基于JPEG-LS的高效掌纹图像安全编码算法

李恒建[1] 王连海[1] 张家树[2]
(山东省计算中心 山东省计算机网络重点实验室 济南 250014)[1]
(西南交通大学信号与信息处理四川省重点实验室 成都 610031)[2]

摘 要 提出一种基于JPEG-LS的对掌纹图像压缩的加密算法,它将JPEG-LS编码系统进行改进,增加了基于前馈反馈非线性动力学滤波器(FFNDF)的安全系统,即针对图像压缩编码最后的熵编码阶段,引入混沌系统,去除图像的空间冗余和相关冗余,以尽可能地降低图像加密对压缩的影响。对算法进行了安全性分析。与其它混沌压缩编码加密算法进行比较的实验结果表明,提出的压缩加密算法不仅具有较高的加密效率和安全性,且计算复杂度低,对压缩性能没有影响。

关键词 无损压缩,图像加密,混沌加密,JPEG-LS
中图法分类号 TN918.1 **文献标识码** A

Secure Palmprint Image Coding Algorithm for JPEG-LS

LI Heng-jian[1] WANG Lian-hai[1] ZHANG Jia-shu[2]
(Shandong Computer Network Key Laboratory, Shandong Computer Science Center, Jinan 250014, China)[1]
(Sichuan Province Key Lab of Signal & Information Processing, Southwest Jiaotong University, Chengdu 610031, China)[2]

Abstract Based on forward-feedback nonlinear dynamic filter(FFNDF), a secure JPEG-LS coder was proposed, and then the proposed algorithm was employed in palmprint image. According to the characteristics of JPEG-LS, FFNDF was employed to generate chaotic stream cipher and then encrypt the coded stream during in the regular mode and run mode. The security of proposed scheme was also analyzed and some other compression and encryption algorithms were also compared. The experimental results show that the proposed palmprint image encryption algorithm has the incomprehensible nature of the encryption with high efficiency and security, as well as low-complexity and no affect on image compression performance.

Keywords Image lossless compression, Image encryption, Chaotic encryption, JPEG-LS

1 引言

生物特征识别技术是指通过计算机利用人体所固有的生理特征或行为特征来进行个人身份鉴定。生物特征识别技术在网络身份鉴定和国家安全方面等领域起着越来越重要的作用。相对于先有的其他生物特征,掌纹图像具有采集方便、识别率高等优点[1]。在一些掌纹识别应用中,如对掌纹图像存档以作为刑事犯罪调查的证据时,由于掌纹图像的数据量大,需要高保真地存储原始掌纹图像。然而,掌纹图像包含个人隐私(判断亲子关系和健康状况)以及疾病信息(白血病等)[2],因此,对掌纹图像存档时采取压缩加密等保护措施,在信息安全相关领域中都有较好的发展前景。

传统上常用的加密算法,如数据加密标准DES和高级数据加密标准AES,由于计算复杂度高、加密速度慢,不适合加密图像等数据量比较大的多媒体文件。另一方面,传统的加密算法并未充分去除图像的空间冗余、视觉冗余,使得加密得到的图像未能得到充分的混淆和置乱[3]。为了提高图像加密速度,针对图像的关键部分进行部分图像加密,该类算法的重要特征是满足不可见性和不可感知性[4]。以上针对空域图像加密,然而空域图像加密破坏了图像相邻像素的相关性,不利于图像的压缩传输。K. w. wong从变换域角度出发提出变换域加密算法,其主要是通过置乱变换系数进而达到对图像加密的目的,但这些置乱措施改变了变换域系数原有的统计规律,影响了编码效率,与现有的图像压缩标准框架不兼容[5]。对于生物特征图像,如掌纹图像,一方面需要对整幅掌纹图像进行全加密以及加密后的图像具有不可感知性,即要求满足高安全性;另一方面要求加密后的图像的数据量尽可能少,以便于进一步的存储和压缩。

混沌系统通常具有伪随机性、初始值敏感性、混合性和遍历性等特点,这些特点使得混沌系统具有许多良好的密码学特性[6],在基于搜索机制的混沌加密算法基础上,许多研究者提出了在压缩过程中的嵌入式加密算法[7-9]。为了尽可能降

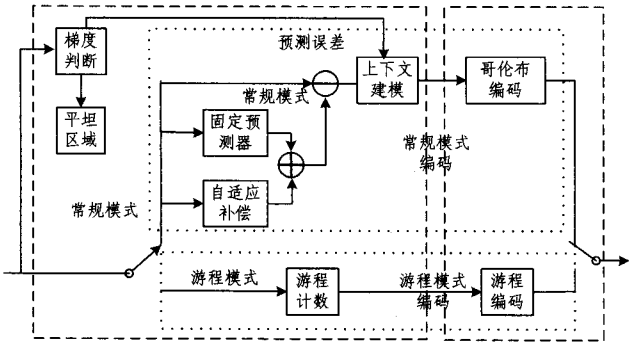
到稿日期:2012-11-07 返修日期:2013-03-01 本文受国家自然科学基金项目(61070163),山东省优秀中青年科学家科研奖励基金(BS2011DX034),山东省自然科学基金(ZR2011FQ030)资助。
李恒建(1980—),男,博士,助理研究员,主要研究方向为图像压缩加密和生物特征模板保护,E-mail:hengjianli2000@126.com;王连海(1969—),男,硕士,研究员,主要研究方向为计算机取证;张家树(1969—),男,博士,教授,主要研究方向为生物特征识别、图像处理。

低图像加密对压缩的影响并与原有图像压缩框架兼容，Grangetto 提出了随机算术编码的安全熵编码[10]，并用于 JPEG2000 的压缩加密中，实现了对图像的部分加密、全加密和访问控制。然而，JPEG2000 的无损压缩模式并不适用于较低分辨率掌纹图像无损压缩编码[11]。文献[11]将无损压缩算法分为 3 大类，分别为基于上下文的自适应预测压缩编码算法、基于字典的无损压缩方法和基于可逆变换的无损压缩编码方法。通过理论分析、算法比较和掌纹数据库测试，综合考虑压缩性能和计算复杂度，认为 JPEG-LS 这种无损压缩算法适合较低分辨率的掌纹图像压缩。

本文在文献[11]的基础上，提出了一种基于 JPEG-LS 的高效掌纹图像安全编码算法。具体而言，研究的是一种基于 JPEG-LS 的对掌纹图像压缩的加密算法，它将 JPEG-LS 编码系统进行改进，增加了基于前馈反馈非线性动力学滤波器(FFNDF)的安全系统[12]，即针对图像压缩编码最后的熵编码阶段，引入混沌系统，去除图像的空间冗余和相关冗余，以尽可能降低图像加密对压缩的影响。算法进行了安全性分析，同时和其它压缩加密算法的方案进行了定量的比较说明。

2 JPEG-LS 算法概述

JPEG-LS 是 ISO 和 IEC 合作开发的一种无损和近无损压缩标准，核心算法是基于 LOCO-I 的预测算法，编码阶段采用哥伦布编码，具有编码效率较高和运算速度快的特点[13]。JPEG-LS 主要的压缩编码技术包括：非线性预测、基于上下文统计的建模、哥伦布编码、游程编码。图 1 是 JPEG-LS 算法结构图及其相邻图像像素的因果邻域示意图。由图 1 可知，JPEG-LS 算法由模型器和编码器两部分组成，这两部分包含常规和游程两种模式。当依次读入图像像素值数据后，根据图 1(b)计算图像像素的灰度梯度值，并根据灰度梯度值的大小判断当前的图像块是否为平滑区域，若为平滑区域，表明当前块灰度值相同，编码器进入游程模式；否则进入常规模式。



(a)

c	b	d
a	x	

(b)

图 1 JPEG-LS 算法结构图及其相邻图像像素的因果邻域示意图

2.1 常规编码模式

常规模式下的预测器具体过程为，由邻域 a,b,c 的值确定一个预测值 u，这个预测器称为固定预测器，对预测残差 $e=x-\mu$ 还要附加一个自适应补偿 β，因此得到的实际差值为

$$e=s(x-\mu)-\beta, s\in\{-1,1\} \tag{1}$$

式中，s 是符号取反项，偏差 β 的作用是对差值的分布进行调整，从而使其后的编码效率最高。对预测差值 e 使用哥伦布编码方法，哥伦布编码方法适用于具有集合递减分布的非负信源，在编码前首先对差值进行 e 映射。映射后得到的 e' 满足近似几何递减分布，有助于进行哥伦布编码。Rice 第一次应用这个映射并对差值进行哥伦布编码，其称为哥伦布/Rice 编码。接下来对 e' 使用参数为 $m=2^k$ 的限长哥伦编码，参数 m 是以统计均值 $E[e']$ 的估计为基础的，即

$$k=\max\{0,\left\lceil\frac{1}{2}\log_2(E[e'])\right\rceil\}$$

$$\approx\log_2 E[\frac{\overline{E'}}{2}|\lambda_x]=\left\lceil\log_2\frac{A_{\lambda_x}}{N_{\lambda_x}}\right\rceil \tag{2}$$

限长哥伦布编码对原始哥伦布编码做了修改，因为逗号编码部分的长度 $h=\lceil 2^{-k}\cdot e'\rceil$ 有可能与 e' 的最大允许值 $e'_{\max}$ 一样大，必须使用一种方法避免过长的编码字。给定一个编码最大长度 L，只要 $h<L-\log_2 e_{\max}'-1$，就可采用普通的哥伦布编码过程。否则就产生一个逃逸编码，该编码由 $L-\log_2 e_{\max}'-1$ 位 0、后跟一位 1 组成，紧跟在这个逃逸编码之后的是值 $e'-1$ 的 $\lceil\log_2 e_{\max}'\rceil$ 位二进制表示。在 JPEG-LS 中，所有的图像样本值都是无符号整数，设其范围为 $0\leqslant x<x_{\max}$，在 JPEG-LS 中明确发送最大样本值。同时系统要求确保符号的预测差值 e_x 满足 $-\left\lfloor\frac{x_{\max}+1}{2}\right\rfloor\leqslant e_x<\left\lfloor\frac{x_{\max}+1}{2}\right\rfloor$，从这里可以推测 $\overline{e_{\max}}=x_{\max}+1$。并且，编码字限长 L 被设为

$$L=2(\max\{2,\lceil\log_2(x_{\max}+1)\rceil\}+\max\{8,\lceil\log_2(x_{\max}+1)\rceil\}) \tag{3}$$

2.2 游程编码模式

$$T[I]=\begin{cases}\lfloor I/4\rfloor, & 0\leqslant I<16\\ \lfloor I/2\rfloor, & 16\leqslant I<24\\ I-16, & 24\leqslant I<32\end{cases} \tag{4}$$

当进入游程模式后，对游程的长度和引起游程中断的数值进行游程编码，得到相应的游程比特流。通过游程编码，有可能采用相对较少的编码位来表示大量样本。令 r 表示游程长度，游程在两种情况下终止：当样本值不等于参考量时(中断)或当前图像行结尾时(耗尽)。在中断情况下，游程长度和导致中断的样本值都必须被编码；在耗尽情况下，只对游程长度编码。游程长度编码过程如图 2 所示。

游程长度编码：
Set k=T[I_{mel}],m=2^k
While r≥m
输出“1”(击中)
　更新剩余游程长度，r←r−m
　更新状态索引，$I_{mel}\leftarrow\min\{I_{max},I_{mel}+1\}$
Set k=T[I_{mel}],m=2^k
If 游程中断(游程在行结尾提前终止)
输出 0(错过)
输出 r 的二进制编码
更新状态索引，$I_{mel}\leftarrow\min\{0,I_{mel}+1\}$
Else(耗尽)
　If r>0
　输出“1”(伪击中)

图 2 游程长度编码过程

当行程在行结尾时的这一特殊过程时，没有必要显式地

发送准确的游程长度。传统的自适应哥伦布编码只有当对每次游程编码后才调整参数 k。若原始资料的统计量完全未知或频繁变化，则运用改进的哥伦布编码效果更好。在改进的哥伦布编码中，在逗点编码每一位发出后，在游程中调节参数 k；采用与传统逗点编码的规律相反的办法，改用 0 作为逗点，一个 1 代表“击中”一次，0 代表“错过”。假定 m 是 2 的整数次方（$m=2^k$），一次没有击中(0)之后，对余下的游程长度采用 k 比特二进制表示。

3 JPEG-LS 无损压缩加密算法

无损图像快速加密算法应同时满足以下要求：(1)较高的安全性：该算法应使攻击者无法从加密的数据中恢复出原始图像的相关信息，能够抵抗现有的密码攻击手段；(2)较低的计算量：这是所有加密算法都应考虑的；(3)尽可能地保留原有压缩性能：应在保证安全性的前提下，尽量提高图像的压缩性能以减少传输的数据量。从原理上讲，哥伦布编码有无限个编码字符，其特殊结构能在没有查找操作的前提下有效地进行编解码，编解码速度比较快，效率比较高。由于上述这些优良的性质，哥伦布编码已被无损图像压缩标准 JPEG-LS 采用。然而 JPEG-LS 编码系统并没有考虑安全场合下的应用。

从 JPEG-LS 编码过程的整体结构上看，JPEG-LS 算法由模型器和编码器两部分组成。模型器的构建是根据图像像素预测的残差冗余满足几何分布来设计的，使编码器尽可能地压缩图像信源。如果在建模阶段进行置乱加密，不但会影响后续压缩过程的编码效率，而且加密产生的秘密图像数据可能还面临着已知/选择明文攻击。为了保持现有的 JPEG-LS 压缩性能和在不改变原无损压缩框架的基础上实现 JPEG-LS 的安全功能，本文只考虑编码器在编码模式下进行加密，即压缩和编码过程的加密。

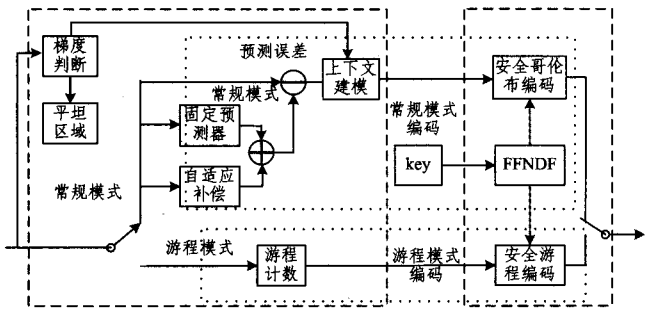


图 3 基于 FFNDF 的 JPEG-LS 加密框图

编码过程包含常规模式的自适应哥伦布编码和游程模式编码。基于 FFNDF 的混沌流密码具有密钥空间大等优点[12]，为了获得好的加密效果，利用了流密码来随机控制哥伦布编码和游程编码的编码方式，达到了加密的目的，加密的框图如图 3 所示。在 JPEG-LS 常规模式编码中，只提供一种哥伦布编码方式。在安全的随机哥伦布编码中，通过混沌密钥流控制选择不同的哥伦布编码方式。对于游程编码算法而言，根据混沌流密码控制“击中”和“错过”随机输出，编码过程如图 4 所示。为了提高其安全性，对中断样本编码采用直接异或的加密方式。在没有密钥的情况下解码时，无法正确定位出击中和错过情况，因此无法正确得到解密图像。游程编码能对图像的平滑区域进行有效压缩，在这些区域大量的图像像素值相同，随机化击中和错过，将有可能造成游程在行结尾前提前终止，造成解码后的图像比原始的图像要小。随机化击中和错过避免了利用图像某一区域大部分像素都一致的情况下的统计攻击，增加了加密算法的安全性。

基于混沌的游程编码，设混沌流密码的序列为 s_i

```
Set k=T[I_mel], m=2^k
While r≥m
  If s_i=1
      输出“1”(击中)
  else
      输出“0”(伪击中)
  更新剩余游程长度, r←r−m
  更新状态索引, I_mel←min{I_max, I_mel+1}
  Set k=T[I_mel], m=2^k
  If 游程中断(游程在行结尾提前终止)
    If s_i=1
        输出 0(错过)
    Else
        输出 1(伪错过)
    输出 r 的二进制编码
  更新状态索引, I_mel←min{0, I_mel+1}
Else(游程继续直到行结尾,耗尽)
If r>0
      If s_i=1
          输出“1”(伪击中)
      Else
          输出“0”
```

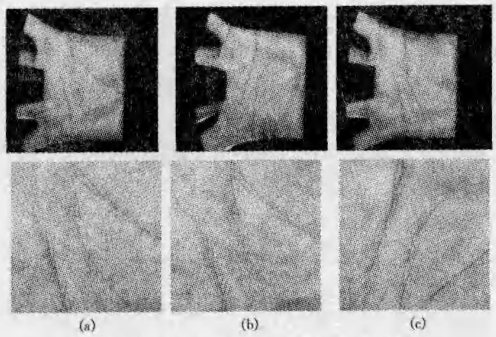
图 4 基于 FFNDF 的游程编码加密过程

由于 JPEG-LS 解密过程和加密过程相反，在加密过程中，如果对常规模式和游程编码模式都加密，将会导致常规和游程模式编码的码流混合在一起。解密时，在没有正确密钥的情况下，将无法对当前采用的常规和游程模式进行正确判断。由于 JPEG-LS 是一种预测编码算法，若当前解码数据发生错误，也将导致后面的预测结果错误即无法正确建模，无法得到有意义的图像。

4 实验测试结果及分析

4.1 实验设置

实验平台为普通的 PC 机，机器配置为：Windows 7 操作系统，内存为 2G，整个仿真程序通过 VC++6.0 实现，通过在 JPEG Lossless Version2.2 上增加加解密部分实现无损安全编解码，所有运算均采用 IEEE754 双精度浮点格式。所选择的掌纹图像源自香港理工大学的掌纹图像库[14]。该数据库包含 7752 个大小为 384×284 的灰度掌纹图像，图像的编码格式为 BMP。掌纹图像的分辨率为 75dpi，来自 386 个手掌，分两个阶段对每个手掌采集大约 20 幅图像，每个阶段大约采集 10 幅掌纹图像，采集的时间间隔大约为 2 个月。采用类似于文献[15]中的预处理方法，提取大小为 128×128 的感兴趣 ROI 区域。该数据库上典型的原始掌纹及其感兴趣区域如图 5 所示，下文选择图 5 中的 6 幅图像作为测试的掌纹图像。实验采用 2 阶 FFNDF，其初始值为 0.6587，状态参数为0.3564和 0.8021，控制参数为 0.35 和 0.85。

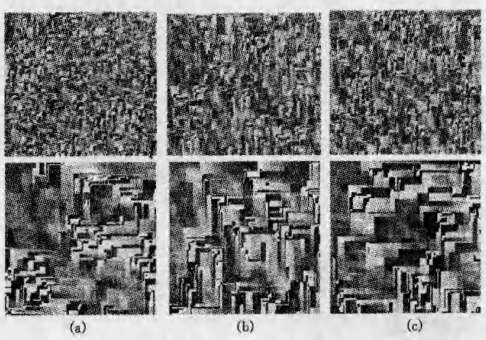


(a)、(b)和(c)的上面3幅图为原始的掌纹图像，
下面3幅图为对应的感兴趣区域

图5　原始掌纹及其感兴趣区域

JPEG-LS包括两部分：预测器和预测残差像素编码器。为了能更加直观地显示加密常规模式和游程模式对解码重构的掌纹图像的影响，实验分别给出常规模式加密的结果、游程模式加密结果以及常规和游程模式全加密的结果，并考察对每一类压缩编码数据加密的算法安全性，给出了加密算法的密钥空间。实验中，算法是在压缩编码的过程中对其中的编码模式进行加密，下面从压缩得到的比特流的统计随机性和重建的掌纹图像的可感知性两方面讨论掌纹加密算法的安全性。具体而言，采用峰值信噪比(PSNR，Peak Signal-to-Noise Ratio)来衡量未正确解码时图像的质量、可读性以及包含的信息，根据密钥流的长度与JPEGLS无损压缩算法产生的符号个数来衡量加密效率，并根据压缩倍数(原始图像所占有的数据量和安全编码后数据量之比)来衡量本文算法的压缩效果以及是否影响原有的JPEGLS的压缩性能。

4.2　JPEG-LS的常规模式加密



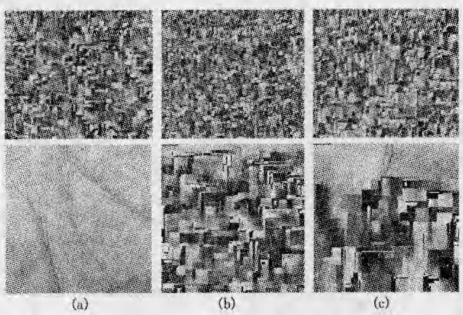
从左到右，从上到下，其PSNR依次为：6.2281dB，6.5456dB，
6.3389dB，8.1168dB，8.2087dB和8.0742dB

图6　常规模式加密后得到的解码图像

图6为只对JPEG-LS的常规编码模式进行加密而按照正常的解码方式进行解码得到的结果。由于全加密得到的图像的PSNR较低，得到的掌纹图像不具有可读性和理解性，也无法查看到掌纹图像的任何信息，这就保护了掌纹图像以及蕴含的身份信息。对JPEG-LS的常规编码模式加密时，利用混沌流对JPEG-LS中的两种常见的哥伦布编码方式进行随机切换。在解码时，只按照其中的一种哥伦布编码方式进行解码，如果攻击者无法获得正确的解密密钥，就有可能把游程模式的压缩编码数据码流误判为常规数据进行解码。在JPEG-LS中，由于利用相邻像素的关系对上下文建模，如果当前的图像像素灰度值解码发生错误，就会导致后面的预测模式和上下文环境标志的选择发生错误，进而导致将图像像素灰度值错误很快传播到整个掌纹图像，产生雪崩效应，使整个解码得到的图像看起来“面目全非”，这有利于保护掌纹蕴含的隐私信息。这表明在不影响压缩效率的情况下，对JPEG-LS中常规模式进行加密能够达到图像不可感知和不可理解，保护了掌纹中的隐私信息。

4.3　JPEG-LS的游程模式加密

图7为只对JPEG-LS编码系统的游程模式进行加密得到的结果。对于原始掌纹图像，由于存在黑色背景，在掌纹部分和黑色背景部分存在着突变的情形，出现混淆“击中”和“错过”的情况，导致游程编码长度错乱，得到的掌纹图像不具有可读性和理解性，也无法查看到掌纹图像的任何信息。而对于ROI部分只进行游程部分加密，根据图像的像素灰度变化表现出不同情况，大概分为3种，分别如图7(a)、(b)和(c)的ROI区域所示。在图7(a)的ROI区域游程编码的次数为0，在图7(b)的ROI区域游程编码的次数为5，在图7(c)的ROI区域游程编码的次数为2。由于在JPEG-LS编码过程中，不存在游程编码模式或者游程编码出现的次数比较少，导致出现没有加密或者部分加密的情况，这显然不能对掌纹图像的隐私进行保护。JPEG-LS在解码时，是通过上下文进行建模决定当前的编码模式，当前解码错误导致后面的都不能正确解码。因此，尽管JPEG-LS在进行模式选择时，图7(c)的ROI区域游程编码仅出现2次，但是在没有正确密钥时，大部分掌纹内容不能正确解码。



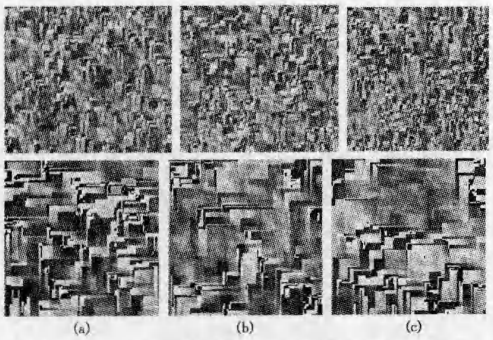
从左到右，从上到下，其PSNR依次为：6.4663dB，6.4670dB，
6.2710，+∞dB，9.2019dB和15.4457dB

图7　游程模式加密后得到的解码图像

4.4　JPEG-LS的常规模式和游程模式全加密

该部分研究JPEG-LS编码系统的常规模式和游程模式全加密的情况。图8是对游程模式和常规模式加密、没有解密密钥解码得到的掌纹图像。JPEG-LS编码分为两种模式，对两种模式都加密，就不会出现由于只对游程模式加密而导致部分或者没有加密的情况，图8也说明了这一点。在常规模式中，解码只用一种方式，将造成游程和常规模式中的数据码流误判混用，导致错误解码。在JPEG-LS解码中，需要根据已解码的图像灰度值建模上下文，所以当前的错误会扩展到后续解码过程。常规模式的解码错误有可能导致在游程编码中混淆“击中”和“错过”，产生游程解码长度的错误。一般而言，常规编码和游程编码都交替进行，这样就增加了正确解码的难度，提高了算法的安全性。全加密得到的图像的PSNR较低，得到的掌纹图像不具有可读性和理解性，也无法查看到掌纹图像的任何信息，这就保护了掌纹图像以及蕴含

的身份信息。



(a) (b) (c)

从左到右，从上到下，其 PSNR 依次为：6.4978dB，6.4217dB，6.0814dB，7.2710dB，8.4919dB 和 9.0820dB

图 8 全加密的图像，得到的解码图像

为了能更加真实、客观反映本文算法的效果，表 1 给出了整个图像库的测试统计结果，需要说明的是，表 1 的数据是计算整个掌纹库（包括 7752 张掌纹图像）得到的平均值，它包括未正确解码图像的 PSNR（单位：dB）、压缩倍数、计算时间和加密效率。从表 1 的数据和上面的实验可以看出，对掌纹图像进行加密，保护掌纹的隐私信息，必须选择对常规模式加密。事实上，常规模式对相邻像素相关比较强的图像（一般图像都具有这样的属性）进行编码。而游程模式主要针对图像的平滑部分进行编码，如果图像存在这样的特殊区域，将大大提高算法对图像的压缩性能。因此，从加密效率而言，游程模式的加密效率最高，远远高于常规模式加密。然而由于图像的平滑区域有限，可能出现加密强度不够、安全性能不高的情况。对于不具有足够平滑的图像，如图 5(a)的 ROI 区域，由于编码过程没有游程部分，将导致其不能加密。

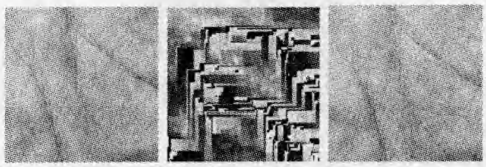
表 1 整个图像的测试统计结果

加密方式		未正确解码图像的 PSNR（单位：dB）	压缩倍数	计算时间（单位：s）	加密效率
部分加密（常规模式加密）	原始掌纹	6.3021	2.3540	0.0537	4.1828
	掌纹的 ROI	7.9823	1.4031	0.0149	5.7347
部分加密（游程模式加密）	原始掌纹	12.7561	2.3540	0.0348	78.6827
	掌纹的 ROI	6.2984	1.4031	0.0096	38159
全加密（常规和游程模式加密）	原始掌纹	6.2376	2.3540	0.0657	3.9712
	掌纹的 ROI	7.5380	1.4031	0.0205	5.7306

综上所述，对于非光滑的图像，由于用 JPEG-LS 进行无损压缩时，并不存在游程模式或存在的游程模式较少，因此，只对游程模式加密不能很好地保护掌纹的隐私信息。为了提高算法的安全性和掌纹隐私保护性能，要联合常规模式加密。加密算法也不影响 JPEG-LS 的压缩性能。相对于普通的流密码，加密效率提高了大约 4～5 倍。在压缩编码的过程中进行加密，耗时比较少，速度也比较快。

4.5 密钥敏感性和密钥空间

相对于部分加密算法，全加密算法具有高的安全性，而加密效率稍微低于常规模式。为了能够很好地保护掌纹图像的隐私，采用全加密算法的掌纹图像。为了不被穷举攻击破解所提的安全编解码算法，采取的混沌加密系统应具有尽可能大的密钥空间。本文考察的是 2 阶 FFNDF 算法对密钥的初始值敏感性，它反映了密钥空间的大小，衡量了算法抵抗攻击的能力。在混沌序列的产生过程中，2 阶 FFNDF 有 1 个初始值、2 个状态参数和 2 个控制参数。在双精度的浮点运算下，不同参数的精度是不同的。图 9(a)为密钥正确的解码图像；图 9(b)为解密密钥和加密密钥差值为 1.0×10^{-15} 的解密图像，得到的图像峰值信噪比为 8.5511dB；图 9(c)为解密密钥和加密密钥差值为 1.0×10^{-16} 的解密图像，解密图像和原始图像相同。这说明初始值的精度为 10^{-15}，同理可得出两个状态参数的精度为 10^{-16}，两个控制参数的精度也为 10^{-16}。又由于参数的变化范围在(−1，1)之间，因此密钥空间为 $2\times10^{15}\times10^{16\times4}=2\times10^{79}$。密钥空间足够大，可有效抵抗密钥的穷举攻击。



(a) 正确密钥解密 (b) 加密敏感性 1.0×10^{-14} (c) 加密敏感性 1.0×10^{-15}

图 9 密钥敏感性测试

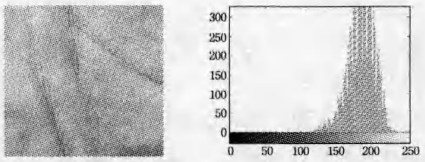
5 与其它基于混沌的压缩加密方案比较

5.1 与基于图像空域的混沌算术编码的压缩加密方案比较

该方案直接用算术编码对掌纹空域图像进行加密。为了方便加解密操作，需要在加密前做一个预处理，即把图像像素转化为比特数据流的形式。一般而言，掌纹图像为灰度图像，每一个像素占 8 比特，如果掌纹图像的大小为 $M\times N$，那么在加密时需要将其转化为 $M\times N\times8$ 的比特数据流，然后把这些数据流作为明文输入加密。掌纹图像的 ROI 为 128×128，平均熵值为 6.2022。即在空域，如果直接对掌纹图像进行熵编码，那么最大压缩倍数可以达到 8/6.2022=1.2899。而在 Mi 的方案中[16]，首先将图像数据转化为二进制数据，输入编码的数据量为 131072bit，加密压缩后的数据量为 12981bit，压缩倍数为 1.0097（比为 1∶0.9904）。在转化为二进制的数据中，符号“1”的概率为 0.5566，符号“0”的概率为 0.4434。在加密密钥和解密相差 0.01 的情况下，对数据进行解密压缩后得到符号“1”的概率为 0.6038，符号“0”的概率为 0.3962。实验统计得到的错误比率为 0.4874，而按照文献[17]的计算公式得到的为 0.4882，理论和实际计算的基本相符合。

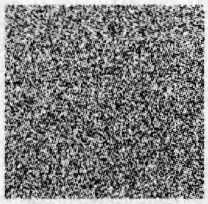
$$\begin{aligned} BER &= 1-p_0\times q_0-p_1\times q_1 \\ &= 1-0.6038\times0.5566-0.3962\times0.4434 \\ &= 0.4882 \end{aligned} \tag{5}$$

图 10 给出了原始掌纹图像（图 10(a)）及其像素值的灰度直方图（图 10(b)）。在解密和加密密钥相差 0.02 的情况下，为了更加直观地显示加密前后图像像素灰度直方图的变化情况，给出了在没有密钥时得到的解码图像及其直方图（图 11）。图 11(c)显示了灰度值为 100 到 160 之间的直方图，解密得到的图像的 PSNR 比为 9.9793dB，具有不可感知和理解性。在加密过程中，论文采取的措施是对图像像素的位平面按照比特进行加密，因此，解码得到的掌纹图像的灰度直方图并不像传统对空域图加密算法中需要满足置乱+扩散那样具有均匀分布的属性。

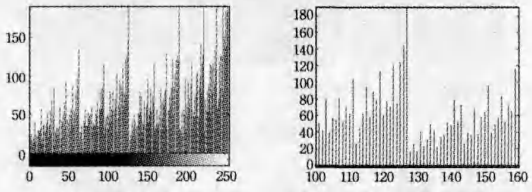


(a) 原始图像　　(b) 灰度直方图

图 10　原始的掌纹图像及其灰度分布直方图



(a) 没有密钥的前提下解密后图像



(b) 灰度直方图　　(c) 局部放大

图 11　在没有密钥时的解密图像及其灰度直方图

未知密钥的情况下，解码得到的数据比特流中符号“1”出现的概率(0.6038)要大于符号“0”的概率(0.4434)，因此在相邻像素值中，像素灰度值奇数的图像像素个数应大于相应的前一个像素值为偶数的像素个数，如像素值为 127 的个数要大于 126；并且在一定范围内，出现连续“1”符号的灰度值的像素个数在增加，这将导致一些灰度值在某些位置可能产生突变，如 127 的二进制表示为“01111111”，128 的二进制表示为“10000000”。

5.2　与嵌入式压缩加密方案比较

在基于搜索机制的 Baptisa 混沌加密方案中[18]，为了避免混沌轨迹的泄漏，需要很多次的混沌迭代，因此加密得到密文的数据量是原来明文的两倍甚至更多[7]。为了降低密文的数据量以便存储和传输，香港城市大学 K. W. Wong 提出了一种基于搜索机制的混沌数据压缩加密算法[7]，它的基本思想是根据信源符号的个数和概率分布进行搜索迭代，并把迭代次数作为密文。与 Baptisa 基于迭代搜索机制的混沌加密算法不同的是：(1)它的混沌相空间的划分范围是根据信源符号的概率确定的，而文献[16]的混沌相区间是均匀的。对于符号出现频次较多的，混沌相空间分配的占用区间范围就较大，概率小的符号区间长度就较短，甚至一些出现频率非常低的符号无需迭代，直接进行异或加密。这种不平均分布将增加密文的可压缩性。(2)对迭代次数用 Huffman 进行编码，对编码的数据进行加密。K. W. Wong 使用的静态的 Huffman 编码，在很多场合，往往需要在计算时估计动态信源的概率，进而动态设计查找表(Look-Up Table)。对此，李恒建等进行了如下改进：用自适应概率估计的方法设计动态查找表，用动态的自适应算术编码压缩获得的字符，进而获得较高的压缩比[8]。对实验采用的掌纹图像而言，其压缩倍数为 1.0229(压缩比为 1:0.9776)。

掌纹图像等多媒体数据中存在的不仅仅是熵冗余，而更多的是其它冗余，如空间冗余、相关冗余等。事实上，图像的主要冗余存在相邻像素的相关性，空间域图像像素间熵冗余占很少一部分。仅仅考虑图像像素熵冗余方式而采用压缩编码算法得到的图像压缩效率非常低，得到的加密文件大小和原来的差别不大，实验也说明了这一点。因此在基于图像的多媒体数据压缩加密编码中，更多的是去除图像的其它冗余。JPEG-LS 是先预测后熵编码的无损图像压缩算法，对其中的哥伦布编码和游程编码算法加密，如果解密时没有正确密钥，将会导致预测建模错误，并且将错误传播到整个图像，使图像具有不可理解性，从而保护掌纹图像包含的个人隐私信息，进而推动生物特征识别技术的应用和发展。

结束语　随着对生物特征技术的深入研究及其应用范围的扩大，生物特征图像包含的个人遗传和健康信息越来越引起人们的关注。生物特征图像中，如虹膜图像包含糖尿病等健康信息，掌纹上出现猿线的人很大可能也患有白血病。本文提出一种基于 JPEG-LS 的对掌纹图像压缩的加密算法，其通过加密等密码手段实现掌纹图像的隐私保护。首先对 JPEG-LS 编码系统进行改进，增加了 FFNDF 的安全系统，即针对图像压缩编码最后的熵编码阶段，引入混沌系统，去除图像的空间冗余和相关冗余，尽可能地降低图像加密对压缩的影响；设计出适合掌纹图像的无损压缩加密算法，与其它基于混沌的压缩加密算法的方案相比，提出的算法具有较高的安全性，对压缩无影响。

参 考 文 献

[1] 岳峰，左旺孟，张大鹏. 掌纹识别算法综述[J]. 自动化学报，2010,36(3):353-365

[2] Adams K, David Z, Mohamed K. A survey of palmprint recognition[J]. Pattern Recognition, 2009, 42(7): 1408-1418

[3] Grangetto M, Magli E, Olmo G. Multimedia selective encryption by means of randomized arithmetic coding[J]. IEEE Trans. Multimedia, 2006, 8(5): 905-917

[4] Massoudi A, Lefebvre F, Vleeschouwer C D, et al. Overview on Selective Encryption of Image and Video: Challenges and Perspectives[J]. EURASIP Journal on Information Security, 2008, 179290

[5] Yuen C H, Wong K W. A chaos-based joint image compression and encryption scheme using DCT and SHA-1[J]. Applied Soft Computing, 2011, 11(8): 5092-5098

[6] Kocarev L. Chaos-based cryptography: a brief overview [J]. IEEE Circuits and Systems Magazine, 2001, 1(3): 6-21

[7] Wong K W, Yuen C H. Embedding Compression in Chaos-based Cryptography IEEE trans[J]. On circuits and systems-II: Express BRIEFS, 2008, 55(11): 1193-1197

[8] Li H J, Zhang J S. Embedding arithmetic coding in Chaos-based cryptography[J]. Chinese Physics B, 2010, 19(5): 1-9

[9] Wong K W, Lin Q Z, Chen J Y. Simultaneous arithmetic coding and encryption using chaotic maps[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2010, 57(2): 146-150

[10] Grangetto M, Torino E M, Olmo G. Multimedia Selective Encryption by Means of Randomized Arithmetic Coding[J]. IEEE Transactions on Multimedia, 2006, 89(5): 905-917

(下转第 181 页)

2004,30(5),295-310

[3] Object Management Group: Unified modeling language: superstructure, version 2[R]. OMG Adopted Specification, formal/05-07-04 ,2005

[4] Object Management Group: UML profile for schedulability, performance, and time specification[S]. OMG Adopted Specification ptc/05-01-02, July 2005

[5] D'Ambrogio A, Bocciarelli P. A model-driven approach to describe and predict the performance of composite services[C]// Cortellessa V, Uchitel S, Yankelevich D, eds. WOSP. ACM, 2007:78-89

[6] Hillston J, Wang Y. Performance evaluation of UML models via automatically generated simulation models[C]// Jarvis S A, ed. Proceedings of the 19th Annual UKPerformance Engineering Workshop. Warwick, UK, 2003:64-78

[7] Tribastone M, Gilmore S. Automatic Extraction of PEPA Performance Models from UML Activity Diagrams Annotated with the MARTE Profile[C]// Princeton, WOSP. ACM, New Jersey, USA, 2008:67-78

[8] Bernardi S, Donatelli S, Merseguer J. From UML sequence diagrams and statecharts to analysable Petri net models[C]// Proc. 3rd Int. Workshop on Software and Performance (WOSP02). Rome, July 2002:35-45

[9] Lo'pez-Grao J P, Merseguer J, Campos J. From UML Activity Diagrams To Stochastic Petri Nets[C]// Fourth Int. Workshop on Software and Performance (WOSP 2004). Redwood City, CA, Jan. 2004:25-36

[10] Merseguer J. Software performance engineering based on UML and Petri nets[D]. University of Zaragoza, Spain, March 2003

[11] Petriu D C, Shen H. Applying the UML performance profile: Graph grammar-based derivation of LQN models from UML specifications [C] // Computer Performance Evaluation / TOOLS. Lecture Notes in Computer Science, Springer, 2002: 159-177

[12] Gu G P, Petriu D C. XSLT transformation from UML models to LQN performance models[C]// WOSP'02. Rome, Italy, July 2002

[13] Koziolek H, Reussner R. A Model Transformation from the Palladio Component Model to Layered Queueing Networks[C]// Kounev S, Gorton I, Sachs K, eds. SIPEW 2008. LNCS 5119, 2008:58-78

[14] Woodside C M, Petriu D C. Performance by unified model analysis(PUMA)[C]// Proceedings of the Fifth International Workshop on Software and Performance, WOSP. ACM, 2005:1-12

[15] Woodside C M. From Annotated Software Designs(UML SPT/MARTE)to Model Formalisms[C]// Bernardo M, Hillston J, eds. SFM 2007. LNCS 4486, 2007:429-467

[16] Mizan A, Franks G. An Automatic Trace Based Performance Evaluation Model Building for Parallel Distributed Systems [C]// Proceedings of the second joint WOSP/SIPEW international conference on performance engineering(ICPE 2011). 2011

[17] Jiang De-jun, Pierre G, Chi C-H. Autonomous Resource Provisioning for Multi-Service Web Applications [C]// 19th proceeding: International World Wide Web Conference. 2010

[18] Zhang Wen-bo, Huang Xiang, Wei Jun. An Aspect-oriented Modeling Approach to Predict Performance of JCA-based Systems[C]// International Conference on Interoperability for Enterprise Software and Applications, I-ESA2009. 2009:140-146

[19] http://oncepd.sourceforge.net/

[20] Woodside M. Software Resource Architecture [J]. Journal of Software Engineering and Knowledge Engineering, 2001, 11(4)

[21] Woodside M. Resource Architecture and Continuous Performance Engineering[C]// Overhage S, et al., eds. QoSA 2007. LNCS 4880, 2007:1-14

[22] Welsh M, Culler D, Brewer E. SEDA: An architecture for well-conditioned, scalable Internet services[C]// Proceedings of the 18th Symposium on Operating Systems Principles(SOSP). October 2001

[23] Cherkasova L, Fu Y, Tang W, et al. Measuring and Characterizing End-to-End Internet Service Performance [J]. Journal ACM/IEEE Transactions on Internet Technology (TOIT), 2003, 3(4):347-391

[24] Woodside M, Frank G. The Future of Software Performance Engineering[C]// IEEE Future of Software Engineering (FOSE'07). 2007:171-187

[25] Woodside M, Franks G. Tutorial Introduction to Layered Modeling of Software Performance[OL]. http://www.sce.carleton.ca/rads/lqns/lqn-documentation

[26] Marsan M A, Balbo G, Conte G. Modelling with generalized stochastic Petri nets[J]. ACM SIGMETRISS Performance Evaluation Review, 1998, 26(2)

[27] Krogmann K, Kuperberg M, Reussner R. Using Genetic Search for Reverse Engineering of Parametric Behavior Models for Performance Prediction[J]. IEEE Transaction on Software Engineering, 2010, 36

[28] Woodside M, Li J, Chinneck J, et al. Performance Model Driven QoS Guarantees and Optimization in Clouds [C]// ACM/IEEE ICSE Workshop on Cloud Computing. Vancouver, May 2009

(上接第 146 页)

[11] Li H J, Wang L H, Zhao S, et al. Research on Lossless Compression Algorithms of Low Resolution Palmprint Images[J]. Research Journal of Applied Sciences, Engineering and Technology, 2012, 4(14):2072-2081

[12] Zhang J S, Wang X M, Zhang W F. Chaotic keyed hash function based on feedforward-feedback nonlinear digital filter[J]. Physics Letters A, 2007, 362(5/6):439-448

[13] Weinberger M, Seroussi G, Sapiro G. Lossless image compression algorithm: Principles and standardization into JPEG-LS[J]. IEEE Transactions on Image Processing, 2000, 9(8):1309-1324

[14] http://www4.comp.polyu.edu.hk/~biometrics/

[15] Zhang D, Kong W K, You J, et al. On-line palmprint identification[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2003, 25:1041-1050

[16] Mi B, Liao X F, Chen Y. A novel chaotic encryption scheme based on arithmetic coding Chaos[J]. Solitons and Fractals, 2008, 38(5):1523-1531

[17] Li H J, Zhang J S. A secure and efficient entropy coding based on arithmetic coding[J]. Communications in Nonlinear Science and Numerical Simulations, 2009, 14(12):4304-4318

[18] Baptista M S. Cryptography with chaos[J]. Physics Letters A, 1998, 40(1/2):50-54