第 58 卷 第 7 期 2009 年 7 月
1000-3290/2009/58(07)/4477-08

物 理 学 报
ACTA PHYSICA SINICA

Vol.58,No.7,July,2009

一种基于 TD-ERCS 的生物特征密钥产生算法*

周 庆† 胡 月 廖晓峰

(重庆大学计算机学院,重庆 400030)

(2008 年 9 月 20 日收到;2008 年 10 月 23 日收到修改稿)

提出了一种新的思路,即由生物特征直接生成系统所需的密钥,从而降低了系统的成本和复杂性,并方便用户操作.为了保证该方法的安全性,采用改进后的切延迟椭圆反射腔混沌系统(TD-ERCS)对生物特征进行处理.实验结果表明该算法具有极高的运算速度,良好的生物特征敏感性、抗碰撞性和随机性,可实际用于生物特征密码系统.

关键词:混沌,切延迟椭圆反射腔系统,生物特征密码系统,密钥产生算法

PACC:0545,0540

1. 引 言

生物特征(biometric characteristics)指个体独有的生理或行为模式,如人的指纹、虹膜、视网膜、脸型、声音、键盘敲击模式和手写签名等.目前,生物特征识别技术已广泛应用于各种身份识别系统中,如机要部门的虹膜和视网膜识别系统、银行的手写签名识别系统以及车辆指纹识别系统.与传统的口令识别系统相比,生物特征识别系统具有毋须记忆、便于携带、难窃取、难仿造和难抵赖的优点.但是生物特征识别技术不能实现加密功能,这一功能目前只能通过密码技术来实现[1].为了综合生物特征识别技术与密码技术各自的优势,研究者们提出了生物特征密码技术[2].生物特征密码技术对生物特征和密钥进行计算,将计算结果存储在计算机或智能卡中.攻击者即使窃取了计算结果,如果不能提供正确的生物特征,也无法获得密钥.另一方面,只要用户的生物特征与标准特征非常相似,系统就可恢复出正确的密钥,进而实现加密功能.

生物特征密码技术很好地解决了密钥记忆和密钥安全之间的矛盾,用户毋须记忆复杂的密钥就可实现加密功能.但该技术仍然需要外部的真随机数或伪随机数产生器来生成密钥,增加了系统的复杂性.此外,真随机数产生器会增加系统的成本,而伪随机数产生器则达不到密钥所要求的安全性.

为了解决这一问题,本文提出了一种新的思路,即直接利用生物特征产生密钥,从而降低系统的复杂性,方便系统的实施和用户的操作.用户可在系统注册或身份识别的同时实现密钥的生成和更换.然而用户的生物特征具有很强的相似性,为了使产生的密钥满足随机性要求,必须对生物特征进行处理.由于混沌系统天然的敏感性和随机性等特点,本文采用 TD-ERCS 混沌系统对生物特征进行处理.实验结果表明,本文算法产生的密钥对用户的生物特征具有敏感性,同时也通过抗碰撞性和 NIST 随机性测试.

2. 生物特征密码系统与 TD-ERCS

2.1. 生物特征密码系统

生物特征密码系统对生物特征和密钥进行计算,其计算结果存储在计算机或智能卡上.攻击者即使窃取了计算结果,由于不能提供正确的生物特征,也无法恢复出密钥.生物特征密码技术的困难在于即使是合法用户,其生物特征在每次检测时也会有细微的差别.而传统密码学技术则具有"雪崩效应",输入最微小的变化也会导致输出的巨大差异.因此在设计生物特征密码系统时,必须对传统的密码学

* 国家自然科学基金(批准号:60573047,60703035 和 60873201)和重庆市自然科学基金(批准号:2009BA2024)资助的课题.

† E-mail:zhou@cqu.edu.cn

技术进行修改.

目前,生物特征密码技术得到广泛研究[2].1998年,Davida等人提出了一种基于虹膜特征的密码系统[3].密钥即为虹膜特征转换成的2048比特的数T,然后为T附加K比特的纠错位C,并计算$s=\mathrm{sig}(\mathrm{Hash}(T\parallel C))$,其中$s$表示对$T$和$C$连接后的Hash值的数字签名,最后将$s$与$C$存储在计算机中.提取时系统根据纠错位$C$对用户输入的虹膜特征$T_1$进行纠错,得到$T_2$,如果$\mathrm{sig}(\mathrm{Hash}(T_2\parallel C))$与存储的$s$相等,则通过认证,并将$T$作为加密密钥.该方法运算速度很快,但由于用户每次检测时T_1的变化较大,该方案并不具备实用性.Monrose等人提出一种基于键盘敲击模式的密码系统[4].由于用户口令通常较短,无法满足安全需求,Monrose等人建议首先根据Shamir的秘密共享方案[1]生成指令表,该指令表说明如何由用户的键盘敲击特征和弱口令生成一个强口令.用户在登陆时根据指令表的操作生成强口令.由于键盘敲击特征只有15个比特,该方案对口令安全性的增强很有限.Juels和Wattenberg提出了一个"模糊承诺"(fuzzy commitment)的生物特征密码系统[5].首先对密钥k进行纠错编码得到C,将用户的生物特征转换成向量X,计算$d=C-X$,在计算机中存储d和$h=\mathrm{Hash}(k)$.在提取密钥时,根据用户提供的生物特征X_1和d计算$C_1=X_1+d$,对C_1进行纠错解码得k_1,若$h=\mathrm{Hash}(k_1)$则认证通过,将k_1作为加密密钥.该系统最大的缺点是要求生物特征向量X各分量必须完全有序,若某些特征在检测时出现增加、遗漏或改变顺序的情况,则无法通过认证.这对大多数生物特征检测是不现实的.

目前研究最多的生物特征密码技术是由Juels和Sudan提出的"模糊保险箱"(fuzzy vault)技术[6].用户的密钥首先被转换为多项式$p(x)$的系数,生物特征则被转换为一系列点的横坐标$(x_1,x_2,\cdots,x_n)$,多项式$p(x)$将这些横坐标映射成对应的纵坐标$(y_1,y_2,\cdots,y_n)$,从而得到平面上n个点(x_1,y_1),(x_2,y_2),$\cdots$,(x_n,y_n)的集合G.为了保护多项式的系数不被窃取,在这些点的基础上再添加足够多的噪声点集合N.最后将G和N中所有的点随机排列后存储到计算机上.提取时先将用户的生物特征转换成一系列点的横坐标,并从存储的点中找到横坐标上的点.对这些点进行多项式拟合即可恢复出$p(x)$.图1显示"模糊保险箱"的工作原理.生物特征向量的各个分量可以是无序的,因此很适合生物特征检测.该技术目前已被运用到多种生物特征中.如Clancy等人将之应用到指纹特征中[7],Freire等人提出一种基于离线签名的"模糊保险箱"方案[8].

生物特征密码技术很好地解决了密钥记忆和密钥安全之间的矛盾.人们无需记忆密钥就可实现数据加密功能.但是生物特征密码技术并未解决密钥的产生问题.通常情况下,人们可采用各种随机数产生器来生成密钥.但这种方式增加了系统的复杂性和实现成本.

2.2. 混沌Hash函数与TD-ERCS

混沌系统对初始状态和系统参数具有极高的敏感性,同时它还具有伪随机性、遍历性等特点.鉴于这些特点,混沌系统被广泛用于设计各种加密技术,包括Hash函数、图像加密算法、分组加密算法、流密码算法和公开加密算法等等.尽管混沌系统经离散化后,其性能有所退化,但在敏感性和随机性方面仍具有很好的表现,因此研究者们基于混沌系统设计了各种性能优异的Hash函数.如Yi提出了一种基于混沌帐篷映射的Hash函数[9],Xiao等人提出了一种基于分段线性混沌映射的Hash函数[10],Liu等人提出了一种基于双向耦合映像系统的Hash函数[11],Zhang等人提出的基于前向反馈非线性过滤器的Hash函数[12]等等.

2004年,盛利元等人提出了一种基于切延迟椭圆反射腔系统(TD-ERCS)的混沌加密系统.该系统模拟射线在椭圆中的运动轨迹.为了弥补离散化导致的性能退化,反射切线取前m次反射点的椭圆切线,称为切延迟.自2004年以来,该模型被深入研究.理论分析和实验结果表明,该模型具有很强的抗退化和抗差分分析的能力[13—15].此外,基于该模型设计的Hash函数与现有的各种混沌Hash函数相比,在同样满足敏感性和抗碰撞的前提下,具有更快的运算速度[16].基于TD-ERCS的Hash函数过程如下:

1)初始化密钥:设置射线的起始点横坐标x_0和角度α,切延迟m和椭圆参数μ;

2)过渡态迭代:切延迟设为1,μ保持不变,对系统进行m次迭代;

3)正常态迭代:切延迟设为m,μ由N个明文分组按正序和逆序依次确定,对系统共进行$2N$次迭代;

4)最终迭代:切延迟设为m,μ取初始值,对系

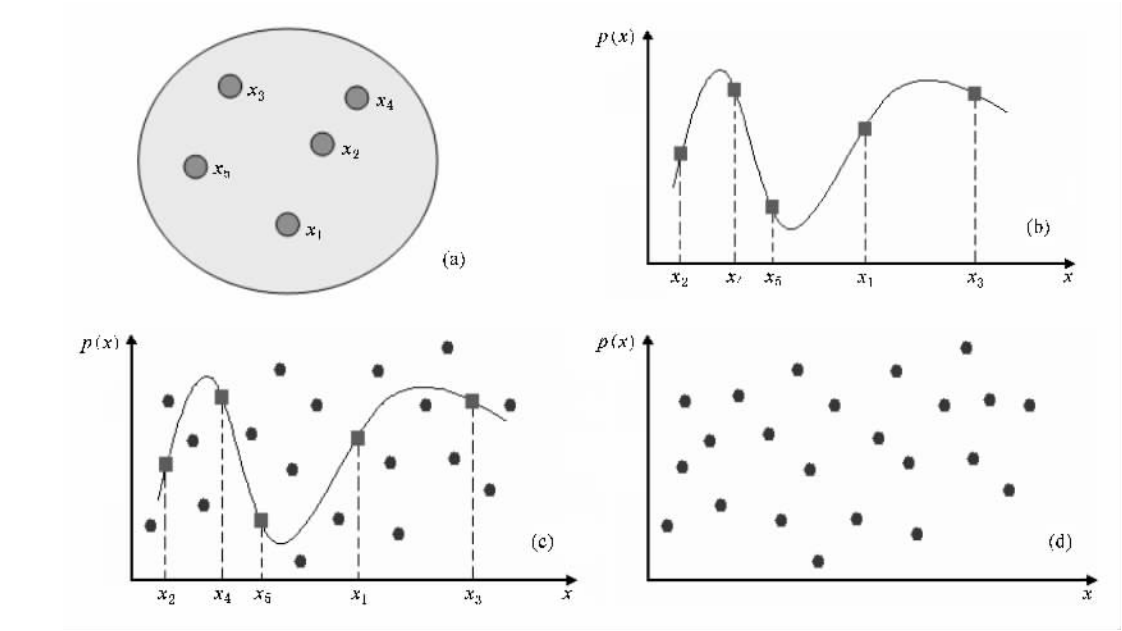

图 1　模糊保险箱'的工作原理　(a)将生物特征转换成集合 G;(b)多项式对 G 的投影;(c)在 G 中添加一些随机点;(d)最后存储的点

统作最后的 38 次迭代；

5)获得 Hash 值：从最终的 38 次迭代状态中抽取 160 比特 Hash 值.

在以上 3)4)5)步中,系统迭代由以下式决定：

$$x_n = -\frac{2k_{n-1}y_{n-1} + x_{n-1}(\mu^2 - k_{n-1}^2)}{u^2 + k_{n-1}^2}, \quad (1)$$

$$k_n = \frac{2K_n - k_{n-1} + k_{n-1}K_n^2}{1 + 2k_{n-1}K_n - K_n^2}, \quad (2)$$

其中 x_n, y_n, k_n 分别表示第 n 个反射点的横坐标、纵坐标以及反射线的斜率;K_n 表示第 n 个反射点的切线斜率,由下式计算：

$$K_n = \begin{cases} -\dfrac{x_{n-1}}{y_{n-1}}\mu^2, n < m, \\ -\dfrac{x_{n-m}}{y_{n-m}}\mu^2, n \geqslant m. \end{cases} \quad (3)$$

由于该 Hash 函数在处理每个分组时平均只进行 2 次左右的混沌迭代(其他 Hash 函数至少需要几十次混沌迭代),且每次迭代所需的乘除法运算很少,其运算速度比现有的各种 Hash 函数更快.该 Hash 函数同时也满足敏感性和抗碰撞要求(关于此 Hash 函数更详细的内容参见文献[16]).但是文献[16]提出的 Hash 函数并非为生物特征设计,为了适应生物特征处理的特点,进一步提高处理速度,需要对原算法进行改进.

3. 基于 TD-ERCS 的生物特征密钥产生算法

3.1. 产生生物特征密钥的新方法

2.1 节曾指出生物特征密码技术需要额外的随机数产生器来生成密钥,但这种方式增加了系统的复杂性和实现成本.对用户来说,他在注册特征密码的同时还需要输入其密钥,也增加了操作不便.有没有办法可以进一步简化系统呢？为此,我们提出了一种新的思路,即根据人的生物特征直接产生密钥.采用这种方法,生物特征密码系统不再需要外部的随机数产生器,用户在注册时只需要输入其生物特征.图 2(a)和(b)显示了现有生物特征密码系统与新方法在用户注册时的流程对比.

虽然从直观上看新方法简单明了,但是这种方法在技术上却存在一个难点.众所周知,同一用户的生物特征往往具有很大的相似性,这也是生物特征识别技术得以成功的基础.然而根据安全性要求,密钥的产生又必须具有随机性.因此,解决生物特征的相似性与密钥的随机性之间的矛盾是生物特征密钥产生算法的关键问题.这就要求在设计生物特征处理函数时必须有足够的科学依据.

从另一角度考虑,虽然同一用户的生物特征很相

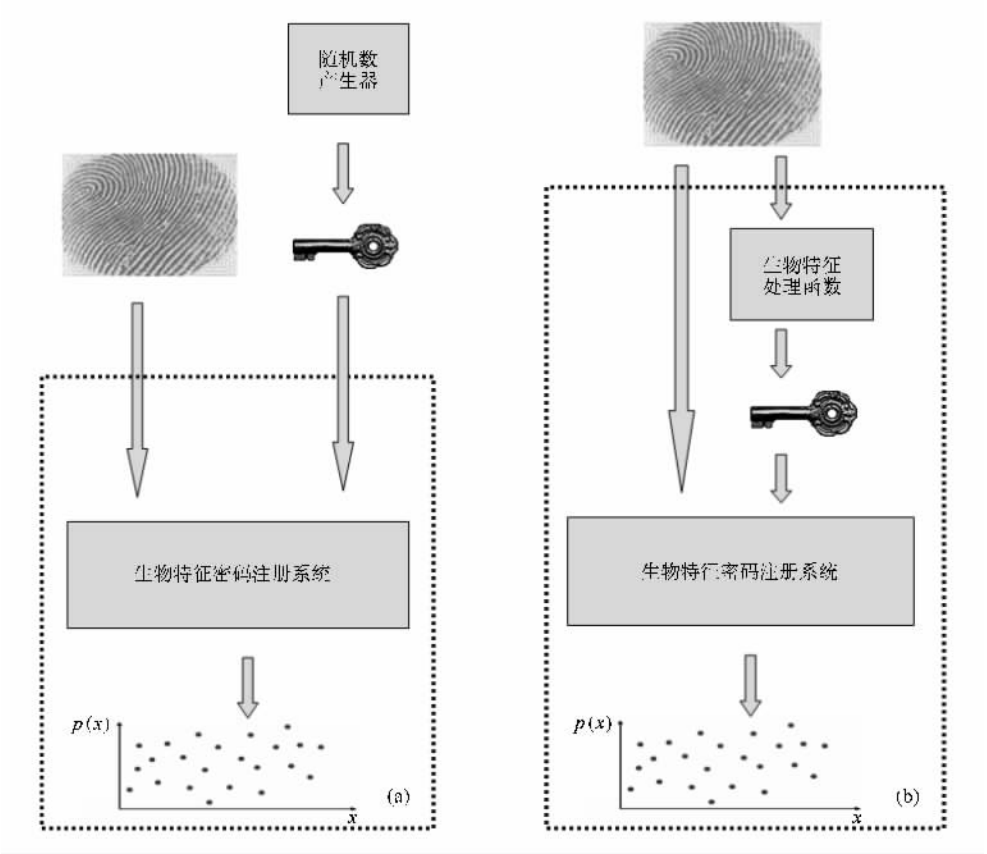

图 2 生物特征密码注册流程 (a)现有生物特征密码系统的注册流程;(b)新方法的注册流程

似,但在每次检测中,生物特征完全相等的概率极小.也就是说,选用的处理函数应满足以下两个要求:

1)敏感性:即使输入出现最微小的变化,输出的密钥也有显著变化,最好满足"严格雪崩效应".

2)随机性:产生的密钥能通过各种统计测试,以说明密钥中不存在特定模式.

毋庸置疑,混沌系统恰好具有这两项特性.

3.2. 一种基于 TD-ERCS 的生物特征处理函数

由图 2(b)可以看出,生物特征处理函数是新方法中最关键的部分.由于混沌系统天然的敏感性和随机性,非常适合用于设计生物特征处理函数.根据已有的理论分析和实验结果,TD-ERCS 系统表现出了很强的密码学特性,且运算速度很高,可作为生物特征处理函数的主要部件.但是,为了适应生物特征的特点,进一步提高生物特征处理速度,需要对文献[16]中的算法进行改进.

假设生物特征用一系列位于区间[0,1]的浮点数(c_1,c_2,…,c_L)表示,则本文设计的生物特征处理函数的步骤如下:

1)初始化密钥:设置射线的起始点横坐标 x_0 和角度 α,切延迟 m 和椭圆参数 μ;

2)正常态迭代:设置切线斜率 K_n 等于生物特征 c_i(生物特征按先顺序再逆序输入),对系统进行 $2L$ 次迭代;

3)最终迭代:切延迟设为 m,对系统作最后的 38 次迭代;

4)生成密钥:抽取最后 32 次迭代中的横坐标 x_n 的最低 8 比特,组成 256 比特的密钥.

与文献[16]中的算法相比,本文主要作了四项改动:

1)省去了过渡态迭代过程.由于正常态迭代未采用切延迟迭代方式,故可省去过渡态迭代,从而提高处理速度.

2)省去了二进制转换成浮点数的过程.在原算法第 3 步正常态迭代中有两处需要将二进制转换成浮点数.首先是正序输入时,各明文分组需要转换成浮点数;其次在逆序输入时,明文分组的各比特需重新排列再转换成浮点数.由于二进制转换成浮点数会占用大量的运算时间,改进算法可成倍地提高处

理速度.

3)在整个处理过程中椭圆参数 μ 保持不变，K_n 的值则等于输入的生物特征 c_i.改进的算法减少了(1)式和(3)式中的乘除法运算，从而提高了处理速度.事实上，原算法通过明文来确定椭圆参数 μ，进而确定 K_n，与改进算法由生物特征直接确定 K_n，在原理上是相通的.

4)生成的 Hash 值/密钥由 160 位增加到 256 位.这是因为目前许多加密标准都支持长度为 256 比特的密钥.

两相比较，改进的算法更适合用于生物特征处理；从结果来看，它不但简化了概念和操作，同时也提高了运算速度(表 1 对改进前后算法以及 SHA-1 Hash 函数的运算速度作了对比).但改进算法在敏感性、抗碰撞性和随机性方面的表现仍需进一步的检测，该实验结果在第 4 节中给出.

4. 实验结果

我们把第 3 节中提出的算法应用到在线签名这一生物特征中，并检测算法的敏感性、抗碰撞性能和密钥的随机性.

签名认证是现实生活中最常见的身份认证方法之一.签名认证分为在线和离线签名认证两种.与离线签名只记录签名的轮廓不同，在线签名还可记录签名的时间顺序、速度甚至用力的大小和方向，从而为认证提供更丰富的信息.实验采用著名的在线签名资料库 SVC2004[17].该资料库提供了 40 名用户共 800 个签名(在 SVC 资料库中，每个用户对应 20 个真实签名和 20 个伪造的签名.在本实验中，只采用真实签名，共计 800 个).各手写签名抽样点的横坐标被线性映射到[0,1]的浮点数(最小值映射为 0，最大值映射为 1)，作为生物特征序列.图 3 显示了第 1 个用户前两个签名的生物特征序列曲线.从图中可以看到，同一用户的生物特征序列曲线非常相似，但也有细微的差别.如果设计适当的处理函数，可以利用这种微小的差别产生安全的密钥.

为了检测改进算法的性能，我们设计了几个实验.我们同时也采用文献[16]中的原算法将生物特征转换成密钥，以便于性能对比.在各实验中，除非明确说明，两个算法的密钥(x_0，α，m，μ)设为(0.5，0.2，4，0.5).

表 1　改进算法与原算法产生密钥的平均时间对比

	原算法	改进算法	SHA-1
产生一次密钥的时间/ms	31.8	10.5	26.16
密钥长度	160	256	160
生成 1 比特密钥的时间/ms	0.1988	0.0410	0.1635

表 1 列出了两个算法对 800 个签名进行处理时，生成一个密钥的平均时间对比(程序在同一计算机上用 matlab 实现，CPU 为 1.5G 的 Intel Celeron).由表 1 可知改进算法的生成 1 比特密钥的速度大约是

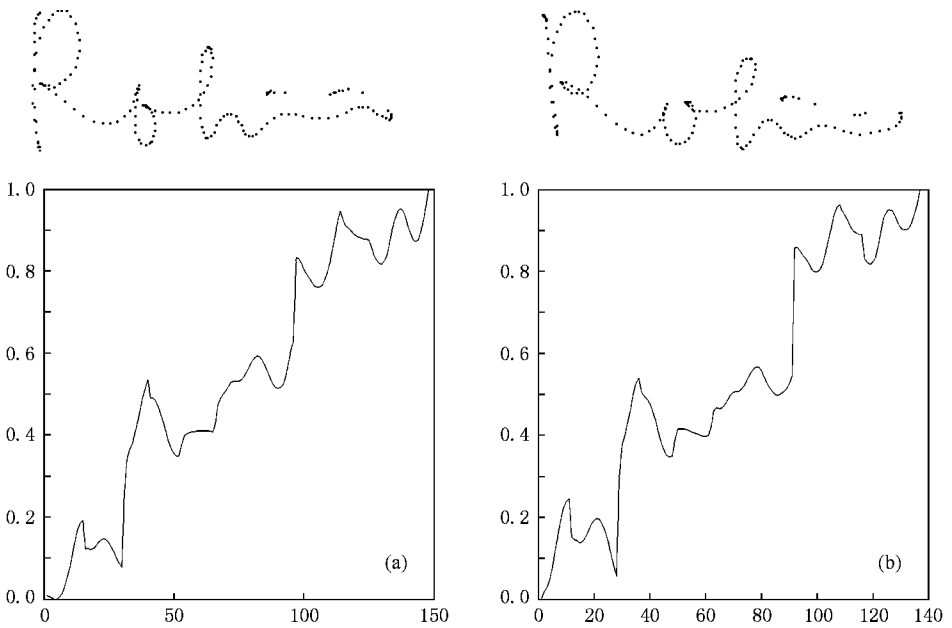

图 3　用户 1 的两次签名及生物特征序列曲线　(a)第 1 次签名；(b)第 2 次签名

原算法的 5 倍.进一步的实验表明,在原算法中二进制与浮点数之间的转换占用了大量的运算时间,平均为 17.6 ms.

我们同时还将改进的算法与国际上通行的 Hash 函数 SHA-1 的运算速度进行了对比.从表 1 可以看出改进后的算法比 SHA-1 更快.这是因为 SHA-1 每处理一个 512 比特的分组(相当于 10 个抽样点产生的比特数)需要 80 次迭代;而在 TD-ERCS 中处理一个抽样点,只需 1 次迭代.因此在处理相同的抽样点个数时,TD-ERCS 的迭代次数平均只有 SHA-1 的 1/8 左右.尽管 SHA-1 每次迭代的速度比 TD-ERCS 快,其产生一个密钥的总体时间仍为改进算法的 2.5 倍.若再考虑两个算法产生的比特数差异(SHA-1 为 160 比特,改进算法为 256 比特),则 SHA-1 产生 1 比特的速度约为 TD-ERCS 改进方案的 1/4.

4.1. 敏感性测试

敏感性测试检查当生物特征发生微小变化时,密钥的改变情况.理想情况下,密钥应有一半比特发生变化,即"严格雪崩效应".我们改变生物特征向量最后一个分量的最后一比特,并检查密钥比特数的改变情况.表 2 列出了两种算法对 800 个在线签名所做的实验中,密钥比特变化率的平均值和标准差.在理想情况下,比特变化率的平均值等于 0.5,而标准差越小则说明算法的稳定性越高.表 2 说明,改进算法虽然在比特变化率的平均值上比原算法稍差,但也非常接近理论值,且算法稳定性比原算法更高.

表 2 特征向量发生微小变化时,密钥比特变化率的平均值和标准差

	比特变化率的平均值	比特变化率的标准差
原算法/%	49.99	4.08
改进算法/%	50.14	3.17

4.2. 碰撞分析

碰撞分析实验改变生物特征向量最后一个分量的最后一比特,并检查两个密文中对应字节相等的个数.表 3 列出了 800 个在线签名中,恰有 $i(i=0,1,2,\cdots)$ 个密钥字节相等签名的占 800 个签名的百分比.表 3 说明,改进算法的实验结果非常接近理论值,具有良好的抗碰撞性能.

另一个测试抗碰撞性能的方法是检查当生物特征发生微小变化时,两个密钥在数值上的距离.理想情况下,平均每个字节之间的距离等于 65535/768(约为 85.3320).表 4 列出了改变生物特征向量最后一个分量的最后一比特前后,密钥之间的距离.从平均距离来看,改进算法非常接近理想值.从最大距离来看,改进算法的值更小,说明其稳定性更高.

表 3 特征向量发生微小变化时,密钥中字节相等个数的分布

密钥中字节相等的个数	0	1	2	≥3
理论值/%	88.23	11.07	0.67	0.03
实际值/%	88.501	0.00	1.50	0

表 4 特征向量发生微小变化时,密钥之间的距离

	最大距离/字节	最小距离/字节	平均距离/字节
原算法	128.6	47.6	84.89
改进算法	122.2	47.5	85.0561

4.3. 随机性测试

为了满足安全性要求,使用生物特征产生的密钥应是随机的.我们采用了美国 NIST 机构建议的随机数测试软件[18]对生成的密钥序列进行严格的测试.NIST 随机数测试软件共包含 15 种测试(原为 16 种,自版本 1.7 后,Lempel-Ziv 复杂性测试不再使用).每个序列每种测试的结果用 $p\_value(0\leqslant p\_value\leqslant 1)$ 表示,若 p_value 大于一预先设定的阈值 T,则说明该序列通过了相应的测试.为了保证实验结果的科学性,同一种测试需重复进行 m 次(每次测试不同的序列),并由此计算出该测试的通过率.只有当 15 种测试的通过率均大于(4)式定义的值时,才认为该算法生成的密钥序列是随机的:

$$p_T = (1-T) - 3\sqrt{\frac{T(1-T)}{m}}. \tag{4}$$

在本实验中,$T=0.01$,$m=800$,$P_T=0.9794$.

在 NIST 随机数测试软件中定义的 15 种测试中,FT,FBT,RT,ST,AET 以及 CST 要求每个序列的长度大于 100 比特,其他测试则需要更多的比特.特别是 PTMT,LZCT,RET,REVT 测试要求每个序列的比特数至少为 1,000,000.由于整个实验需要 800 个序列,因此实验所需的数据量很大.对于 FT,FBT,RT,ST,AET,LROBT 以及 CST 测试,每次产生的密钥即作为一个序列,长度为 160 比特;对于其他测试,通过改变系统参数 μ 来产生足够多的测试数据量(μ 从 0.5 取到 0.56249,间隔为 10^{-5},共 6250 个不同的值),使每个签名产生的序列长度为 1,000,000 比特.

ATMT，ST，CST，RET 及 REVT 等测试（在表 5 中用 * 标记）包含多个子测试，其通过率以各子测试中的最小通过率表示．此外，由于改变了序列的默认长度，某些测试的参数需要重新设置，表 5 中列出了这些测试的参数．表 6 列出了该算法在 15 种测试中的通过率．从表 6 可以看出，所有测试的通过率均大于 0.9794，因此本文提出的算法产生的密钥满足随机性要求．

表 5　需要修改参数的测试

测试名称	ST	AET	FBT	LROBT
参数	Block = 5	Block = 3	Block = 32	$M = 8$（需修改源程序）

5. 结　论

生物特征密码技术很好地解决了密钥记忆和密钥安全之间的矛盾．人们只需提供个人的生物特征就可实现数据的加密，而毋须记忆冗长的密钥．生物特征密码系统需要额外的随机数产生器，这增加了系统实现的成本和复杂性．本文的创新工作主要包括三个方面：

1．提出了一种新的方案，即利用个人的生物特征直接产生密钥，从而简化了系统的实施，方便了用户操作．

2．提出利用混沌系统对生物特征进行处理的思路，从而消除同一用户产生的生物特征的相似性．

3．对 TD-ERCS 混沌 Hash 函数进行改进，以适应生物特征处理的特点．通过对800例个人签名的实验，表明改进的 Hash 函数具有令人满意的敏感性、抗碰撞性和随机性；在速度方面，改进算法不仅比原来的 TD-ERCS 混沌 Hash 函数快，也超过了国际上通行的 SHA-1 算法．综合各方面的性能，本文提出的改进算法可用于实际系统．

利用个人的生物特征为密码系统产生密钥是一种新的思路，同时也涉及到生物、信息和物理等多个学科．虽然在本文的实验中只采用了在线签名这一生物特征，但该算法的原理同样适用于其他生物特征．在下一步的工作中，我们将对更多的生物特征进行考查和测试．

表 6　密钥序列的随机性检测结果

测试名称	通过率
FT	0.9850
FBT	0.9912
CST*	0.9850
RT	0.9850
LROBT	0.9950
AET	0.9862
ST*	0.9862
RBMRT	0.9938
DFTT	0.9875
ATMT*	0.9938
PTMT	0.9850
MUST	0.9912
RET*	0.9894
REVT*	0.9863
LCT	0.9900

[1] Schneier B 1994 *Applied Cryptography* (New York: John Wiley & Sons)

[2] Davida G, Frankel Y, Matt B 1998 *IEEE Symp. Privacy and Security*

[3] Monrose F, Reiter M, Wetzel S 1999 *The Sixth ACM Conf. Computer and Communications Security*

[4] Uludag U, Pankanti S, Prabhakar S, Jain A 2004 *Proceedings of the IEEE* **92** 948

[5] Juels A, Wattenberg M 1999 *The sixth ACM Conf. Computer and Communications Security*

[6] Juels A, Sudan M, A fuzzy vault scheme 2002 *IEEE Int. Symp. Information Theory*

[7] Clancy T, Kiyavash N, Lin D 2003 *ACM Multimedia, Biometrics Methods and Applications Workshop*

[8] Manuel R, Fierrez J, Marcos M, Javier O 2007 *The ninth International Conference on Document Analysis and Recognition*

[9] Yi X 2005 *IEEE Trans. Circuits Syst.* Ⅱ **52** 354

[10] Xiao D, Liao X F, Deng S J 2005 *Chaos, Solitons & Fractals* **24** 65

[11] Liu J D, Yu Y M 2007 *Acta Phys. Sin.* **56** 1297 (in Chinese) [刘建东、余有明 2007 物理学报 **56** 1297]

[12] Zhang J S, Wang X, Zhang W 2007 *Phys. Lett.* A **362** 439

[13] Sheng L Y, Sun K H, Li C B 2004 *Acta Phys. Sin.* **53** 2871 (in Chinese) [盛利元、孙克辉、李传兵 2007 物理学报 **53** 2871]

[14] Sheng L Y, Cao L L, Sun K H, Wen J 2005 *Acta Phys. Sin.* **54** 4031 (in Chinese) [盛利元、曹莉凌、孙克辉、闻　姜 2005 物理学报 **54** 4031]

[15] Sheng L Y, Wen J, Cao L L, Xiao Y Y 2007 *Acta Phys. Sin.* **56** 78 (in Chinese) [盛利元、闻　姜、曹莉凌、肖燕予 2007 物理学报 **56** 78]

[16] Sheng L Y, Li G Q, Li Z W 2006 *Acta Phys. Sin.* **55** 5700 (in Chinese) [盛利元、李更强、李志炜 2006 物理学报 **55** 5700]
[17] Yeung D, Chang H, Xiong Y *et al* 2004 *First International Signature Verification Competition*
[18] NIST Special Publication 800-22, 2001 http://csrc.nist.gov/rng/rng2.html

A key generation algorithm for biometric cryptosystems based on TD-ERCS*

Zhou Qing† Hu Yue Liao Xiao-Feng
(*College of Computer, Chongqing University, Chongqing* 400030, *China*)
(Received 20 September 2008; revised manuscript received 23 October 2008)

Abstract

Biometric cryptosystems are widely studied recently, which bind a cryptographic key with the biometric characteristic of a user in such a way that the key cannot be recovered without a successful biometric authentication. By now, the key is generated from extra random number generators, which makes the system more complex. A novel method is proposed, which generates the key from biometric characteristics directly, and makes the biometric cryptosystems much cheaper, simpler and more convenient. To make the keys secure enough, the TD-ERCS is adopted and revised in the proposed algorithm. Experiments show that the algorithm is sensitive to biometric characteristics, free of collision, and the generated keys seem also random. It is believed that such a algorithm can be practically used for various biometric cryptosystems.

Keywords: chaos, TD-ERCS, biometric cryptosystem, key generation
PACC: 0545, 0540

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60573047, 60703035 and 60873201) and the Natural Science Foundation of Changqing, China (Grant No. 2009BA2024).

† E-mail: tzhou@cqu.edu.cn