基于模糊循环随机映射的人脸生物特征加密算法

吴懿晨 方昱春 谭 盈
(上海大学计算机工程与科学学院 上海 200444)

摘 要 随着生物特征识别技术的广泛应用,其安全性方面的缺陷也逐渐暴露出来。密码技术与生物特征识别技术相结合的生物特征加密技术,就是为了弥补生物特征识别在安全方面的不足而产生的。在研究已有人脸生物特征识别技术的基础上,提出一种兼具安全性及容错能力的人脸生物特征加密算法:模糊循环随机映射(Fuzzy Cyclic Random Mapping,FCRM)。在每次循环中,加密模型使用前一次循环的密钥作为随机种子生成映射矩阵,对用户的人脸特征进行映射,形成一个循环的随机映射过程。加密过程中,还使用了容错技术来减少合法用户人脸图像和特征的随机噪声对识别率的影响,而循环的映射过程能够在不减少认证准确率的前提下,阻止非法用户通过认证。

关键词 人脸识别,生物特征加密,生物特征哈希
中图法分类号 TP391.4 **文献标识码** A

Face-hashing Algorithm Based on Fuzzy Cyclic Random Mapping

WU Yi-chen FANG Yu-chun TAN Ying
(School of Computer Engineering and Science, Shanghai University, Shanghai 200444, China)

Abstract With the broad application of various biometric technologies, their deficiencies on safety are gradually exposed. The biometric encryption technology, as the combination of biometric recognition and cryptography technology, was proposed to ensure the safe usage of biometrics. Based on our previous researches on face biometrics, we proposed a face-hashing algorithm, i. e. Fuzzy Cyclic Random Mapping(FCRM), which considers both the security and the fault tolerance. In each cycle, the encryption model utilizes the key of the previous cycle as a random seed to generate a mapping matrix and makes random mapping of the face features. Thus the proposed algorithm forms a cyclic random mapping process. We also adopted the fault-tolerant technology in the proposed algorithm to reduce the impact of random noise existing in the face images of the genuine users, while the cyclic mapping process can simultaneously prevent the imposter to authenticate the system without reducing the accuracy.

Keywords Face recognition, Biometric encryption, Biometric hashing

1 引言

近几年来,生物特征识别技术已经从研究阶段转向应用阶段,并逐渐显示出巨大的市场潜力。但是随着应用的深入,生物特征识别技术本身的一些缺陷也逐渐暴露出来,最主要的就是生物特征所涉及到的个人隐私以及由此而带来的安全性问题。生物特征是人所固有且无法更改的,一旦服务器中保存的特征信息被盗,就会带来严重的安全问题。如果生物特征识别技术要大规模应用,那它就需要具备足够的安全和保密性。将生物特征识别技术与密码技术相结合的生物特征加密技术可以在一定程度上解决上述问题。

生物特征加密(Biometric Encryption)或称生物特征哈希(Biometric Hashing),是通过使用密码算法保护用户生物特征不被窃取的一种技术。该技术将密钥和用户的生物特征绑定并以密文方式保存,系统中并不保存用户的生物特征信息,所以不易被攻击者获得。当用户登录系统时,提供的生物特征信息如果与注册时提供的样本足够接近,它就能够生成相同的密钥。因此,其安全性与便捷性比传统的口令认证更高。该技术的关键是采用适当的技术保证生物特征信息和密钥的安全性。

1999年,由美国RSA实验室的Juel等人[1]基于编码理论的思想提出的模糊委任机制(Fuzzy Commitment Scheme,FCS)将编码理论与密码算法结合在一起,并使用容错技术来抵御密码中随机噪声的影响,生成一个稳定的加密密钥。在该方案中,加密分为注册和认证两部分。注册时,首先提取二进制表示的生物特征,将其与一个带有纠错码的随机密钥绑定,作为模板保存在系统服务器中。在认证阶段,提取认证用户的生物特征,通过模板计算释放出密钥,如果两次提取的生

到稿日期:2011-06-17 返修日期:2011-09-29 本文受国家自然科学基金(60605012),上海市自然科学基金(08ZR1408200),上海市重点学科建设项目(J50103),模式识别国家重点实验室开放课题资助。
吴懿晨(1982—),男,硕士生,主要研究领域为生物特征加密,E-mail:wuyichen1982@hotmail.com;方昱春(1975—),女,博士,副研究员,主要研究领域为生物特征识别、模式识别、机器学习和图像处理等;谭 盈(1988—),男,硕士生,主要研究领域为人脸识别、模式识别和图像处理。

物特征足够相似，那么密钥中的错误可以用纠错码来改正。但 Juel 并没有给出应用于具体生物特征的实现及实验数据。付波等人[2]结合 FCS 方案给出了具体的实验结果，但样本数量较少，结果不具代表性。文献[3,4]在人脸特征提取阶段使用了特征融合技术，该技术将两种不同的人脸特征融合成为一个人脸向量。实验结果表明，当认证人脸相同时，能够得到非常接近的特征向量。张祥德等人[5]使用神经网络替代海明码纠错，能达到 FRR=7.5%，FAR=2.46%的效果。而 Juel 本人针对 FCS 要求有序向量的缺点，使用 RS 码替代海明码进行纠错[6]。但上述算法的问题是它们都要求认证时提取多张图像作为样本，降低了算法的实用性。另一方面，虽然成功重构密钥的比率很高，但它们都可能接受非法用户认证，从而降低了安全性。

随机多空间量化（Random Multispace Quantization，RMQ）[7]使用一种可重现的变换将人脸特征映射到随机空间，并在映射后的空间中进行密钥提取。该算法除了需要提供生物特征，还需要一个密钥作为随机映射的种子，该密钥可以保存在用户令牌中或由用户输入。注册时，使用密钥作为随机种子生成一组伪随机映射矩阵。通过随机映射矩阵将 N 维人脸特征映射到 P 维空间中（$P<N$）。最后用一个阈值对结果进行离散化处理，生成一个二进制的人脸哈希值。在验证时，采用同样的方法处理用户样本，比较结果与原哈希值之间的海明距离。通过改变密钥就可以生成不同模板。根据 Teoh 的实验报告[7]，当令牌和用户特征都为真时，RMQ 可以获得非常高的识别率，并且错误率也能控制在非常低的程度。陈娜娜[8]使用局部二元模式（Local Binary Patterns，LBP）提取用户的人脸特征信息，然后通过 RMQ 实现了一种人脸特征加密算法，并将其应用到加密系统中，其识别率可以达到 99.6%，错误率为 0.68%。不过，该算法也存在缺点，即 RMQ 的安全性是建立在令牌或密钥安全性的基础上的[10]。如果攻击者得到用户令牌，那么他即使没有用户的人脸特征，仍然有相当大的可能性通过认证。

本文针对现有人脸加密算法在提取时需要多张用户照片的实用性缺陷及非法用户有可能通过验证的安全性缺陷，提出了模糊循环随机映射算法。本算法的目的是在只提取一张用户人脸图片的前提下，以牺牲少量识别率为代价达到是够的安全强度来防止非法用户通过认证。

2 模糊循环随机映射算法

本文在研究已有生物特征加密技术的基础上，将 RMQ 使用的随机映射与 FCS 使用的密钥保存和纠错技术相结合，设计出一种针对人脸图像的人脸生物特征加密算法：模糊循环随机映射算法（Fuzzy Cyclic Random Mapping，FCRM）。在每次循环中，使用上一循环的密钥作为随机种子生成映射矩阵，对用户的人脸特征进行映射，形成一个循环的随机映射过程。模糊循环随机映射算法如图 1 所示。

FCRM 具体过程分为注册和认证两部分。注册过程中，使用上一循环生成的密钥作为随机映射的随机种子，将用户的人脸图像特征通过随机映射降维与离散化后，得到一组特征哈希值。然后随机生成一个加入纠错码的密钥与该哈希值绑定，并将每一轮循环产生的绑定结果与密钥散列值作为模板保存在服务器或用户令牌中。认证过程则与上述过程相反，使用上一循环提取的特征哈希值从模板中释放出密钥进行随机映射，如果最终释放的密钥散列值与模板中保存的完全相同，则认证通过。

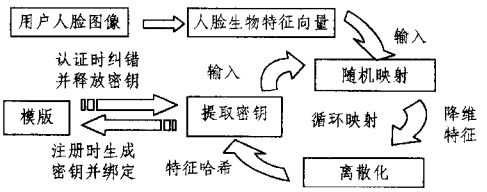

图 1 模糊循环随机映射算法

FCRM 的核心过程为循环随机映射。它利用循环随机映射过程中产生的雪崩效应来提高算法的安全性。雪崩效应是指明文或密钥的少量变化会导致结果密文的完全不同，它是加密算法中经常使用的一种技术。在本算法中，如果某一循环提取的密钥不同，则在下一循环中，会产生一个误差极大的特征哈希值。通过多次进行循环映射，可以有效防止与合法用户人脸图像特征非常接近的非法图像通过认证。

作为生物特征加密安全性的一个重要指标，密钥与生物特征的保存是一个非常关键的问题。如果服务器模板中保存明文的人脸特征值，一旦服务器遭到入侵，用户的生物特征不再可用，但生物特征对于用户来说又是不可更改的，所以一种可更换的、加密的保存方式，是决定一个生物特征加密技术安全性的关键技术。FCRM 使用的模板机制可以非常方便地将生物特征与一组随机密钥绑定，从而保证了用户生物特征的安全性。而认证时，如果认证用户的特征哈希值与注册时相差过大，就无法释放出相同的密钥，从而保证了模板的安全性。

为了防止用户人脸图像特征中的随机噪声对识别率的影响，在模板中引入了纠错机制，使得认证用户的特征哈希与注册用户相差在一定范围内时，能够得到正确的密钥。

2.1 生物特征提取

研究过程中发现，使用主分量分析（Principal Component Analysis，PCA）提取的人脸特征在随机映射后将产生较大的形变，识别率将会产生比较大的下滑[7,8]。这一现象与 Teoh[7] 的结论相同，这可能是由于 PCA 提取的特征中高维投影分量的过描述性造成了随机噪声的产生。

LBP 是一种有效的局部纹理特征算子，在每一个分块中，其中心像素与邻域内的采样像素灰度经过比较、离散化后，编码计算其值，以块为单位建立统计直方图。多数人脸识别算法都采用 Ojala 等[9]提出的均匀局部二值模式（Uniform LBP）算子。我们在前期研究中发现，通过融合多方向的旋转不变均匀局部二值模式（Rotation Invariant Uniform LBP，RIU-LBP）特征，可以在保证识别率的同时大大降低特征的维数[9]。因此，本文以 RIU-LBP 特征作为人脸特征向量进行了特征加密算法的研究。

2.2 随机映射

随机映射是一种非常有效的降维方法，其通用公式可表示为

$$v=\kappa\mathcal{R}\omega \tag{1}$$

随机矩阵 $\mathcal{R}\in\mathcal{R}^{p\times m}(m\leqslant p)$，$p$ 与 m 分别为映射前后特征向量维数，κ 为常量。

Johnson-Lindenstrauss(J-L)引理[7]证明了在 p 维欧式空间内的任意 n 个数据点都能够映射到一个维度为 $O(\frac{\ln(n)}{\varepsilon^2})$ 的空间内，并可以保证它们之间的距离保持在一个很小的范围内。

映射的随机性由映射矩阵产生，本文使用密钥作为随机种子进行映射，改进后的公式为

$$s_n=\{k_0,\cdots,k_{n-1}\} \tag{2}$$

$$v_n=R(s_n,m)\cdot\omega \tag{3}$$

式中，n 表示当前循环次数，符号 $\cdot$ 表示矩阵乘法，$v\in\mathcal{R}^m$ 为通过随机映射降维后的 m 维特征向量，且 m 的大小可根据实际需要变动。k_i 表示第 i 次循环产生的随机密钥，且 $0\leqslant i\leqslant n-1$，当 $i=0$ 时，$k_0=\lambda$(λ 为常量)。$Rnd(x,m)$表示随机矩阵生成函数，它以 x 为随机种子，生成一个 $p\times m$ 的映射矩阵。通过该矩阵，可以将 p 维的人脸特征映射到 m 维空间中。

式(2)表示将前 $n-1$ 次循环产生的密钥连接为一个新的向量，并以此作为种子生成随机映射矩阵。使用该矩阵对原始特征进行映射，得到第 n 次循环的降维特征 v_n。

2.3 特征离散化

因为后续处理需要在二进制空间上进行，所以需要将欧式空间上的特征向量转换到二进制空间中。本文对式(3)中的 v 进行零均值化和离散化，得到用户的生物特征哈希值 h。零均值化方法为

$$v=v-\bar{v} \tag{4}$$

式中，v 表示某次循环中产生的降维特征，$\bar{v}$ 表示 v 所有维度的数学平均。

离散化方法为

$$h_k=\begin{cases}0, & v_k\geqslant 0\\ 1, & v_k<0\end{cases} \tag{5}$$

式中，h 即为映射产生的特征哈希值，h_k 表示 h 的第 k 维数据，v_k 表示降维特征的第 k 维数据，且 $0<k\leqslant m$(m 为 v 的维数)。

2.4 注册过程中的模板生成

注册时，在每一次的循环映射过程中都会随机生成一个密钥，其作用如下：

1)作为下一次映射过程使用的随机种子运用于式(2)中。

2)通过绑定保护本次循环产生的特征哈希的安全性。绑定就是将密钥与式(4)中的特征哈希 h 相结合的过程。

3)在密钥中融入纠错码，可以减少用户人脸图像特征中的随机噪声对识别率的影响。

模板生成过程如图 2 所示。

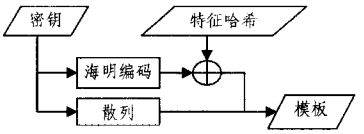

图 2 模板生成过程

密钥与特征哈希绑定后的结果将与密钥的散列值作为模板保存在服务器或者令牌中，在认证释放密钥时使用。在绑定前，需要对密钥加入纠错码。第 n 次循环的模板 T_n 生成公式可表示为

$$c_n=Encode(k_n) \tag{6}$$

$$b_n=c_n\oplus h_n \tag{7}$$

$$T_n=\{b_n,Hash(k_n)\} \tag{8}$$

式中，$Encode(x)$表示纠错编码算法，本文使用海明码纠错，c_n 为对 k_n 进行海明编码后的结果。k_n 和 h_n 分别表示第 n 次循环产生的随机密钥和生物特征哈希值，符号⊕表示二进制空间中的按位异或运算，$Hash(x)$表示散列函数，可使用比较常见的 SHA-1(Secure Hash Algorithm 1)或 MD5(Message-Digest Algorithm 5)算法。

2.5 认证过程中的密钥释放与判定

在认证阶段，随机映射认证用户的人脸图像，得到特征哈希值，并使用该值从模板中释放出密钥。由于用户表情或背景等随机噪声的影响，这个特征哈希与注册时提取的不会完全相同。为了能够保证合法用户的识别率，释放过程必须减少随机噪声对其的影响。释放公式可表示为

$$c_n'=b_n\oplus h_n' \tag{9}$$

$$k_n'=Decode(c_n') \tag{10}$$

式中，c_n'表示认证时从模板中释放的带有纠错码的密钥，h_n'表示认证过程中得到的特征哈希值，k_n'表示释放出的密钥，$Decode(x)$表示海明解码算法。

在上节的绑定过程中，k_n 在绑定前已经通过海明编码植入了纠错位。所以在认证过程中，如果认证用户与注册用户的特征哈希足够接近，通过纠错算法，可以忽略特征提取时产生的少量随机噪声，释放出与注册时相同的密钥。通过调节纠错算法的纠错率，可以控制算法认证严格程度，使其应用于不同安全级别的场合。

释放出的密钥除了作为下一轮随机映射的种子，还要用来判定认证用户是否合法。如果密钥与注册时不同，那么该用户就被认为是非法用户，认证过程终止。为了保护密钥的安全性，模板中不保存明文的密钥，而是保存密钥的散列值，通过判断认证和注册过程的密钥散列值来进行认证。可见，如果 $hash(k_n')=hash(k_n)$，那么就可以认为用户合法，继续下一轮循环映射。否则认证不会通过。密钥释的与判定如图 3 所示。

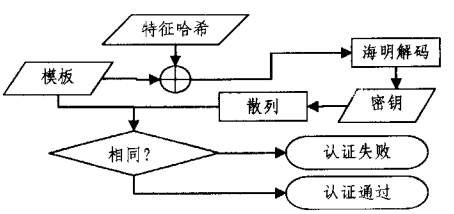

图 3 密钥释放与判定

3 实验分析

本文在 FERET(Face Recognition Technology)人脸库上测试了 FRCM 算法。FERET 库是 1993 年美国国防部高级研究项目署(Advanced Research Projects Agency)和美国陆军研究实验(Army Research Laboratory)建立的人脸数据库，用于评价人脸识别算法的性能。本文实验使用 1199 位用户的人脸图片(此为 FERET 库中拥有 2 张及以上正面人脸图像的最大用户数)，并从每位用户的正面脸像中随机抽取 2 张不同的图片分别作为注册和认证过程的图像。这些图像经过光照校正和几何配准后标准化为 160 * 140 分辨率，然后提取参数为采样密度 16、半径为 2、分块数为 8 * 7 的 RIULBP 特征，所得特征向量维数为 1009 维。通过本文的加密算法，生成长度为 128 位的密钥，因为 128 位是目前比较常用的加密算法密钥长度，认证用户可使用释放出的密钥进行各种数据的加解密操作。实验结果中的接受率为对 1199 位用户各自的 2 张图片进行注册和认证后得到的结果，则测试次数为 1199 次。认证错误率为对每一位用户与其他 1198 位用户的 2 张图片分别进行测试的结果，则测试次数为 2872804 次。

3.1 离散化和随机映射有效性验证

图 4 为 RIULBP 提取的特征向量经过零均值化与离散化后海明距离的比较，红线表示合法用户 2 张不同照片之间的海明距离，蓝线表示不同用户照片之间的海明距离。从图中可以发现，合法用户之间的海明距离总体上比非法用户与合法用户之间的相差更少，所以 RIULBP 特征经过离散化以后，仍然能够区分合法用户和非法用户之间的差别。

图 5 表示特征向量经过一次随机映射后得到的特征哈希值之间海明距离的比较。可见，原始特征在一次映射后的空间中仍能基本保持不变，从而说明随机映射是一种效果良好的降维手段。

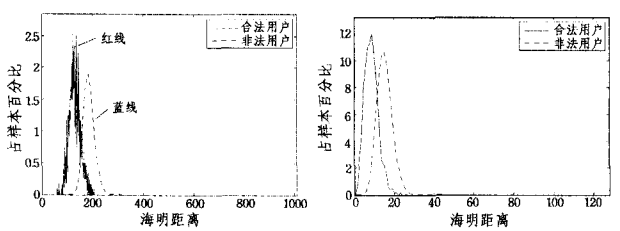

图 4 原始特征向量的海明距离

图 5 一次随机映射后的海明距离

但是从图中也可以发现，虽然合法用户和非法用户之间有一定的距离，但是仍然相当接近，单纯一次随机映射，无法将他们有效分开。对比文献[7]的 RMQ 方法，同样使用了 1 次随机映射，如果用户令牌被盗，那么攻击者即使没有用户的生物特征数据，也很可能会产生与原始特征非常接近的哈希值。

3.2 FCRM 性能分析

实验发现，纠错算法的纠错率必须控制在能够识别大部分合法用户的程度，否则识别率会受到很大的影响。由图 5 可知，合法用户曲线大致位于哈希长度的 0%～30%范围内。所以本文通过对密钥插值，使(7,4)海明码支持 33%的纠错率。

循环次数对算法的结果也有比较直接的影响。随机映射的次数越多，识别率会大幅下降。在循环次数为 3 时，接受率和错误率都可以控制在比较好的程度。图 6 为进行 3 次循环映射提取得到的特征哈希值之间海明距离的比较。对比图 5 可见，通过循环随机映射后，由于雪崩效应的形成，非法用户的特征哈希值从原来的非常接近合法用户，变为正态分布在 $\frac{m}{2}$(m 为密钥长度)附近，从而能够有效地区分出合法用户和非法用户。

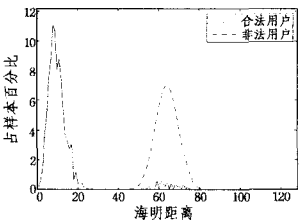

图 6 3 次循环随机映射后的海明距离

此外，密钥长度对于识别率和安全性也起到十分重要的作用。如果密钥过短，将使非法用户有机会得到与合法用户相同的密钥。反之，如果密钥过长，则会导致识别率下降。所以在实验中得到一个合理的密钥长度，也是十分重要的。表 1 列出不同密钥长度情况下循环 3 次时合法用户认证失败的错误拒绝率(False Reject Rate，FRR)和非法用户认证通过的错误接受率(False Accept Rate，FAR)。由于随机映射对人脸特征进行映射的结果具有随机性，因此实际 FRR 有±5%左右的浮动，不过错误接受率因为采样数量大，所以结果几乎不受影响。

表 1 不同密钥长度的认证结果

k_1 长度	k_2 长度	FRR(%)	FAR(%)
6	6	4.17	0.0015
6	9	6.51	0.0017
9	9	7.42	0
9	12	9.34	0
12	12	17.51	0

将不同密钥长度下 FCRM 提取的特征哈希做 ROC 曲线，比较其效果，结果如图 7 所示。

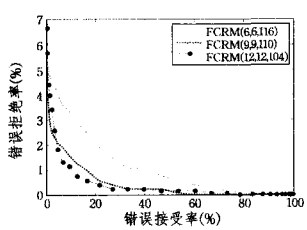

图 7 不同长度密钥的 ROC 曲线

由上述结果可知，随着每次循环密钥长度的增长，FRR 增加，FAR 降低，说明密钥越长，算法的接受率越低，但安全性越高。所以可以根据系统的实际需要，选择合适的密钥长度。实验过程中发现，使用 $k_1=9, k_2=9, k_3=110$，可以取得 128 位的密钥且识别率能够控制在比较理想的效果。

3.3 FCRM 与同类算法比较

将国内外其他同类人脸特征加密与使用 $k_1=9, k_2=9, k_3=110$ 情况下的 FCRM 进行比较，结果如表 2 所列。

表 2　同类算法比较

算法	文献	FRR(%)	FAR(%)
PCA+FCS	[2]	5	—
PCA+神经网络	[5]	7.5	2.46
PCA+RMQ-90	[7]	1.56	1.31
FDA+RMQ-90	[7]	0.002	0.001
RHLBPQ-90	[8]	0.6837	0.021
FCRM	本文	7.42	0

由此可见，FCRM 能够在牺牲少量认证成功率的前提下，提高认证的安全性。在实际应用中，相比其他算法需要采集多个人脸图像或者需要用户持有一份密钥，FCRM 只需要采集一次图像并且无需用户持有密钥就能进行认证，具有更高的实用价值。并且 FCRM 可通过调节密钥长度，调整算法的安全性，以满足不同应用的需求。其防止非法用户通过认证的能力超过其他同类的算法，且不会泄漏用户的特征信息，具有很高的安全性。

3.4　FCRM 安全性分析

将模板保存在服务器中是安全的。因为模板中没有包含用户的生物特征信息，可以防止用户的生物特征泄漏，同时无法从模板中推导出密钥信息，所以，攻击者即使突破了服务器的防护获得模板，也很难获得有用信息。即使攻击者使用穷举攻击，在一定时间内有机会能够计算出密钥，但 FCRM 可以非常方便地将用户特征哈希重新与一组新的密钥进行绑定。如果系统定时为用户重新绑定新的密钥，只要更新密钥的周期小于穷举破解所消耗的时间周期，那么密钥的安全性也能得到保证。

从加密过程的安全性来看，认证用户的生物特征在循环映射过程中每次产生的密钥必须相同，否则无法还原出与注册用户完全相同的密钥。实验表明，如果作为随机种子的密钥不同，那么提取的哈希值将呈随机的正态分布于 $\frac{m}{2}$（m 为密钥长度）附近。如图 8 所示，它与上节中非法用户曲线的位置一致，这将产生与注册生物特征相差很大的哈希值，无法释放出最终密钥，从而加强了加密过程的安全性。

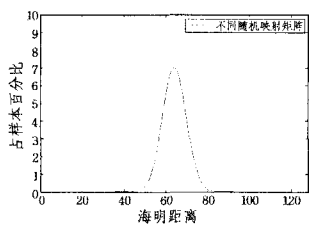

图 8　随机映射矩阵不同时的海明距离

在认证过程中，不同密钥发生碰撞的概率为 $\frac{1}{len(k_1+\cdots+k_{n-1})}$（$n$ 为循环次数）。当 k_1，k_2 长度都为 9 时，碰撞概率为 $\frac{1}{262143}$；k_1，k_2 长度都为 12 时，碰撞概率为 $\frac{1}{16777215}$。所以，攻击者很难通过穷举尝试破解密码。

结束语　本文在研究已有算法优缺点的基础上，提出了 FCRM 算法。算法通过对人脸生物特征循环使用随机映射增强认证安全性，在密钥中融入纠错码抵御随机噪声的影响，并使用模板机制保护用户的生物特征及密钥的安全性。

通过实验证明，FCRM 在使用单一人脸图像进行认证的情况下认证成功率能够超过 92%，虽然落后于其他使用多张图像的人脸识别算法，但在实际应用中，相比其他算法需要采集多个人脸图像，FCRM 具有更高的实用价值。并且 FCRM 可通过调节密钥长度调整算法的安全性，以满足不同应用的需求。其防止非法用户通过认证的能力超过其他同类的算法，且不会泄漏用户的特征信息，具有很高的安全性。

另外，本算法可以从以下方向改进：FCRM 的认证需要预先得知用户身份，才能使用该用户的模板进行认证，可以设计一种无需知道用户身份就可以自动定位用户的算法来实现安全的人脸识别功能。由于海明码纠错算法本身的限制，需要对密钥进行插值才能提高纠错率，可以考虑使用其他的纠错算法，如 RS 编码。也可以考虑在其他类型生物特征比如指纹和虹膜特征上对该算法的有效性进行验证。通过其他人脸特征提取算法，比如特征融合算法提取的人脸特征，在 FCRM 中的效果也是一个值得研究的内容。

参 考 文 献

[1] Juels A, Wattenberg M. A Fuzzy Commitment Scheme[C]// Proceedings of the 6th ACM Conference on Computer and Communications Security. ACM Press, 1999: 28-36

[2] 付波，李建平. 人脸特征密钥的容错生成算法[J]. 计算机应用研究，2008，25(1)：260-262

[3] Zhao Z, Paul W. A face hashing algorithm using mutual information and feature fusion[C]// Proceedings of the 2007 IEEE International Conference on Networking, Sensing and Control. UK (London): IEEE, 2007: 386-391

[4] Zhao Z, Paul W. A Novel Face Hashing Method with Feature Fusion for Biometric Cryptosystems[C]// Proceedings of the Fourth European Conference on Universal Multiservice Networks. France(Toulouse): IEEE, 2007: 439-444

[5] 张祥德，唐青松，陆小军，等. 基于神经网络和人脸特征的密钥管理方法[J]. 东北大学学报：自然科学版，2009，30(6)：817-820

[6] Juels A, Sudan M. A Fuzzy Vault Scheme [J]. Designs, Codes and Cryptography, 2006, 38(6): 237-257

[7] Teoh J, Goh A, Ngo L. Random Multispace Quantization As an Analytic Mechanism for Biohashing of Biometric and Random Identity Inputs [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2006, 28(12): 1892-1901

[8] 陈娜娜. 基于 LBP 的人脸密钥生成算法及其在加密系统中的应用研究[D]. 南京：南京航空航天大学，2008

[9] Ojala T, Pietikainen M, Maenpaa T. Multiresolution Gray-scale and Rotation Invariant Texture Classification with Local Binary Patterns [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002, 24(7): 971-987

[10] Kong B, Cheung K, Zhang D, et al. An Analysis of Biohashing and Its Variants [J]. Pattern Recognition, 2006, 39(7): 1359-1368

[11] 冯全，苏菲，蔡安妮. 生物加密综述[J]. 计算机工程，2008，34(10)：141-143

[12] 牛夏牧，焦玉华. 感知哈希综述[J]. 电子学报，2008，36(7)：1405-1411