从而避免敏感信息泄露是非常有用的。我们进行了加密域的重构实验、水印实验和掌纹分类实验，验证了我们提出加密域自适应提升小波的有效性和可行性。

关键词

自适应提升小波，同态加密系统，加密信息处理

1. 引言

随着云计算的诞生与发展，其涉及的信息安全问题越来越受到人们的重视。处理用户的隐私数据成为了信号处理领域的一大热点，且能够实现数据的安全管理、传输、与处理工作变得至关重要。涉及一些个人用于个人身份识别的信息如虹膜、指纹、面部特征等成为研究的热点，相较而言掌纹具有更多的主线、皱纹、脊和细节点等特征，并且拥有非侵入性和高成本效益的优点，我们提出了一种由服务器端在加密状态下对掌纹进行自适应提升小波运算以及特征提取的过程。另外与媒体、版权许可相关的数字水印等信息，作为不可见水印镶嵌入产品时具有隐秘性，作为保护信息安全以及辨别版权真伪的关键信息，数字水印尤其是不可见水印有十分广泛的应用背景，我们所提出的加密信息处理方案同样可以应用于加密水印的嵌入和提取，即服务器端在加密图片上直接嵌入不可见水印，并且可以从中直接提取加密后的水印。在方案的实施过程中，针对可能出现的数据非整数，非正数，数域可能出现扩充等问题进行了研究和探讨，并且介绍了实验过程中必不可少的同态加密域数值比较的方法。

2. Pallier 同态加密域

2.1. 同态加密域系统

同态加密系统主要由 RSA [1]，ElGamal [2]，Paillier [3]和 Damgard-Jurik [4]等加密算法系统组成，本文所提出的自适应提升小波方案是基于 Paillier 同态加密域的算法方案。

同态加密系统由 Rivest 等人提出，利用这样的系统可以在不对信息解密的前提下处理加密后的信息[5]，显然地，找出明文和密文之间的代数计算关系是同态加密运算的关键。现有的同态加密系统都有其对应的计算方法变换法则，根据对应变换法则的特点可以将同态加密域分为加法同态加密和乘法同态系统，Pascal Paillier 提出的 Pailler 同态系统具有加法同态性[3]，近年来被广泛应用在安全信息处理领域，而针对自适应提升小波原本的计算方法与加法同态的性质，我们选择该加密域进行研究与实验。Paillier 加密系统的运算法则在下小节介绍。

2.2. 加密同态性与计算规则

加法同态性可以被描述为明文域的加法运算转换到密文域后变为乘法运算，令 m_1 和 m_2 表示明文，E[·]表示加密过程，D[·]表示解密过程，{pk, sk}表示一对秘钥，分别对应公钥和私钥，加密算法的加法同态性可以表示为：

$$D_{sk}\left(E_{pk}\left(m_1\right)\cdot E_{pk}\left(m_2\right)\right)=m_1+m_2 \tag{1}$$

文献[6]较详细地介绍了基于第三类陷阱门技术的一种陷阱门机制，它是复合剩余类问题的一种，除了具有加法同态性，该方法同时也具有随机自约性和自束性，因此即使不改变明文也可以得到不同的密文，研究主要用到其加密的过程，这里仅介绍算法计算规则部分。

2.2.1. 秘钥机制

参数 p 和 q 为两个大质数并计算它们的乘积，得到 $N=pq$，这样所得到的 N 很大以至于很难被分解，非零基整数 g 随机取 Z_{N^2} 的子集，使其满足 N 整除 g 的阶 $\left(g\in Z_{N^2}^{*}\right)$，通常为了方便起见，$g$ 可以取值为 $N+1$。公钥 λ 由 g 和 N 共同组成，满足条件：$\lambda=lcm\left(p-1,q-1\right)$，式中 l cm 代表最小公倍数。

2.2.2. 加密过程

规定明文 m 的范围为 $m<N$，之后随机选取一个整数 $r<N$，可以得到加密运算过程为：

$$E_{pk}\left(m\right)=g^{m}\cdot r^{N}\bmod N^2=c \tag{2}$$

其中 c 表示密文 $c\in Z_{N^2}^{*}$。

2.2.3. 解密过程

令密文满足 $c<N^2$，明文 m 可以根据以下公式计算得到：

$$D_{sk}\left(c\right)=\frac{L\left(c^{\lambda}\bmod N^2\right)}{L\left(g^{\lambda}\bmod N^2\right)}\bmod N=m \tag{3}$$

其中 $L\left(x\right)=\left(x-1\right)/N$。

特别地，根据公式(2)和(3)我们可以得到以下关系式：

$$D_{sk}\left(E_{pk}\left(m_1\right)E_{pk}\left(m_2\right)\bmod N^2\right)=m_1+m_2\bmod N \tag{4}$$

$$D_{sk}\left(E_{pk}\left(m_1\right)E_{pk}\left(m_2\right)^{-1}\bmod N^2\right)=m_1-m_2\bmod N \tag{5}$$

$$D_{sk}\left(E_{pk}\left(m\right)^{k}\bmod N^2\right)=km\bmod N \tag{6}$$

3. 同态加密特征提取算法

上小节对 Paillier 同态加密过程进行了基本算法介绍，本节在此基础上提出了相应的同态加密域下的自适应提升小波和 LBP 策略，在研究过程中同样关注了同态加密域的数值比较问题。

3.1. 同态自适应提升小波方案

通过对自适应提升小波算法的运算过程进行分析[7]，结合 Paillier 加密系统的加法同态性，我们提出了在同态加密域内实现该方案的具体方法：

首先，用户对大小为 $N\times M$ 原明文图像函数 $f(x,y)$ 按照公式(2)进行加密运算，之后得到相同大小的加密后图像 $f_e(x,y)$（下标“e”表示加密域的参数，下文中出现同样适用），将其传送给服务器端后，服

务器端在加密的情况下对密文进行相应的小波运算，特征提取等处理攻错。与传统提升小波的计算过程相类似的，本方案的准备工作为图像的像素奇偶位置重组，我们将从 $f_e(x,y)$ 分离得到 4 个密文图像子块：$x_e(n,m)=f_e(2n,2m)$，$y_{eh}(n,m)=f_e(2n-1,2m)$，$y_{ev}(n,m)=f_e(2n,2m-1)$，$y_{ed}(n,m)=f_e(2n-1,2m-1)$。为使该方案在明文域得到二值决策矩阵 $D(n,m)$，八个方向相邻像素均值和偏差值关系表，需要经过以下的运算过程：

$$\mu=\frac{1}{8}\left[y_h(n-1,m)+y_h(n,m)+y_v(n,m)+y_v(n,m-1)+y_d(n-1,m)+y_d(n,m)+y_d(n,m-1)+y_d(n-1,m-1)\right] \tag{7}$$

$$\begin{aligned}\sigma(n,m)=&\left|y_h(n-1,m)-\mu\right|+\left|y_h(n,m)-\mu\right|+\left|y_v(n,m-1)-\mu\right|\\&+\left|y_v(n,m)-\mu\right|+\left|y_d(n-1,m)-\mu\right|+\left|y_d(n,m-1)-\mu\right|\\&+\left|y_d(n,m)-\mu\right|+\left|y_d(n-1,m-1)-\mu\right|\end{aligned} \tag{8}$$

在公式(7)和(8)的基础上可以得到二值决策阵 $D(n,m)$ 的算法：

$$D(n,m)=\begin{cases}0 & \sigma(n,m)>T\\1 & \sigma(n,m)\le T\end{cases} \tag{9}$$

其中 T 为阈值我们可以根据具体情况和需要进行调整。

近似信号 $x'(n,m)$ 被定义为：

$$x'(n,m)=\begin{cases}x(n,m) & D(n,m)=0\\\frac{1}{2}\left[x(n,m)+U\right] & D(n,m)=1\end{cases} \tag{10}$$

其中 U 为更新因子，被定义为：

$$U=\frac{1}{4}\left[y_h(n-1,m)+y_h(n,m)+y_v(n,m-1)+y_v(n,m)\right] \tag{11}$$

预测参数可以根据以下公式得到：

$$p_h(n,m)=\frac{1}{2}\left[x'(n-1,m)+x'(n,m)\right] \tag{12}$$

$$p_v(n,m)=\frac{1}{2}\left[x'(n,m-1)+x'(n,m)\right] \tag{13}$$

$$p_d(n,m)=\frac{1}{2}\left[x'(n-1,m-1)+x'(n,m)\right] \tag{14}$$

根据上述的公式，细节信号参数 y'_h，y'_v 和 y'_d 可以被定义为：

$$y'_h(n,m)=\left|y_h(n,m)-p_h(n,m)\right| \tag{15}$$

$$y'_v(n,m)=\left|y_v(n,m)-p_v(n,m)\right| \tag{16}$$

$$y'_d(n,m)=\left|y_d(n,m)-p_d(n,m)\right| \tag{17}$$

求得估计信号 $x'(n,m)$ 和细节信号参数 y'_h，y'_v 和 y'_d 的过程包括了四则运算和绝对值运算，显然如果我们对整数进行加减乘运算并不会得到带小数的结果，但是从公式(7)~(17)可以看出，计算过程中同样包含了除法运算，因此我们无法确保计算结果都是整数，公式(9)包含了绝对值运算和两个数之间比较大小的问题，上述提到的运算在明文域进行都是十分方便的，但由于同态加密域中所有参与运算的参数和数据必须以整数形式表达出来这一特点，在同态加密系统中完成上述运算是一项重要且艰巨的挑战。

基于从加密后图像 $f_e(x,y)$ 分离出来的子图像 $y_{eh}(n,m)$， $y_{ev}(n,m)$ 和 $y_{ed}(n,m)$，通过对 $\sigma(n,m)$ 和 T 值扩大 8 倍的运算，我们可以得到同态加密域下的二值决策矩阵 D_e (实际上与明文域下的 D 相同)。具体方法如下：令 $y_{eh8}(n,m)=y_{eh}{}^{Q}(n,m)$， $y_{ev8}(n,m)=y_{ev}{}^{Q}(n,m)$， $y_{ed8}(n,m)=y_{ed}{}^{Q}(n,m)$ 其中 $Q=8$，再根据式(4)~式(8)，可推导出如下计算公式：

$$\mu_e=y_{eh8}(n-1,m)\times y_{eh8}(n,m)\times y_{ev8}(n,m)\times y_{ev8}(n,m-1)\times y_{ed8}(n-1,m)\times y_{ed8}(n,m)\times y_{ed8}(n,m-1)\times y_{ed8}(n-1,m-1) \tag{18}$$

$$\begin{aligned}\sigma_e(n,m)=&\left|y_{eh8}(n-1,m)-\mu_e\right|_e\times\left|y_{eh8}(n,m)-\mu_e\right|_e\times\left|y_{ev8}(n,m-1)-\mu_e\right|_e\\&\times\left|y_{ev8}(n,m)-\mu_e\right|_e\times\left|y_{ed8}(n-1,m)-\mu_e\right|_e\times\left|y_{ed8}(n,m-1)-\mu_e\right|_e\\&\times\left|y_{ed8}(n,m)-\mu_e\right|_e\times\left|y_{ed8}(n-1,m-1)-\mu_e\right|_e\end{aligned} \tag{19}$$

其中，加密域下的绝对值运算 $\left|x_1-x_2\right|_e$ 可以被表示为：

$$\left|x_1-x_2\right|_e=\begin{cases}x_1\cdot x_2^{-1} & x_1\geq x_2\\ x_2\cdot x_1^{-1} & x_1<x_2\end{cases} \tag{20}$$

式中的 x_n^{-1} 表示 x_n 的模逆。

同态加密域的二值决策矩阵 $D_e(n,m)$ 被定义为：

$$D_e(n,m)=\begin{cases}0 & \sigma_e(n,m)>T_e\\ 1 & \sigma_e(n,m)\leq T_e\end{cases} \tag{21}$$

其中 $T_e=E(T,r)^8 \bmod N^2$。如果将所有参数同时扩大相同倍数，他们的数值之间的大小关系并不会发生改变，进行这样运算相当于扩充了仅是为了确保加密域下的所有参数为整数，因此不难得知 $D_e(n,m)$ 与 $D(n,m)$ 的值实际上是相同的。本文的 3.3 小节对同态比较方法进行了介绍。

为了在随后的计算过程中同样避免小数的产生，该运算过程中需要首先将明文域原图像素扩大 16 倍，并根据公式(4)~(6)的同态法则将相应的运算过程转换至密文域中。当从密文图像 $f_e(x,y)$ 求得决策矩阵 $D_e(n,m)$ 之后，可以得到同态加密域下的近似信号 $x'_e(n,m)$ 为：

$$x'_e(n,m)=\begin{cases}E\left(x(n,m)\right)^{16} \bmod N^2 & D_e(n,m)=0\\ E\left(x(n,m)\right)^{8}\times E(U_4)^2 \bmod N^2 & D_e(n,m)=1\end{cases} \tag{22}$$

其中 $U_4=y_{eh}(n-1,m)\times y_{eh}(n,m)\times y_{ev}(n,m-1)\times y_{ev}(n,m)$，原计算公式(12)~(17)可以按法则转换到同态加密系统下，依次为：

$$p_{eh}(n,m)=x'_e(n-1,m)\times x'_e(n,m) \tag{23}$$

$$p_{ev}(n,m)=x'_e(n,m-1)\times x'_e(n,m) \tag{24}$$

$$p_{ed}(n,m)=x'_e(n-1,m-1)\times x'_e(n,m) \tag{25}$$

$$y'_{eh}(n,m)=\left|y_{eh}{}^{Q}(n,m)-p_{eh}(n,m)\right|_e \tag{26}$$

$$y'_{ev}(n,m)=\left|y_{ev}{}^{Q}(n,m)-p_{ev}(n,m)\right|_e \tag{27}$$

$$y'_{ed}(n,m)=\left|y_{ed}{}^{Q}(n,m)-p_{ed}(n,m)\right|_e \tag{28}$$

其中，式(26)~(28)中的 $Q=16$。为了在加密域直接进行图像重构，根据式(26)~(28)中绝对值运算的过程，需要保留运算过程中的数值大小关系矩阵 $C_{eh}(n,m)$， $C_{ev}(n,m)$ 和 $C_{ed}(n,m)$。图 1(a)，图 1(b)分别给出了加密域下的自适应提升小波运算步骤和其逆运算的步骤。

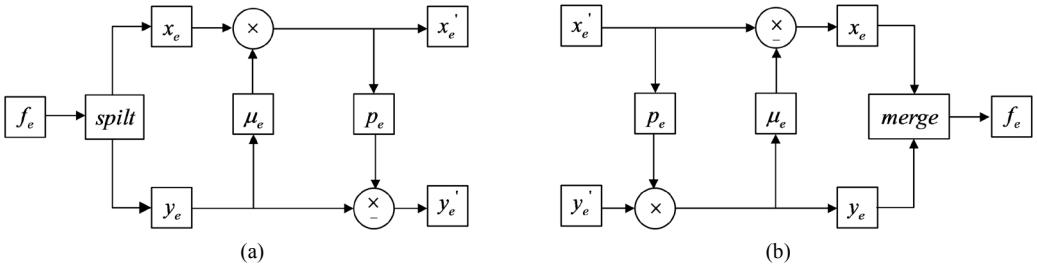


Figure 1. (a) Lifting scheme in encrypted domain; (b) Reversed scheme in encrypted domain
图 1. (a)加密提升小波方案；(b)加密小波逆运算方案

3.2. 同态加密 LBP 方案

LBP (local binary patterns)是一种局部特征算子，近年来被广泛应用于图像的识别工作当中[8] [9] [10]，LBP 算法的基本思想是：将图片分成数个小区域，选区每个区域中的中心点像素的灰度值作为一个阈值，取中心点邻近像素的值与阈值进行对比，根据比较的结果对图像像素进行某种规则的编码。图 2 是中心像素与其邻近像素的示意图，其中 x_c 表示中心像素，$x_p,(p=0,1,\cdots p-1)$ 为邻近像素，这里选取径向距离 $R=1$，$p=8$，表示编码方式考虑 8 个不同方向，由此，每个中心像素点的编码过程可以表示如下：

$$LBP_{p,R}=\sum_{p=0}^{p-1}s\left(x_p-x_c\right)\cdot 2^p \tag{29}$$

其中，门限函数 $s(x)=\begin{cases}1 & x\geq 0\\ 0 & x<0\end{cases}$ [11]，大于等于中心点像素则赋值为 1，小于则赋 0 值，编码顺序可以采取顺时针或逆时针任意一种形式，并根据公式进行加权求和运算得到直方图，保留直方图中的有效数据作为特征向量进行接下来的识别工作。

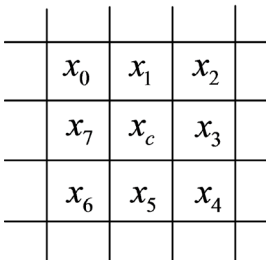


Figure 2. The neighbor sets for p = 8, R = 1in clockwise
图 2. p= 8，R = 1 相邻像素顺时针编码示意图

要在加密域进行 LBP 运算的核心问题依然是同态加密域下的两个数值比较大小的问题，3.3 节详细介绍了所要用到的同态加密域下的比较大小策略，在我们用该方法求出加密域的 $s(x)$ 的值后，式(29)依旧可以用相同的形式来计算密文图像没一个中心像素的 LBP 值。

3.3. 同态数值比较策略

对于加密域两个密文数值大小比较：$c_1=E(m_1,r_1)$，$c_2=E(m_2,r_2)$，用户需要发送 c_1，c_2 至服务器，并且将密文域从 0 到 N^2-1 划分为 k 个区间，区间的个数取决于用户在明文域的门限设置 $T_i\in Z_n$。用户需要首先将数个门限值 T_i 进行加密为 $T_{ei}^{\ u}$：

$$T_{ei}^{\ u}=E\left(T_i,r_u\right)=g^{Ti}r_u^{\ N}\bmod N^2 \tag{30}$$

其中 r_u 分别等于 r_1 和 r_2， $i=1,2,3\cdots,k$。根据文献[8]，同态比较的原则是找到加密数据在整个数据段中的位置，即被 T_{ei}^{u} 分段后所处的段位，根据公式(4)不难得出， $E(m_u,r_u)\cdot E(Inc,r_s)=E(m_u+Inc,r_u\cdot r_s)$ 可以通过计算逐步步长 Inc 接近门限 T_{ei}^{u} 来得到。很明显，m_u 与 T_{ei}^{u} 之间的距离可以通过给 $E(m_u,r_u)$ 逐步乘 $E(1,1)$ 直到 $E(m_u+Inc,r_u)=T_{ei}^{u}$， $(i=1,2\cdots,k)$ 这样的方式来进行度量。具体的比较策略如下：

$$(s_u,d_u)=\arg\min_{i,Inc}\left(E(T_i,r_u)-E(m_u,r_u)g^{Inc}\right) \tag{31}$$

其中 s_u 表示与密文 c_u 数值上最接近的门限值，d_u 衡量了与最接近的门限值之间的距离，因此通过两个密文我们可以得到两组数据 (s_1,d_1) 和 (s_2,d_2)，密文 c_1 和 c_2 之间的数值大小关系比较方法为：如果 $s_1>s_2$，则 $c_1>c_2$；如果 $s_1<s_2$，则 $c_1<c_2$，如果得到的结果是 $s_1=s_2$，则比较的结果取决于 d_u 的值：

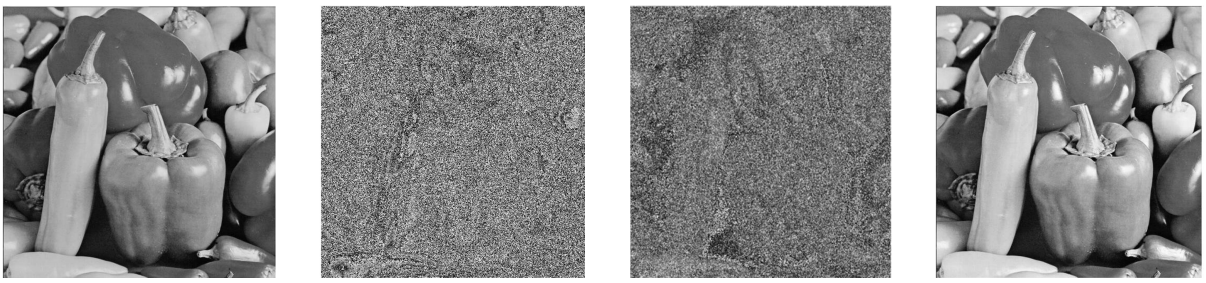
$$\begin{cases} if \quad d_1>d_2 \quad hen \quad c_1<c_2 \\ if \quad d_1<d_2 \quad hen \quad c_1>c_2 \\ if \quad d_1=d_2 \quad hen \quad c_1=c_2 \end{cases} \tag{32}$$

以上介绍的同态数值大小的比较方法可以用于加密系统的绝对值运算，LBP 运算，以及后续实验中要将用到的 K 近邻分类方法的计算过程中。

4. 仿真实验

4.1. 重构实验

图 3(a)为大小为 512 × 512 的灰度图像“peppers”作为我们重构实验的原图像信号，用两个大质数将其加密之后并按照 2.1 节提出的加密提升小波算法进行处理，并且按照公式(18)~(28)的逆运算逐步进行图像的重构过程，这里不重复介绍逆运算的细节，图 3(a)~(d)分别展示了原图像，加密后的图像，重构后的加密图像以及解密后的重构图像，实验过程中 MIM 方案[12]用于减少数域的扩充问题，也就是在运算中利用 MIM 进行数据的除法运算，从而消除了扩张因子 Q 对数域扩充的影响。从图 3(a)和图 3(d)我们可以看出，两张图片在相同位置具有相同的像素值，这意味着解密后的重构图像与原图像完全相同，整个加密重构过程并没有出现失真的问题。



(a) (b) (c) (d)

Figure 3. (a) Original gray-scale image; (b) Encrypted image; (c) Reconstruction image; (d) Decryption of reconstruction image
图 3. (a) 原灰度图像；(b) 加密后的灰度图像；(c) 加密域重构图像；(d) 解密的重构图像

4.2. 水印实验

利用我们提出的自适应提升小波策略，同样在加密域进行了图像的水印实验，本次实验采用了文献[13]中所介绍的水印嵌入方式，嵌入水印的公式为：

$$v_i'=v_i+\alpha w_i \tag{33}$$

其中，v_i表示原图像信号，w_i为需要嵌入的水印信号，选取如图 4(a)所示的陕西师范大学校徽二值图像，大小为 128 × 128 像素作为水印信号进行实验，参数 α 是从$\{1, 2, \ldots, k\}$中随机选取的一个小整数，为适当简化加密域中的水印运算，这里我们取 $\alpha = 2$。值得注意的是，在实验中一般将不可见水印嵌入中频信号中以减少对原宿主图片的影响，即 v_i表示图片的中频信号。因此，将原图进行两次小波分解之后，将水印信号 w_i嵌入第二次分解的高频信号中，此时的高频信号对于原图像来说相当于其中频信号。

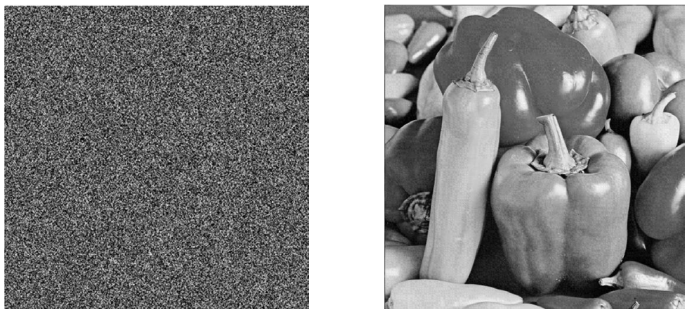
根据同态加密域的性质，水印嵌入公式(33)被改写为以下的加密形式：

$$E\left(v_i'\right) = E\left(v_i\right)E\left(w_i\right)^{\alpha} \tag{34}$$

(a) (b) (c)

Figure 4. (a) School badge as watermarking signal; (b) The extracted watermark in plaintext domain; (c) The extracted watermark in encrypted domain
图 4. (a) 校徽水印图像；(b)从明文中提取的水印图像；(c) 从密文中提取的水印图像

为了避免在水印嵌入后的重构过程中出现非整数运算，经实验验证量化因子 $Q = 2^7$ 可以保证水印嵌入和提取过程中的可行性，图 5(a)是已嵌入水印的加密图像，图 5(b)是解密后的含水印图像，实验过程中同样采取了 MIM 方法来避免数域的扩充。



(a) (b)

Figure 5. (a) Encrypted version of watermarked image; (b) Decryption of watermarked image
图 5. (a) 已嵌入水印的加密图像；(b) 解密含水印图像

由于嵌入的水印图像为二值图像，为了确保提取出的水印像素值仅由整数构成，我们采用了门限比较方案如式(35)所示从宿主图像中提取水印图像。

$$w_i = \begin{cases} 1 & D\left[E\left(v_i'\right)E\left(v_i\right)^{-1}\right] > T \\ 0 & D\left[E\left(v_i'\right)E\left(v_i\right)^{-1}\right] \le T \end{cases} \tag{35}$$

其中，由多次实验选取合适的门限值 T。图 4(b)，图 4(c)分别展示了从明文图像提取出来的水印图像和从密文图像中提取的水印图像。我们分别采用 PSNR 和归一化相关系数(NC) [6]来衡量提取水印的保真度和测量明文域和密文域提取水印信号与原水印信号的相似度。实验结果见表 1。

Table 1. The watermarking embedded and extracted performances in terms of PSNR and NC
表 1. 水印实验 PSNR 值和 NC 值

	明文域	加密域
PSNR	50.3091	50.3094
NC	0.9590	0.9577

通过实验结果可以看出，加密域的水印嵌入和提取实验结果与直接在明文域进行的结果几乎可以达到近似的结果，说明了我们所提出方案的可行性与保真性。

4.3. 掌纹识别实验

在本小节，针对香港理工大学掌纹数据库 Poly-II [14]进行了加密系统的掌纹识别实验，该数据库由两大部分组成，包含了 193 个人的共 386 个掌纹图片，总数为 7720 张大小为 384 × 284 的掌纹灰度图像，两部分图像由两次采集组成，平均时间间隔相差了 69 天，每次分别针对同一个手掌图片采集十张照片，二次采集过程中相机的焦点和光源不同，因此可以看成是由不同的掌纹采集设备所得到的数据集。

4.3.1. 实验一

本实验目的主要在于比较提出的加密算法和其明文域算法对于掌纹识别工作的准确性。由于在加密域中反复进行同态比较运算需要大量的计算时间，因此从该数据库的每部分中随机抽取了 500 张图片进行实验。分别以第一部分和第二部分十张图片中的前五张作为训练样本构成训练集，后五张作为测试样本，图 6 列举出了一些数据库的样本示例。实验提取特征的过程为：将每张图片加密后实施加密域自适应提升小波方案，得到一张近似图像和三张细节图像，再通过加密域 LBP 算法将每张细节图像转换为二进制编码的形式得到图像特征，在此基础上利用 K 近邻分类的方法对数据进行分类，表 2 分别列出了明文掌纹图片和加密条件下的掌纹图片进行分类的结果。

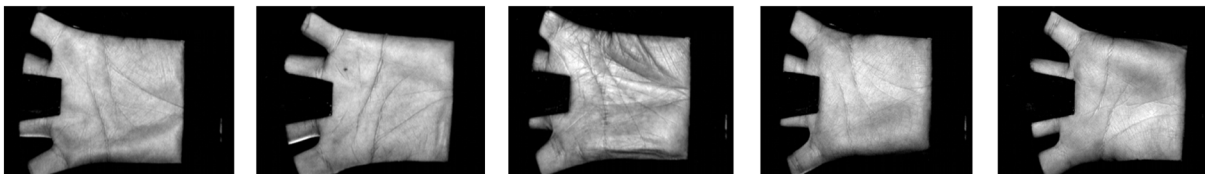


Figure 6. Few samples of palmprint database
图 6. 部分掌纹数据库图片

Table 2. CCPs of palmprints in plaintext and encrypted domain
表 2. 明文域与加密域下的掌纹识别性能

样本数据	正确分类率(CCPs%)	
	明文数据集	加密数据集
第一部分数据	93.0	93.0
第二部分数据	99.6	99.2

从表 2 可以看出，本文所提出的方案在加密数据集下进行实验，与明文条件下直接进行小波运算并提取特征再分类的识别率几乎相同，并没有因为加密过程对图像像素造成的混乱而影响识别精度，即保证了信息安全的同时也可以完成相应的识别任务。

4.3.2. 实验二

本实验的目的在于验证加密算法下的识别工作对不同聚焦光照条件下的掌纹识别工作的鲁棒性。本次

实验从每部分随机抽取 250 张图片，两部分共 500 张图片，第一部分十张图片的前五张作为训练样本，第二部分的前五张作为训练样本，对样本进行加密后用本章提出的方法进行特征提取工作，与此同时，Pan [15]，Kong [16]，2D-Gabor 小波[17]，以及传统的主成分分析[18]，线性判别分析[19]的方法也在这里与我们的方法进行了比较，表 3 分别列出了这些方法分别针对明文掌纹图像和加密掌纹图像下的识别率。

Table 3. Pattern classification percentage on the original database and encrypted palmprint with various methods
表 3. 多种方法下的明文数据与加密数据分类正确率

方法	正确识别率(%)	
	明文数据集	加密数据集
Pan 方法	96.00	30.40
Kong 方法	92.80	28.80
2D-Gabor 小波	97.20	37.20
主成分分析	94.00	44.40
线性判别分析	92.80	42.80
本文的方法	99.20	99.20

通过实验结果可以看出，我们提出的方法在明文数据集下具有更好的分类性能，而在应用于加密数据上，由于加密过程造成的掌纹结构与纹理信息的混乱，导致传统方法的识别过程无法得到需要的高精度的识别结果，而我们提出的方案由于其应用于加密域时所具有的无损的性质，从而在加密的样本数据上依然保持了与明文域等同的正确识别率，这样可以得出结论是，我们的算法在加密域中具有鲁棒性，可以应用于隐私保护相关领域的识别工作。

5. 总结

本文提出了一种无精度损失的 Pallier 加密域自适应提升小波的实现方案，在此基础上同样提出了加密域 LBP 的实现方法。基于 Paillier 同态加密系统的性质与特点与原有的自适应提升小波思想，我们科学合理推导了其在加密域的计算公式，并给出了相关扩张因子的大小以确保计算过程无误差地进行。相较于已有的其他加密系统的 SIFT，DCT 等图像变换方法，我们所提出的方案通过准确扩大像素的倍数以及通过采用相对较小的扩张因子，使加密域数据的计算更加精确。相关实验分别验证了其在图像重构、水印嵌入提取和掌纹识别方面都具有良好的应用前景，即保证了敏感隐私信息的安全性，也完成了相应的图像信息处理任务。

致　谢

在此感谢王晅导师对我研究选题方向以及科研过程中的指导，感谢杨腾飞师兄对本次论文实验方面的帮助，同时感谢实验室同学日常与我共同探讨学术问题以及在我遇到困难时伸出援助之手。

参考文献

[1] Rivest, R., Shamir, A. and Adleman, L. (1978) A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, **21**, 120-126. https://doi.org/10.1145/359340.359342

[2] Elgamal, T. (1985) A Public-Key Cryptosystems and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, **31**, 469-472. https://doi.org/10.1109/TIT.1985.1057074

[3] Paillier, P. (1999) Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. *International Conference on the Theory and Application of Cryptographic Techniques*, Prague, 2-6 May 1999, 223-238. https://doi.org/10.1007/3-540-48910-X_16

[4] Damgard, I. and Jurik, M. (2001) A Generalization, a Simplification and Some Application of Paillier's Probabilistic

Public-Key System. 4*th International Workshop on Practice and Theory in Public Key Cryptography*, Cheju Island, 13-15 February 2001, 119-136. https://doi.org/10.1007/3-540-44586-2_9

[5] Rivest, R., Adleman, L. and Dertouzos, M. (1978) On Data Banks and Privacy Homomorphisms. In: DeMillo, R.A., *et al*., Eds., *Foundations of Secure Computation*, MIT Press, Cambridge, 169-178.

[6] Run, R.S., Horng, S.J., Lai, J.L., Kao, T.W. and Chen, R.J. (2012) An Improved SVD-Based Watermarking Technique for Copyright Protection. *Expert Systems with Applications*, **39**, 673-689. https://doi.org/10.1016/j.eswa.2011.07.059

[7] Wang, X., Liang, J.H. and Wang, M.Z. (2013) On-Line Fast Palmprint Identification Based on Adaptive Lifting Wavelet Scheme. *Knowledge-Based Systems*, **42**, 68-73. https://doi.org/10.1016/j.knosys.2013.01.013

[8] Hsu, C.H., Lu, C.S. and Pei, S.C. (2012) Image Feature Extraction in Encrypted Domain with Privacy-Preserving SIFT. *IEEE Transactions on Image Processing*, **21**, 4593-4607. https://doi.org/10.1109/TIP.2012.2204272

[9] Dalali, S. and Suresh, L. (2016) Daubechive Wavelet Based Face Recognition Using Modified LBP. *Procedia Computer Science*, **93**, 344-350. https://doi.org/10.1016/j.procs.2016.07.219

[10] Yang, W.K., Wang, Z.Y. and Zhang, B.C. (2016) Face Recognition Using Adaptive Local Ternary Patterns Method. *Neurocomputing*, **213**, 183-190. https://doi.org/10.1016/j.neucom.2015.11.134

[11] Ojala, T., Pietikäinen, M. and Mäenpää, T. (2002) Multiresolution Gray-Scale and Rotation Invariant Texture Classification with Local Binary Patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **24**, 971-987. https://doi.org/10.1109/TPAMI.2002.1017623

[12] Zheng, P.J. (2013) Student Member, Discrete Wavelet Transform and Data Expansion Reduction in Homomorphic Encrypted Domain. *IEEE Transactions on Image Processing*, **22**, 2455-2468. https://doi.org/10.1109/TIP.2013.2253474

[13] Cox, I., Kilian, J., Leighton, F. and Shamoon, T. (1997) Secure Spread Spectrum Watermarking for Multimedia. *IEEE Transactions on Image Processing*, **6**, 1673-1687. https://doi.org/10.1109/83.650120

[14] Zhang, D., Kong, A., You, J. and Wong, M. (2003) Online Palmprint Identification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **25**, 1041-1050. https://doi.org/10.1109/TPAMI.2003.1227981

[15] Pan, X. and Ruan, Q.Q. (2008) Palmprint Recognition Using Gabor Feature-Based (2D) 2 PCAJ. *Neurocomputing*, **71**, 3032-3036. https://doi.org/10.1016/j.neucom.2007.12.030

[16] Kong, W.K., Zhang, D. and Li, W. (2003) Palmprint Feature Extraction Using 2-D Gabor Filters. *Pattern Recognition*, **36**, 2339-2347. https://doi.org/10.1016/S0031-3203(03)00121-3

[17] Wang, X., Lei, L. and Wang, M. (2012) Palmprint Verification Based on 2D-Gabor Wavelet and Pulse-Coupled Neural Network. *Knowledge-Based Systems*, **27**, 451-455. https://doi.org/10.1016/j.knosys.2011.10.008

[18] Wu, X., Zhang, D. and Wang, K. (2003) Fisherpalms Based Palmprint Reconition. *Pattern Recognition Letters*, **24**, 2829-2838. https://doi.org/10.1016/S0167-8655(03)00141-7

[19] Lu, G., Zhang, D. and Wang, K. (2003) Palmprint Recognition Using Eigenpalms Features. *Pattern Recognition Letters*, **24**, 1463-1467. https://doi.org/10.1016/S0167-8655(02)00386-0