DOI: 10.19650/j.cnki.cjsi.J1905560

局部置乱结合双随机相位编码的双虹膜身份模板保护方法*

刘笑楠,张文云,高艳娜
(沈阳工业大学信息科学与工程学院 沈阳 110870)

摘 要:针对基于不可逆变换的虹膜模板保护在进行虹膜识别时面临特征模板泄露的问题,提出一种结合局部置乱和双随机相位编码双虹膜身份模板保护方法。该方法首先采用 log-Gabor 变换提取用户虹膜特征,然后设定置乱次数以及变换矩阵参数,利用 Arnold 变换对虹膜特征矩阵进行无重叠分块置乱,对原始特征进行第一重加密保护。再在分数傅里叶变换域应用双随机相位编码方法构建加密特征向量,采用用户设定掩膜 $\boldsymbol{M}_1$ 和同一用户的另一只虹膜图像掩膜 $\boldsymbol{M}_2$ 对置乱矩阵进行第二重加密保护。最后依据汉明距离对加密模板进行匹配识别。为验证算法性能,采用 CASIA-IrisV3-Interval、MMU-V1 以及 CASIA-IrisV4-Lamp 虹膜图库的图像进行测试。结果表明,该方法识别正确率能够达到 98.73%,可生成模板的总数量为 52^2,并且恢复原始数据需要尝试 $314^{52\times624}\times42$ 次,能够满足生物特征模板保护的不可逆性、可撤销性和不可链接性标准。

关键词:虹膜模板保护;局部置乱;Arnold 变换;双随机相位编码
中图分类号:TP391.41 TH786 **文献标识码**:A **国家标准学科分类代码**:510.40

Double iris identity template protection method combining partial scrambling and double random phase coding

Liu Xiaonan, Zhang Wenyun, Gao Yanna
(*School of Information Science and Engineering, Shenyang University of Technology, Shenyang 110870, China*)

Abstract: Aiming at the problem that iris template protection based on irreversible transformation is faced with feature template leakage in iris recognition, this thesis proposes a method of double iris identity template protection method combining partial scrambling and double random phase encoding. Firstly, the iris feature of the user is extracted with log-Gabor transform, and then the scrambling times and transformation matrix parameters are set. The non-overlapping block scrambling of iris feature matrix is carried out using Arnold transformation, and the first encryption protection of the original features is carried out. Then, double random phase coding method is used to construct the encryption feature vector in fractional Fourier transform domain. The user set mask $\boldsymbol{M}_1$ and the same user's other iris image mask $\boldsymbol{M}_2$ are adopted to perform the second encryption protection of the scrambling matrix. Finally, the Hamming distance is used to match and identify the encryption template. In order to verify the performance of the algorithm, the iris images in the CASIA-IrisV3-Interval, MMU-V1 and CASIA-IrisV4-Lamp iris libraries were used for testing. The results show that with the proposed method the recognition accuracy can reach 98.73%, the total number of the generated templates is 52^2, and the recovery of the original data needs $314^{52\times624}\times42$ attempts, which can meet the criteria of irreversibility, revocability and unlinkability of biometric template protection.

Keywords: iris template protection; partial scrambling; Arnold transform; double random phase encoding

0 引 言

近年来,生物特征识别技术成为研究热点,并在实际中得到广泛应用。但是,该技术中用于识别身份的生物特征模板有可能被盗取从而泄露隐私,威胁用户的隐私安全[1]。并且生物特征是不可再生的,一旦被窃取,用户损失无法挽回。针对该问题已提出多种模板保护方法,

收稿日期:2019-09-01 Received Date: 2019-09-01
*基金项目:辽宁省自然科学基金(20180520022)项目资助

但是攻击者仍可通过窃取存储在数据库中的已加密模板进行逆向变换或采用不法手段获取原始模板,从而窃取用户的信息。因此寻找一种保护最原始特征数据的方法是保证生物特征识别技术实用化的关键问题。

虹膜是被广泛应用的生物特征之一,目前已提出的虹膜特征模板保护方法可分为虹膜生物特征加密技术和可撤销虹膜识别技术两大类[2]。虹膜生物特征加密技术是将生物特征信息和密码学相结合,这类方法包括模糊保险库[3]、模糊承诺[4-5]和模糊提取器[6]等。这类方法可能出现隐私泄漏和交叉匹配等安全问题[7]。可撤销虹膜生物特征识别技术通过某种变换函数转换生成特征模板,从而对虹膜模板起到保护作用。该类方法可分为生物哈希法和不可逆变换法两大类[8]。其中,生物哈希法主要是采用引入外部因素的方法加密模板,利用不同的密钥生成不同的模板,从而实现可撤销性。例如文献[9]中引入不同"令牌"与模板相结合,并且通过修改"令牌"实现可撤销性。Bringer 等[10]则将模板与一个标记的伪随机数相结合实现模板保护。然而,生物哈希法一旦被攻击者攻破引入的数据,模板信息将被获取。不可逆变换法利用不可逆变换函数无法恢复出原始数据的特性实现数据保护。Rathgeb 等[11]首先将不可逆变换应用于图像领域,并引入可撤销的概念。此类方法包括随机投影和稀疏表示法[12-13]、随机移位和异或(exclusive OR,XOR)操作变换法[14-16]、Bloom 滤波器方法[11]等。由于随机移位和 XOR 操作变换法会减少可用于识别的信息量,后续许多学者对该类方法提出改进,如采用 Bloom 滤波器方法,文献[17-18]分析了基于 Bloom 滤波器的特征保护方法的不可链接性,并且引入了采用数据不均匀性的不可逆性分析。Dong 等[19]提出了一种基于遗传算法的相似性攻击框架,针对生物哈希法和 Bloom 滤波器方法进行实验。Dwivedi[20]等提出一种基于随机查表映射的可撤销的虹膜模板生成方法。上述方法几乎都满足不可逆变换这条特性,并且都是在基于二值模板的基础上采取保护措施,这类方法一旦攻击者获取变换函数的相关参数,并且采用多重放攻击以及解方程即可得到原始模板,导致信息泄露等问题。2018 年 Randa 等[21]提出了一种基于双随机相位编码的可撤销虹膜识别方法。该方法是一种编码加密方法,从获取的特征数据直接通过双随机编码得到加密的二值模板,但是通过逆推法以及解方程也可能获得原始模板。

综上所述,基于不可逆变换的虹膜模板保护方法已取得了较好的结果。但是,现有方法针对二值特征编码进行变换,尚缺乏对虹膜图像原始特征数据的保护。为了解决这一问题,本文提出一种基于局部置乱结合双随机相位编码的虹膜模板保护方法。尝试将原始虹膜特征信息作为保护对象,根据人体具有两只虹膜的特点,首先将用户的左虹膜图像的特征矩阵采用 Arnold 分块置乱,以获得"虹膜特征码(IrisCode)"的第一重保护,然后从同一用户的右虹膜图像中提取 IrisCode 作为双随机相位编码的第二相位掩膜,通过结合双随机相位编码加密的方法生成新的模板,以达到双重保护的作用。实验结果表明,该方法能够在满足虹膜识别正确率的同时保护用户的生物特征信息。

1 算法基本原理

1.1 Arnold 变换

Arnold 变换是一种基于空间域的像素置乱算法,该算法是由 Arnold[22]在研究环面上的同态时首次提出。该变换的本质操作是拉伸和折叠,从而改变图像内各像素点的空间位置,破坏像素点之间的关联以降低像素之间的相关性。Arnold 变换的原理如下:

设输入图像为 $\boldsymbol{I}(x,y)$,其中 $x \in [0,1,\cdots,N-1]$,$y \in [0,1,\cdots,N-1]$。设 (x_k,y_k) 为像素置乱后的坐标,则 (x,y) 与 (x_k,y_k) 映射关系如式(1)所示。

$$\begin{pmatrix} x_k \\ y_k \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod(N) \tag{1}$$

式中:$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 为变换矩阵;$a,b,c,d \in Z_+$,并且满足 $|ad-bc|>0$;$mod(\cdot)$ 为取模运算,为了将变换后的像素坐标折回到特征图谱中,一般地,在变换矩阵中 $a=1$,$b>0$,$d=1+bc$。则式(1)可表示为式(2)所示的方程组形式。

$$\begin{cases} x_k = (x+by)\,mod(N) \\ y_k = \{cx+(1+bc)y\}\,mod(N) \end{cases} \tag{2}$$

通过 Arnold 变换,图像像素点坐标实现了空间域位置的改变。为了提高运算效率,可将虹膜图像进行分块并行 Arnold 变换实现整幅图像的像素置乱。

1.2 分数傅里叶变换域的双随机相位编码加密

分数傅里叶变换(fractional fourier transform,FRFT)是传统傅里叶变换在分数阶次上的延伸,即引入 Wigner 空间中的角度参数 α,且该参数在 $p\pi/2$ 的任意角度旋转,参数 p 表示变换的阶数。随着阶数的变化 FRFT 展示出信号从时域逐步变化到频域的所有变换特征[21]。在本文中,FRFT 用于增强安全性。

双随机相位编码(double random phase encoding,DRPE)是一种光学加密技术,通过在信号空域和频域上各加一个互不相关的随机相位掩膜,DRPE 将原图像编码成固定序列的模板,从而实现对输入信号的加密,获得平稳的伪白噪声作为密文[23]。本文的 DRPE 图像加密方法如下:设 $\boldsymbol{I}(x,y)$ 为待编码图像,$\boldsymbol{Q}(x,y)$ 为所得编码

图像,首先,用一个相位掩膜 $e^{[2\pi i M_1(x,y)]}$ 与图像做积,其中 $\boldsymbol{M}_1(x,y)$ 为用户设定密钥;然后经过 *FRFT*,再将该结果与 $\boldsymbol{h}(x,y)$ 做卷积,其中 $\boldsymbol{h}(x,y)$ 是另一相位掩膜 $\boldsymbol{M}_2(u,v)$ 的傅里叶逆变换,即 $\hat{\boldsymbol{h}}(u,v)=e^{[2\pi i M_2(u,v)]}$。则图像编码计算方法如式(3)所示。

$$\boldsymbol{Q}(x,y)=F^{p}\{\boldsymbol{I}(x,y)e^{[2\pi i M_1(x,y)]}\}*h(x,y) \tag{3}$$

式中:F 表示分数傅里叶变换;p 表示阶次;"$*$"表示卷积。

2　虹膜模板保护方法

2.1　算法流程

本文提出的虹膜模板保护方法利用同一用户的左右两只虹膜信息对虹膜特征信息进行双重加密保护。首先,通过 Arnold 算法将一只虹膜图像特征矩阵置乱,对虹膜图像原始数据进行第一重保护;然后,将另一只虹膜的特征信息作为掩膜运算密钥,在分数傅里叶域中应用双随机相位编码系统,获得最终模板,实现第二重模板保护。算法具体运算过程如下:

首先,对预处理后所得的归一化虹膜图像进行 log-Gabor 变换,获得虹膜图像特征矩阵 $\boldsymbol{I}(x,y)=\boldsymbol{A}=\begin{bmatrix} a_{11} & \cdots & a_{1N} \\ \vdots & \ddots & \vdots \\ a_{M1} & \cdots & a_{MN} \end{bmatrix}_{M\times N}$,其中 a_{ij} 表示点 (x,y) 处的特征值。

其次,对该矩阵进行无重叠分块,将矩阵 $\boldsymbol{A}$ 分成若干个 $M\times M$ 的子矩阵,得 $\boldsymbol{A}=[\boldsymbol{A}_{11},\cdots,\boldsymbol{A}_{1n}]$,其中 $\boldsymbol{A}_{11},\cdots,\boldsymbol{A}_{1n}$ 表示各分块特征子矩阵。分块算法不但能够实现快速降维以利于并行运算,并且可以提高置乱后所得模板对轻微旋转和平移的鲁棒性。

然后,根据式(1)对每一块子矩阵进行置乱变换,再对块数置乱。设置乱次数为 k,则置乱后的矩阵可记作 $\boldsymbol{I}'(x_k,y_k)=\boldsymbol{A}'_k=[\boldsymbol{A}'_{11},\cdots,\boldsymbol{A}'_{1n}]$。由于 Arnold 本身具有周期性,置乱一定的次数之后会恢复到原始数据,如表 1 所示,并且不同的置乱次数将影响虹膜识别的准确率。根据本文图像的归一化尺寸,可选择不高于 42 的置乱次数。再通过对置乱次数与识别正确率关系的统计分析如图 1 所示,当置乱次数为 38 时,识别率达到最高,为 98.73%。因此,本文算法的置乱次数设定为 38 次。

表 1　不同尺寸图像的变换周期

Table 1　Transformation period T of the images with different sizes

$M\times N$	10×20	20×60	41×418	52×624	61×317	118×146
T	60	12	41	42	61	219

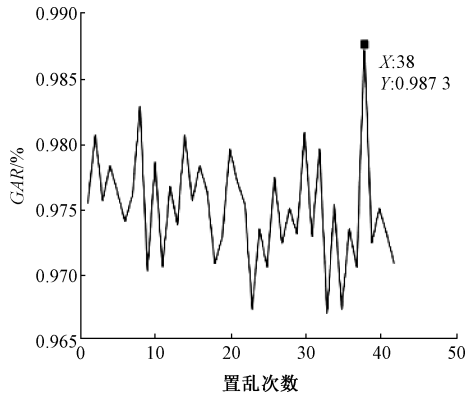


图 1　不同置乱次数对应的识别率

Fig. 1　Recognition rate corresponding to different scrambling times

最后,将用户设定的第一相位掩膜 $\boldsymbol{M}_1(x,y)$ 与上述置乱结果相乘,再对其进行 *FRFT*,将结果与第二相位掩膜 $\boldsymbol{M}_2(u,v)$(即同一用户的右虹膜特征矢量)乘积,再进行 *FRFT* 得到最终的加密模板。整个加密过程的数学表达式如式(4) ~ (6)所示。

$$\boldsymbol{G}^{e}(u,v)=F^{p_1}[\boldsymbol{I}'(x_k,y_k)e^{[2\pi i M_1(x,y)]}] \tag{4}$$

$$\boldsymbol{H}^{e}(u,v)=\boldsymbol{G}^{e}(u,v)e^{[2\pi i M_2(u,v)]} \tag{5}$$

$$\boldsymbol{Q}(x,y)=(F^{p_2})^{-1}[\boldsymbol{H}^{e}(u,v)] \tag{6}$$

式中:上角标"e"表示加密过程中所得函数;F^{p_1} 表示 p_1 阶 FRFT,F^{p_2} 表示 p_2 阶 FRFT,$p_1=p_2=0.67$。

2.2　算法安全性分析

根据生物特征信息保护标准,安全的虹膜特征模板保护方法应满足不可逆性、可撤销性以及不可链接性[24]。下面将针对上述 3 个要求对本文算法的安全性进行理论分析。

1)不可逆性

不可逆性要求从原始数据到安全模板的转换是不可逆的。本文算法的不可逆性可从整个算法的逆变换过程说明当攻击者获取 $\boldsymbol{Q}(x,y)$ 而不知道 $\boldsymbol{M}_2$ 以及矩阵变换参数 b 和 c 的情况下将不能恢复出原始数据 $\boldsymbol{I}(x,y)$。具体分析如下:

当进行逆变换时,首先需将加密后的特征模板 $\boldsymbol{Q}(x,y)$ 的共轭即 $Q^{*}(x,y)$ 进行 p_2 阶的 FRFT,所得结果乘以 $e^{[2\pi i M_2(u,v)]}$,再进行 p_1 阶的 FRFT。然后,将所得结果进行 Arnold 置乱逆变换,再通过确定 Arnold 置乱次数以及求得恢复矩阵 $\boldsymbol{B}$ 得到 $\boldsymbol{I}(x,y)$ 原始数据。

文献[25]指出,在进行双随机相位编码的逆过程时,若 $\boldsymbol{M}_1(x,y)$ 已知,要想恢复出原始数据 $\boldsymbol{I}(x,y)$,就必须构造第二相位掩膜 $\boldsymbol{M}_2(u,v)$。假设攻击者通过不法手段获得相应的第二相位掩膜,得到置乱后的数据

$\boldsymbol{I}'(x,y)$,但是要恢复原始模板,仍需要求出准确的置乱次数 k 以及恢复矩阵 $\boldsymbol{B}$。依据 Arnold 置乱变换的定义可得其反变换如式(7)所示。

$$\begin{bmatrix} x \\ y \end{bmatrix} = \boldsymbol{T}_k \begin{bmatrix} x_k \\ y_k \end{bmatrix} mod(N) \tag{7}$$

求解(7)式可得:

$$\boldsymbol{T}_k = (\boldsymbol{B}^k)^{-1} mod(N) \tag{8}$$

由于尚缺乏上述逆变换的求解方法,所以只能采用穷举法获得原始数据 $\boldsymbol{I}(x,y)$。由本文实验分析可知,利用穷举法获取原始数据的概率极小,为 $(314^{52\times624} \times 42)^{-1}$,即利用数据库中虹膜模板恢复原始的特征数据的可能性极小。因此,本文方法满足生物特征信息保护的不可逆性。

2)可撤销性

可撤销性要求受损或泄露的模板可以被撤销,并且新的模板可以重新发布。在本文方法中,当某用户的模板被盗取时,提供虹膜识别服务的服务器可以删除泄露模板,并要求用户重新提交一个模板,服务器通过改变置乱参数 b、c 以及改变第一相位掩膜 $\boldsymbol{M}_1(x,y)$ 密钥,可以重新获取新的模板。具体地说,b 和 c 为变换矩阵的参数,文献[26]已证明变换参数的改变不会影响置乱的效果,由式(2)可得:

$$x_{k+1} = (x_k mod N + (by_k) mod N) mod N) = (x_k mod N + (c mod N \times y_k mod N) mod N) mod N \tag{9}$$

由于 x_k 和 y_k 是密钥置乱后的位置坐标,所以 x_{k+1} 的值取决于 $b \bmod N$ 的变换,而 $b \bmod N = (b+N) \bmod N$,所以 b 的取值范围为 $b \in [1,N]$,同理 $c \in [1,N]$,针对每一个确定的 b 或 c,可生成一个新的置乱数据,即得到新的模板,新模板共有 N^2 种可能性。需要注意的是变换参数仅用于生成被盗取模板的用户生成新的模板,其他用户继续使用旧模板,不需要额外重新注册。对于模板泄露的用户,旧模板就不能再用于识别,因为其相关密钥已被更新,而且很难在旧模板和新模板之间执行匹配(这一点由不可链接性保证)。因此,本文所提出的方法满足生物特征信息保护的可撤销性要求。

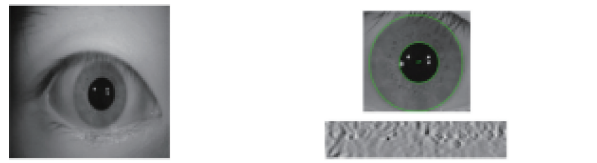
3)不可链接性

不可链接性要求存储在数据库的模板不能跨越不同的应用程序,即攻击者无法确定来自不同应用程序的两个模板是否对应于同一用户。在本文中,不可链接性要求不同的密钥 $\boldsymbol{M}_1(x,y)$ 和变换矩阵(由参数 b、c 决定)产生不同的 $\boldsymbol{I}'(x,y)$,这些 $\boldsymbol{M}_1$ 与 $\boldsymbol{I}'(x,y)$ 是由同一个人在不同应用程序中注册的虹膜数据产生的。由于 $\boldsymbol{M}_1$ 密钥是由客户端自行设定,而 $\boldsymbol{I}'(x,y)$ 是置乱的结果,即可得到不同的 $\boldsymbol{I}'(x,y)$,并且 b、c 在 $[1,N]$ 范围内的取值是随机的(只需满足式(1)要求),如果不事先知道变换矩阵的具体参数,很难判断这些生成的 $\boldsymbol{I}'(x,y)$ 是否是同一个人。因此,本文的方法满足不可链接性。

3 实验结果与分析

为了测试本文方法的各项性能,采用 CASIA-IrisV3-Interval (http://biometrics.idealtest.org/)、MMU-V1 (http://pesona.mmu.edu.my/~ccteo/) 以及 CASIA-IrisV4-Lamp (http://biometrics.idealtest.org/) 虹膜图库进行算法测试。其中 CASIA-IrisV3-Interval 包含 249 个人的虹膜图像,CASIA-IrisV4-Lamp 包含 411 个人的虹膜图像,MMU-V1 包含 46 个人的虹膜图像。

本文的虹膜识别系统包括注册和认证两个阶段。在图像预处理过程中,采用文献[27]的定位方法分割出虹膜区域,为避免睫毛以及阴影等干扰,将所得虹膜区域的下半部分进行归一化处理,获得 52×624 的归一化虹膜图像,如图 2 所示(以 CASIA-IrisV3-Interval 为例)。



(a) 原图像 (a) The original image (b) 虹膜分割及归一化结果 (b)The results of iris segmentation and normalization

图 2 虹膜图像以及预处理结果

Fig. 2 Iris image and its pre-processing results

注册阶段采用每个人的左虹膜特征进行无重叠分块并通过 Arnold 变换置乱,其中,Arnold 变换矩阵是由 b 和 c 构成。用户自行设定第一掩膜,并将同一个人的右虹膜特征矢量作为双随机相位编码的第二掩膜。在验证阶段,应用程序从用户获得虹膜图像以及加密的密钥,通过相同模式得到最终模板并使用汉明距离将其与数据库中的数据进行匹配得到身份识别结果。

3.1 算法识别性能测试结果分析

为了说明本文算法的识别性能,本文通过正确识别率(genuine acceptance rate,GAR)、等错误率(equal error rate,EER)、受试者工作特征曲线(receiver operating characteristic,ROC)下与坐标轴围成的面积(area under curve,AUC)、真阳性率(true positive rate,TPR)等指标将本文方法与其他方法进行比较。其中精准率(positive predictive values,PPV)和阴性预测值(negative predictive values,NPV)为文献[21]中提出的针对模板保护识别方法的匹配性能评估指标。其定义如式(10)和(11)所示。

$$PPV = \frac{TP}{TP + FP} \tag{10}$$

$$NPV = \frac{TN}{TN + FN} \tag{11}$$

式中:*TP* 为真阳性的数量;*FP* 为假阳性的数量;*TN* 为真阴性的数量;*FN* 为假阴性的数量。

可判定性度量 d' 用来区分真实和假冒分布[21],其定义如式(12)所示。

$$d' = \frac{|\mu_i - \mu_g|}{\sqrt{\frac{\sigma_i^2 + \sigma_g^2}{2}}} \tag{12}$$

式中:μ_i 和 μ_g 为假冒者和真实者的均方值;σ_i 和 σ_g 为假冒者和真实者的方差。d' 越大,表明冒名顶替者与真实分布之间的距离越大,则识别性能越好。以上这些性能指标的值是通过真实的和冒名顶替者的得分来评估的。这里采用类间匹配得分评估冒名顶替者得分,将每个用户的虹膜模板与其他用户的模板匹配;采用类内匹配得分评估真实者得分,通过每个用户的虹膜与同一用户的其他虹膜模板相匹配,得到类内的匹配总次数。

分别对 3 种图库进行 100 次随机注册和测试样本选取,所得各项性能指标的平均值如表 2 所示。

表 2　不同算法的识别性能比较

Table 2　Comparison of the recognition performance for different algorithms

性能指标	文献[28]	文献[20]	文献[21]	本文算法
TPR/%	99.50	98.26	98.84	99.13
NPV/%	99.51	98.23	98.83	99.12
PPV/%	99.01	97.98	99.35	99.48
EER/%	0.83	2.001	1.07	1.03
GAR/%	99.25	98.02	98.59	98.73
AUC/%	99.84	98.57	99.03	99.29
d'	4.31	2.708	5.18	5.64

测试结果表明,本文方法由于加入置乱变换使得识别性能相较于文献[28]中未进行加密保护的识别算法识别正确率略低,但其 *PPV* 和 d' 更高,说明本文方法的模板保护性能更好。与文献[20]和[21]中的两种算法相比,本文方法的 TPR、NPV、PPV 以及 GAR、AUC 有明显的提高,说明本文算法性能优于其他两种可撤销虹膜模板保护方法,并且 d' 的值也高出这两种方法,说明冒名顶替者与真实分布之间的距离较大,识别性能更好。因此,本文算法在保证身份模板保护性能的前提下在识别准确率方面仍具有优势。

为了说明本文算法对不同虹膜图像的适用性,将 CASIA-IrisV3-Interval,CASIA-IrisV4-Lamp 以及 MMU-V1 3 种图库的测试结果进行统计,如表 3 所示。其中,基本算法指未加密的虹膜识别方法。结果表明,本文方法在 3 种图库中均能够取得较好的识别效果,并且未置乱加密时的识别性能与本文算法相差无几,说明本文算法在对模板保护的同时能够兼顾识别性能,具有适用性以及有效性。

表 3　不同数据库所对应的 *GAR* 和 *EER*

Table 3　The *GAR* and *EER* corresponding to different databases　%

数据库	基本算法		本文算法	
	GAR	EER	GAR	EER
CASIA-IrisV3-Inrerval	99.25	0.83	98.73	1.03
CASIA-IrisV4-Lamp	84.06	3.80	83.35	4.06
MMU-V1	79.38	4.75	78.65	4.91

3.2　算法安全性能测试结果分析

1)不可逆性

由 2.2 节可知,由于密钥均匀分布在[0,2π]上,并且有效性在小数点后两位,当攻击者在以上情况下攻击加密系统时,首先需构建第二相位密钥矩阵,已知图像大小为 52×624,则利用穷举法得到正确的第二相位密钥矩阵的期望次数是 $314^{52\times624}$。假设通过穷举方法得到正确的第二相位密钥,通过置乱算法得到置乱后的数据 $\boldsymbol{I}'(x,y)$,然而要将 $\boldsymbol{I}'(x,y)$ 恢复至 $\boldsymbol{I}(x,y)$,仍受到置乱次数和变换矩阵的制约。在攻击者不知道置乱次数 k 的前提下,通过盲攻击的方法得到最佳的置乱次数 k,由表 1 得到大小为 52 × 624 的特征矩阵的变换周期为 42,攻击者将尝试 42 次才能成功得到最佳置乱次数 k。

然后,攻击者还需要求出恢复矩阵 $\boldsymbol{T}_k$,恢复矩阵 $\boldsymbol{T}_k$ 会涉及矩阵乘方的问题,对于较大的置乱次数 k,通用计算设备很难计算出正确结果。例如,在本文算法中 $N = 52$,并且当 $k = 38$ 时,矩阵 $\boldsymbol{B}^k$ 为:

$$\boldsymbol{B}^{38} = \begin{bmatrix} 2\,289\,602\,033\,422\,790 & 3\,972\,560\,211\,997\,022 \\ 3\,972\,560\,211\,997\,022 & 6\,892\,566\,658\,997\,073 \end{bmatrix}$$

$$(\boldsymbol{B}^k)^{-1} mod 52 = \begin{bmatrix} 7 & 14 \\ 14 & 20 \end{bmatrix}$$

然而正确的恢复矩阵是把上述矩阵元素 20 改为 21,虽然仅仅差一个数,但是最后得到恢复原始数据 $\boldsymbol{I}(x,y)$ 完全不正确。由此总的尝试次数 $314^{52\times624}\times42$,显然很难恢复出原始数据。

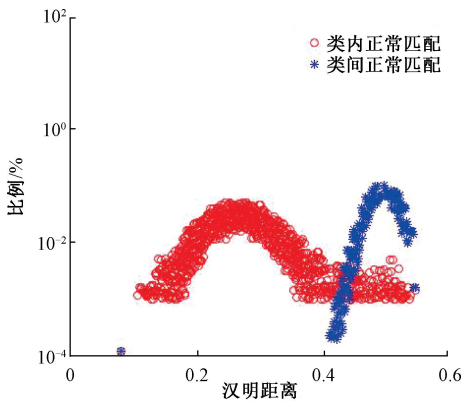
2)可撤销性

由 2.2 节可知,变换矩阵的参数 b、c 可用于生成不同的模板。由于本文算法令每一块置乱矩阵大小为 52 × 52,由式(9)可知 b 的取值范围 $b \in [1,52]$,同理参数 c 的取值范围 $c \in [1,52]$,因此针对每一个用户在改变变换矩阵参数的情况下可生成的模板总数量为 52^2,能够满足算法的可撤销性需求。

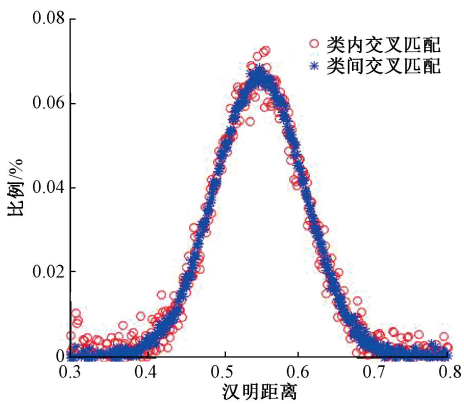
3)不可链接性

为了测试算法的不可链接性,本文采用两组不同的

密钥和参数对算法的识别结果进行测试分析。首先在一组测试中,将所有的用户虹膜由特定的 $\boldsymbol{M}_1$ 与特定的矩阵参数 b 和 c 进行加密保护,得到特征模板 $t_1,t_2\cdots t_N$;在另一组测试中,采用 $\boldsymbol{M}'_1$ 与矩阵参数 b' 和 c',获得特征模板 $t'_1,t'_2\cdots t'_N$。然后,比较同一虹膜在两组加密参数下所得的特征模板,即比较 t_1 与 t'_1,t_2 与 t'_2,$\cdots$,t_N 与 t'_N,计算各距离并且记录,进行类内的交叉匹配;再比较不同虹膜在两组测试中生成的模板即 t_1 与 $t'_2\cdots t'_N$,t_2 与 $t'_3\cdots t'_N$,$\cdots$,t'_{N-1} 与 t'_N。计算各距离且记录,进行类间的交叉匹配。测试样本包含 100 幅虹膜图像,实验结果如图 3 所示,其中,x 轴表示汉明距离,y 轴表示每个相同距离值对应的匹配次数占总次数的比例,图 3(a)所示表示在一个应用程序中类内和类间匹配分布,从图 3 可以看出两者的分布有很大的差别,类内匹配的距离 $HD<0.44$,类间匹配的距离 $HD>0.41$,并且两者相互重叠的区域很小,表明本文算法具有较好的识别性能。图 3(b)所示表示交叉匹配的分布,可以看出类内和类间的匹配几乎重叠,根据匹配结果无法确定两个模板是否来自同一个用户,即一个应用程序的模板无法链接到另外的应用程序进行同一用户的识别。因此本文方法满足不可链接性。



(a) 正常匹配
(a) Normal matching



(b) 交叉匹配
(b) Crossing matching

图 3 类内和类间的距离分布

Fig. 3 The intraclass and interclass distance distribution

4 结 论

本文针对身份模板泄露问题提出一种虹膜模板双重保护的方法,该方法首先将原始模板置乱,以达到混淆攻击者视野的目的,再通过基于 FRFT 域的双随机相位编码系统得到加密模板。对特征模板起到了双重保护的作用,攻击者若采用穷举法需要尝试 $314^{52\times624}\times42$ 次才能得到真实模板,可能性微乎其微,并且实验结果可证明本文算法满足不可逆性,可撤销性以及不可链接性,满足生物特征信息保护标准。另外,测试结果表明,该算法在保护模板的条件下识别正确率能够达到 98.73%,在实现模板保护的同时亦可满足识别性能的需求。

参考文献

[1] JAIN A K, NANDAKUMAR K, NAGAR A. Biometric template security[J]. Eurasip Journal on Advances in Signal Processing, 2008(1):1-17.

[2] RATHGEB C, UHI A. A survey on biometric cryptosystems and cancelable biometrics[J]. EURASIP Journal on Information Security, 2011(1):3-28.

[3] ARI J, MADHU S. A fuzzy vault scheme[J]. Designs, Codes and Cryptography, 2006, 38(2):237-257.

[4] IGNATENKO T, WILLEMS F M J. Information leakage in fuzzy commitment schemes[J]. IEEE Transactions on Information Forensics and Security, 2010, 2(5):337-348.

[5] KELKBOOM E J C, BREEBAART J, KEVENAAR T A M, et al. Preventing the decodability attack based cross-matching in a fuzzy commitment scheme[J]. IEEE Transactions on Information Forensics & Security, 2011, 6(1):107-121.

[6] MARINA B, ALIASGARI M. Analysis of reusability of secure sketches and fuzzy extractors[J]. IEEE Transactions on Information Forensics & Security, 2013, 8(9):1433-1445.

[7] 毋立芳, 马玉琨, 周鹏, 等. 生物特征模板保护综述[J]. 仪器仪表学报, 2016, 37(11):2407-2420.
WU L F, MA Y K, ZHOU P, et al. Summary of biometric template protection[J]. Chinese Journal of Scientific Instrument, 2016, 37(11):2407-2420.

[8] MEETEI T C, BEGUM S A. A variant of cancelable iris biometric based on biohash[C]. IEEE International Conference on Signal and Information Processing, 2016:1-5.

[9] UMER S, DHARA B C, CHANDA B. A novel cancelable iris recognition system based on feature learning techniques[J]. Information Sciences, 2017, 406(9): 102-118.

[10] BRINGER J, MOREL C, RATHGEB C. Security analysis of bloom filter-based iris biometric template protection[C]. IEEE International Conference on

Biometrics, 2015:527-534.
[11] RATHGEB C, BREITINGER F, BUSCH C. Alignment-free cancelable iris biometric templates based on adaptive bloom filters [C]. IEEE International Conference on Biometrics, 2013:1-8.
[12] PILLAI J K, PATEL V M, CHELLAPPA R, et al. Secure and robust iris recognition using random projections and sparse representations [J]. IEEE Transactions on Pattern Analysis & Machine Intelligence, 2011, 33(9):1877-1893.
[13] KAUR H, KHANNA P. Gaussian random projection based non-invertible cancelable biometric templates[J]. Procedia Computer Science, 2015, 54(8):661-670.
[14] PILLAI J K, PATEL V M, CHELLAPPA R, et al. Sectored random projections for cancelable iris biometrics[C]. IEEE International Conference on Acoustics Speech & Signal Processing, 2010: 1838-1841.
[15] TAREK M, OUDA O, HAMZA T. Pre-image resistant cancelable biometrics scheme using bidirectional memory model [J]. International Journal of Network Security, 2017,19(4): 498-506.
[16] ZHAO D, FANG S, XIANG J, et al. Iris template protection based on local ranking [J]. Security and Communication Networks, 2018:1-9.
[17] HERMANS J, MENNINK B, PEETERS R. When a bloom filter is a doom filter: Security assessment of a novel iris biometric template protection system[C]. 2014 International Conference of the Biometrics Special Interest Group (BIOSIG), 2014: 75-86.
[18] BRINGER J, MOREL C, RATHGEB C. Security analysis and improvement of some biometric protected templates based on Bloom filters[J]. Image and Vision Computing, 2017, 100(58): 239-253.
[19] DONG X, JIN Z, JIN A T B. A genetic algorithm enabled similarity-based attack on cancellable biometrics[C]. 10th IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2019:1-7.
[20] DWIVEDI R, DEY S, SINGH R, et al. A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping[J]. Computers & Security, 2017, 65(C): 373-386.
[21] RANDA F, AMIN M, EI-SAMIE F E. A double random phase encoding approach for cancelable iris recognition[J]. Optical and Quantum Electronics, 2018, 50(8):326.
[22] ARNOLD V I, AVCZ A. Ergodic problems in classical mechanics[M]. New York: Benjamin, 1968.
[23] REFREGIER P, JAVIDI B. Optical image encryption using input plane and Fourier plane random encoding[J]. Optics Implementation of Information Processing. International Society for Optics Photonics, 1995,2565(6):62-68.
[24] VENUGOPALAN S, SAVVIDES M. How to generate spoofed irises from an iris code template [J]. IEEE Transactions on Information Forensics & Security, 2011, 6(2): 385-395.
[25] 陈翼翔, 汪小刚. 一种基于迭代振幅-相位恢复算法和非线性双随机相位编码的图像加密方法[J]. 光学学报, 2014, 34(8):119-124.
CHEN Y X, WANG X G. An image encryption method based on iterative amplitude-phase recovery algorithm and nonlinear double random phase encoding [J]. Acta Optics Sinica, 2014, 34(8):119-124.
[26] 李永逵, 冯乔生, 周粉, 等. 二维 Arnold 变换及非等长图像置乱变换[J]. 计算机工程与设计, 2009, 30(13):3133-3135.
LI Y K, FRNG Q SH, ZHOU F, et al. Two-dimensional Arnold transform and non-isometric image scrambling transform[J]. Computer Engineering and Design, 2009, 30(13):3133-3135.
[27] 刘笑楠,杨争威,张海珊. 基于混合测地线区域曲线演化的虹膜定位方法[J]. 电子测量与仪器学报,2018, 32 (10):79-86.
LIU X N, YANG ZH W, ZHANG H SH. Iris Location Method Based on the Evolution of Hybrid Geodesic Area Curves [J]. Journal of Electronic Measurement and Instrument, 2018,32(10):79-86.
[28] SOLIMAN N F, MOHAMED E, MAGDI F, et al. Efficient iris localization and recognition [J]. Optik, 2017,140(7): 469-475.

作者简介

刘笑楠(通信作者),2001 年和 2004 年于吉林大学分别获得学士和硕士学位,2014 年于沈阳工业大学获得博士学位。现为沈阳工业大学讲师,主要研究方向为图像处理及模式识别。
E-mail: april05_liu@126.com

Liu Xiaonan (Corresponding author) received her B. Sc. and M. Sc. degrees both from Jilin University in 2001 and 2004, respectively, received her Ph. D. degrees from Shenyang University of Technology in 2014. Now, she is a lecturer in Shenyang University of Technology. Her main research interests include image processing and pattern recognition.

张文云,2017 年于沈阳工业大学获得学士学位,现为沈阳工业大学硕士研究生,主要研究方向为图像处理及模式识别。
E-mail:xiaoyun_1013@163.com

Zhang Wenyun received her B. Sc. degree from Shenyang University of Technology in 2017. Now, she is an M. Sc. candidate in Shenyang University of Technology. Her main research interests include image processing and pattern recognition.