

基于多模生物模板安全的顽健图像隐藏算法

曹玉强^{1,2}, 龚卫国¹, 柏森²

(1. 重庆大学光电学院, 重庆 400030;

2. 重庆通信学院, 重庆 400035)

摘要: 为了解决多模生物认证中生物模板安全传输问题, 提出把人脸图像隐藏嵌入到指纹图像中, 用于多模生物特征认证, 以提高生物特征识别的安全性和准确性。利用指纹图像归一化、中心点检测, 获取嵌入区域的几何失真不变域, 提出在几何失真不变域基于奇异值分解(SVD)的多重嵌入算法, 嵌入相应的人脸图像。检测者通过相关性优化算法, 盲提取人脸图像, 再结合载体指纹图像进行多模认证。实验结果表明, 该算法能够抵抗旋转、缩放、平移等几何失真, 也能抵抗压缩、滤波、噪声等攻击, 提高了生物模板的传输安全性, 指纹与人脸双模生物认证相比于单模认证具有更高的正确识别率。

关键词: 多模认证; 数字水印; 归一化; 奇异值分解

中图分类号: TN911.73

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00093

Robust image hiding algorithm for secure multimodal biometrics

CAO Yu-qiang^{1,2}, GONG Wei-guo¹, BAI Sen²

(1. College of Optoelectronic Engineering, Chongqing University, Chongqing 400030, China;

2. Chongqing Communication Institute, Chongqing 400035, China)

Abstract: In order to solve the bio-template secure transmission in multimodal biometric authentication, a novel algorithm was presented that hiding face watermarks in fingerprint carrier image to improve security and recognition accuracy. RST invariant embedding region was obtained by carrier image normalization and the core point detection. Multiple embedding based on SVD in the region and watermark optimizations in extraction process were presented in hiding scheme. The security of the proposed algorithm and its robustness against different kinds of attacks were verified by simulations.

Key words: multimodal biometrics, watermarking, normalization, SVD

1 引言

生物认证技术利用计算机对人体所固有的生理特征或者行为特征进行身份识别, 与传统的认证方法相比具有防伪性好、便于携带、不易丢失和遗忘的优点。采用单生物特征进行认证的系统, 普遍存在可靠性和安全性等问题。因此从系统的

安全性和可靠性等因素考虑, 多模生物认证是提高识别性能的切实可行的方法, 也成为当前生物认证技术研究的主流方向^[1]。生物认证的安全性中最重要的是生物数据的安全性, 必须保护它不被攻击或篡改, Ratha 等^[2]总结了生物认证系统的一般攻击类型, 主要有强制攻击、伪造攻击、重放攻击、在特征提取、模板数据库、匹配和判决

收稿日期: 2016-07-20; 修回日期: 2016-09-03。通信作者: 曹玉强, caoyuqiang163@163.com

基金项目: 国家自然科学基金资助项目 (No.61272043)

Foundation Item: The National Natural Science Foundation of China(No.61272043)

处的攻击。攻击可能改变生物图像或模板的内容,造成生物系统的性能下降。本文主要研究多模生物特征认证系统中的生物模板数据保护技术,以此提高生物特征的安全性和识别率的准确性。

早期研究者已经采用加密技术来处理生物系统安全性面临的挑战^[3]。近年来,随着数字水印技术的流行,其逐渐被应用在保护生物图像和模板的安全^[3~5]。其方法主要分为三大类:①在生物图像或模板中嵌入特殊的水印信息,在认证接收方通过提取的水印来判断生物图像或模板的真实性;②把生物图像或模板嵌入到可公开的图像等媒体中,通过保护生物图像或模板的存在来确保其安全性;③把同一人的某一生物特征(如人脸、虹膜等)嵌入到另一生物特征图像中(指纹、人脸等)中。接收方可以通过一个通道秘密接收两类特征,同时用来生物认证。这类双模认证既提高认证的准确性,又提高了生物特征的安全性。

Vatsa^[6]提出基于冗余小波变换的双模认证的算法,把 MFCC (mel frequency cepstral coefficients) 信号作为水印嵌入到彩色人脸图像中,存在嵌入容量偏低,顽健性较差的缺点。WongyumKim^[7]提出两级认证的多模生物图像水印算法,精简的人脸图像特征作为水印被嵌入到指纹图像中,仅用于判断载体图像的受攻击情况。Miao^[8]提出基于相关分析算法把虹膜和掌纹特征作为水印嵌入到普通载体图像中。顽健性尤其是抗几何攻击性能和隐藏容量成为多模生物特征隐藏的主要问题。

信息隐藏技术中的数字水印和隐写术技术本身有很大不同。数字水印技术为了保护载体信号而强调水印的抗攻击顽健性,所以水印容量都很小;隐写术主要是通过载体的隐蔽性保护嵌入其中的秘密信息,主要考虑其嵌入容量,而顽健性差。不管是数字水印还是隐写术,几何攻击都一直是一个难以解决的问题。数字水印技术中抗几何攻击的算法大致可分为三类。①基于失真校正的方法,为了抵抗几何攻击在原始信息中嵌入一个注册模板或者将水印设计为一种特殊形式,使水印检测器可以检测几何失真。这种方法实际是嵌入 2 个水印,一个是真正的水印,另一个用于

检测几何失真的水印。②基于图像归一化的方法,通过对图像进行归一化使其对旋转、平移和尺度变换具有不变性。在水印检测之前对待检测图像做同样处理。③基于图像不变性特征的方法,常采用的不变性特征有 Fourier-Mellin 变换系数、几何矩不变量和 Zernike 矩等。

Zhu^[9]利用不变矩特征校正受几何攻击的含水印图像,再进行水印提取,水印嵌入容量大约 0.038 bit/s; Li^[10]提出利用 harris 角点检测寻找稳定特征点,以特征点为中心形成圆环嵌入区域,该算法嵌入容量仅有十几比特。Niu^[11]利用 SIFT 变换寻找稳定特征点,以特征点为中心形成嵌入圆形区域,再用 Bandelet 变换嵌入水印,此算法嵌入容量 0.003 9 bit/s。从目前的抗几何攻击水印算法来说,嵌入容量都不能满足生物特征隐藏的需求。

本文提出基于奇异值分解 (SVD, singular value decomposition) 变换和图像归一化 (normalization) 相结合的信息隐藏算法,克服嵌入容量和几何攻击问题,使在指纹图像中能够顽健嵌入容量较大的人脸图像,满足双模生物认证的需求。

2 嵌入算法

完整的隐藏算法如图 1 所示。利用图像归一化获取 RST 不变区域 (rotation, scaling and translation invariant), 在归一化的图像中采用 SVD 算法多重嵌入水印图像,为了进一步提高生物模板的安全,引入混沌置乱对图像进行预加密处理。

2.1 图像归一化

图像归一化算法根据图像特征来获取图像的旋转、平移与缩放参数,按照一种标准形式对图像进行几何变换。图像归一化可以消除仿射变换 (RST 攻击) 对图像的影响。目前常用的归一化算法是基于矩的归一化^[12],其过程为坐标中心化、x-shearing 归一化、缩放归一化和旋转归一化。本文采用文献[12]的方法对载体图像进行归一化处理,获得标准图像形式,载体图像经过平移、切变、缩放和旋转后,归一化的图像与原始载体图像保持基本一致,如图 2 所示。

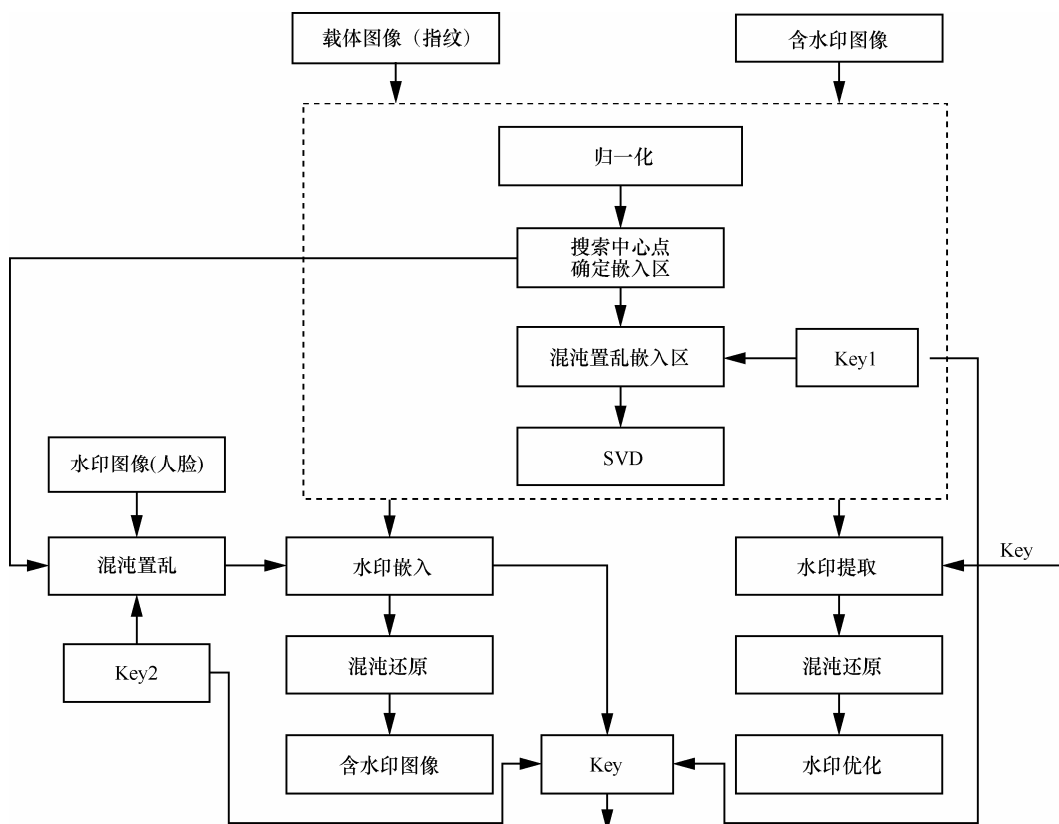


图 1 生物水印隐藏算法

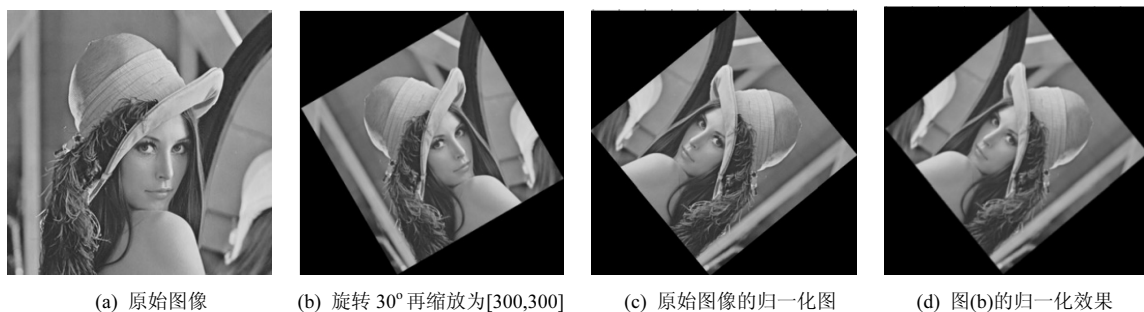


图 2 图像归一化在几何攻击下的比较

几何攻击最主要的危害是破坏了水印嵌入区域的同步性，从图 2 可以看出，归一化处理能够保证在几何攻击下的图像位置基本不变，为在归一化的图像中嵌入水印提供抗几何攻击的保证。

2.2 奇异值分解

基于奇异值分解的水印嵌入策略，由刘瑞祯等^[13]较早提出。随后，在这个基础上，提出了很多改进方法。最早提出的奇异值分解是在整个图像上进行的，水印容量大，但是安全性不够，因为提取水印所需要的辅助信息包含了大部分水印信息。而后提出的先对图像进行分块，然后在各

个子块上进行奇异值分解的水印嵌入方法^[14]，避免了上述的问题，但是嵌入的水印信息较小，不满足本文生物模板嵌入的需求。本文在文献[13]的基础上，改进 SVD 算法，利用混沌理论，置乱加密算法指纹和人脸图像，以增强整个水印算法的安全性。

若一幅图像用 A 表示，定义 $A \in \mathbb{R}^{n \times n}$ ，其中 $\mathbb{R}$ 表示实数域，则矩阵 A 的奇异值分解定义如下。

$$A = USV^T \quad (1)$$

其中， U 、 V^T 均为正交阵， S 为对角阵，其对角线元素为 A 的从大到小排序的非负奇异值。

2.3 Logistic 混沌映射

混沌序列有以下特性：1) 是非周期的序列；2) 混沌序列不收敛；3) 对初始条件及其敏感，生成序列不可预测等。所以常用来生成随机水印信号或者用来置乱图像序列。一类非常简单却广泛应用的混沌系统是 Logistic 映射，定义如下。

$$x_{k+1} = \mu x_k (1 - x_k), x_k \in (0,1) \quad (2)$$

当 $3.571448 < \mu \leq 4$ 时，该混沌映射处于混沌状态。[3.571448, 4]称为混沌区域，在某一初始条件 x_0 下，由式(2)Logistic 映射生成序列为 $\{x_k, k=0,1,2,3,\dots\}$ ，具有上述的混沌序列特性。本文利用混沌序列置乱载体图像和水印图像，增加图像的随机性和安全性。

2.4 水印嵌入区域选择

生物特征识别认证对生物图像质量有较高的要求，生物水印图像经攻击后图像质量往往下降严重，即使能够满足水印认证的要求，但并不一定满足后续的识别认证需求。为了能够获得更高的水印图像质量，本文提出在图像归一化域中选择几何不变域多重嵌入，提取的多个水印图像进行优化组合获得最佳水印图像。

虽然，载体图像经过归一化之后，具有仿射攻击不变性。但在一些攻击依然可能存在小的像素位置偏移，精确的像素定位在水印提取过程中非常重要。因为载体为指纹图像，关于指纹图像的中心点定位算法有很多，本文采用文献[15]确定中心点，依次为基准，确定嵌入区域。以归一化的载体指纹图像的中心点为中心，向外形成 n 个与水印图像尺寸一致，互不重叠的嵌入区域。计算每个嵌入块的平均亮度值 V ，以 V 作为参数确定嵌入系数 a 的取值。图像奇异值与图像的能量有很大关系，平均亮度值越大，奇异值也越大。

2.5 水印预处理

按照文献[13]的算法嵌入水印图像，存在很大安全隐患，需要另外传送水印的 U 、 V 分量，而 U 、 V 分量表示水印图像的细节，随机选择一个较合适的 S 都能恢复出水印的绝大部分信息。为了避免此隐患，本文结合载体图像对水印进行预处理。在归一化的载体图像中心，获取水印大小的载体图像内容 B_{F0} 。根据 2.3 节混沌映射方法，对水印图像 W 和载体图像中心块 B_{F0} 分别进

行混沌置乱，通过下式获得新水印 W_{new} 。

$$W_{new} = W_c + B_{c_{F0}} \quad (3)$$

W_c 、 $B_{c_{F0}}$ 分别表示 W 和 B_{F0} 的混沌置乱后图像。水印图像与载体图像结合，即获得了 U 、 V 分量和 key 等信息，那么合成的图像也极大偏离生物图像的原貌。只有具备完整的密钥信息和含水印的图像等才能完整地恢复出生物水印图像。

2.6 生物水印嵌入过程

具体生物水印嵌入步骤如下。

步骤 1 根据 2.1 节图像归一化方法对载体图像 I 进行归一化，获得标准的归一化图像 ln 。

步骤 2 根据 2.4 节方法选择 n 个嵌入块 B_{Fi} ，并计算每块的亮度均值 Bm_i ， $i=1,\dots,n$ 。

步骤 3 根据 2.3 节混沌映射方法，生成 n 个混沌序列，以此序列分别置乱 n 个嵌入块 B_{Fi} ，得到 $B_{c_{Fi}}$ ，并保存每个序列的初始值 x_0 作为密钥 $key1$ 。

步骤 4 在每个嵌入块 $B_{c_{Fi}}$ 执行 SVD，如下式所示

$$B_{c_{Fi}} = U_i S_i V_i^T, i=1,\dots,n \quad (4)$$

步骤 5 根据 2.5 节方法获取新水印 W_{new} ，并保存混沌序列的初始值 x_0 作为密钥 $key2$ 。

步骤 6 根据混沌置乱的水印图像 W_{new} ，用下式修改每个嵌入块的奇异值矩阵。

$$Sw_i = S_i + \alpha_i W_{new}, i=1,\dots,n \quad (5)$$

这里 α_i 表示嵌入系数。

步骤 7 对被修改的奇异值矩阵 Sw_i 进行 SVD 分解，如下式

$$Sw_i = U_i^{new} S_i^{new} (V_i^{new})^T, i=1,\dots,n \quad (6)$$

步骤 8 用式(7)、式(8)进行 SVD 逆变换，得到含水印的置乱图像和密钥 key

$$Bwc_i = U_i S_i^{new} V_i^T, i=1,\dots,n \quad (7)$$

$$Bkey_i = U_i^{new} S_i^{new} (V_i^{new})^T, i=1,\dots,n \quad (8)$$

步骤 9 根据混沌映射对含水印的置乱块 Bwc_i 进行逆置乱，还原含水印图像块为 Bw_i 替换原始嵌入块 B_i ，并对图像归一化逆变换，得到含生物水印图像 G 。组合密钥 $key1$ 、 $key2$ 和 $Bkey_i$ 为密钥 Key 。

2.7 水印提取过程

生物水印提取过程与嵌入逆过程近似，具体

步骤如下。

步骤1 与嵌入过程的步骤1到步骤4一致，应用密钥 $key1$ 获得含水印的置乱块 Bwc_i' 。

步骤2 对 Bwc_i' 和密钥 Key 中的 $Bkey_i$ 分别进行 SVD 分解，如式 (9) 和式 (10) 所示。

$$Bwc_i' = U_i' S_{w_i} V_i'^T, \quad i=1, \dots, n \quad (9)$$

$$Bkey_i = U_i^{new} S_i (V_i^{new})^T, \quad i=1, \dots, n \quad (10)$$

步骤3 根据式(11)提取各个块的水印 Wc_i^{ext}

$$Wc_i^{ext} = \frac{U_i^{new} S_{w_i} (V_i^{new})^T - S_i}{a_i}, \quad i=1 \dots n \quad (11)$$

步骤4 类似于嵌入过程，提取含生物水印图像 G 的中心块 B_{F0}' ，因为 $B_{F0}' \approx B_{F0}$ 。用 B_{F0}' 代替 B_{F0} 提取生物水印。

$$W_i^{ext} = Wc_i^{ext} - B_{F0}' \quad (12)$$

2.8 水印优化处理

在水印提取过程中，没有原始生物水印图像 W 可参考，提取还原的水印图像 W_i^{ext} 是否正确无法直接判断。含水印图像可能遭到各种攻击，如旋转、剪切、缩放、滤波或压缩等，即本身含有水印，那么有些位置的水印 W_j^{ext} 可能失真较大，而不能利用。本文提出互相关的方法提取出最优生物水印图像。 W_i^{ext} 之间的互相关系数 ρ 采用式(13)计算。

$$\rho_{i,j}(W_i^{ext}, W_j^{ext}) = \frac{|\sum_{x=1}^{Mw} \sum_{y=1}^{Nw} (W_i^{ext}(x,y) - \bar{W}_i)(W_j^{ext}(x,y) - \bar{W}_j)|}{\sqrt{\sum_{x=1}^{Mw} \sum_{y=1}^{Nw} (W_i^{ext}(x,y) - \bar{W}_i)^2 \cdot \sum_{x=1}^{Mw} \sum_{y=1}^{Nw} (W_j^{ext}(x,y) - \bar{W}_j)^2}} \quad (i, j=1, \dots, n, i \neq j) \quad (13)$$

这里 Mw 、 Nw 分别表示水印图像长、宽像素数， $\bar{W}_i$ 表示水印 W_i^{ext} 的均值。因为 W_i^{ext} 之间存在亮度差异，通过 $\bar{W}_i$ 消弱亮度差异带来的干扰。

如果 W_i^{ext} 是遭到严重破坏的水印图像或者虚假水印，那么 W_i^{ext} 与提取的其他水印图像相关性很差；相反，如果 W_i^{ext} 是质量较好的水印图像，必然与其他质量较好的水印图像有很高的相关性。以此，保留互相关性高的那些水印图像，而剔除与其他水印相关性差的水印图像。设置门限

ρ_{thra} ，当 $\rho_{i,j} > \rho_{thra}$ 时，说明 W_i^{ext} 和 W_j^{ext} 是可用的水印图像；当 $\rho_{i,j} < \rho_{thra}$ 时，判断 W_i^{ext} 、 W_j^{ext} 和其他水印图像间的相关系数，如 $\rho_{i,k} > \rho_{thra}$ ，而 $\rho_{j,k} < \rho_{thra}$ ，说明 W_j^{ext} 是不可用的水印，应该舍弃。假如候选 k 个提取的水印图像，最优的水印图像 W^{ext} 由式 (14) 给出。

$$W^{ext} = \beta_1 W_1^{ext} + \beta_2 W_2^{ext} + \dots + \beta_k W_k^{ext} \quad (14)$$

$$\beta_1 + \beta_2 + \dots + \beta_k = 1$$

β_i ($0 < \beta_i < 1$) 表示权重因子，其值与相关系数有关，当水印图像 W_i^{ext} 与其他水印图像相关系数相对较大，那么说明本水印质量较好， β_i 设置较大值，否则设置较小值。

最终得到的水印图像可能存在较大的噪声，对后期的识别认证有影响，通过中值滤波可以消除大部分噪声，大大提高图像质量，如图3所示。图3中，图3(a)~图3(d)分别为4个区域提取的结果，图3(e)为4个图像合成的结果。可以看出质量上有明显提升，但噪声较明显，图3(f)为图3(e)滤波后的效果，质量改善很大，视觉上与原始图像相似。

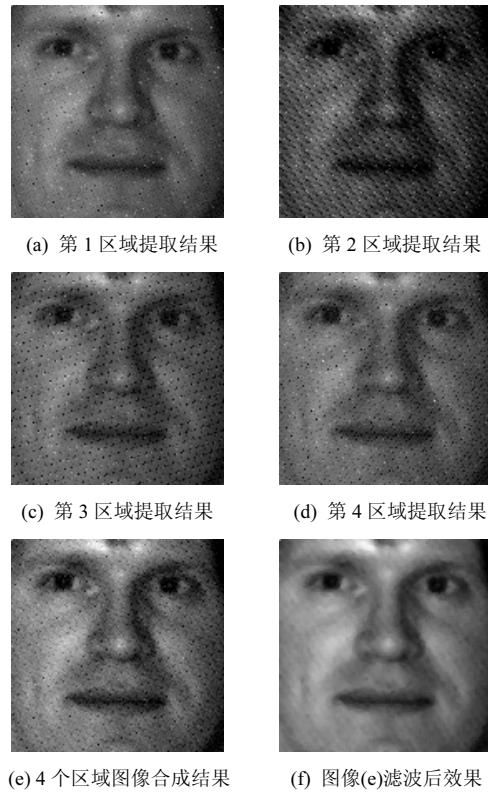


图3 提取人脸图像比较

3 实验结果与性能分析

为了验证本文提出的生物水印隐藏算法，以 DFC V200 指纹数据作为算法测试载体图像数据库，其中共有 64 个不同手指图像，每个手指 8 幅图像，每幅图像尺寸为 256×300 ，8 bit 灰度图像。因为没有本指纹数据库对应的人脸图像库，所以另外选择 Yalefaces 128×128 和 64×64 的灰度人脸数据作为生物水印图像库，其中共有 15 个人，每人 15 张不同表情的图像。

3.1 各类攻击提取效果测试

图 4 给出了无攻击条件下，正常隐藏提取的效果，含密指纹视觉上与原始指纹无差异，

峰值信噪比为 43.53 dB，说明图像质量优良，人脸嵌入对指纹图像影响很小。提取的人脸图像与原始人脸图像的相关系数 $\rho=0.9989$ ，所以从视觉上和相关度上比较，效果都是非常好。图 5 给出了各类攻击条件下，人脸的提取效果。实验结果表明，一定条件的几何攻击，如旋转、剪切、尺度变换，本隐藏提取算法依然能获得较好的人脸图像，相关度 ρ 保持在 0.96 以上；同样在滤波、噪声和增强攻击下也能保持很好的提取效果。因此，从视觉效果和相关度上评价，该算法能够保持较好的抗攻击能力，较好的顽健性。

JPEG 图像是最常用的图像压缩格式，下面本

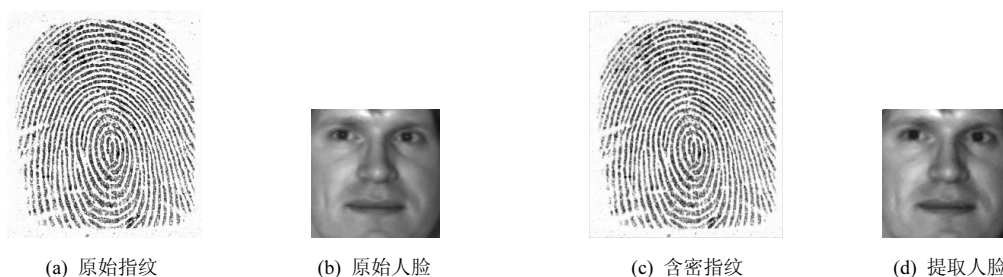


图 4 无攻击的隐藏提取效果

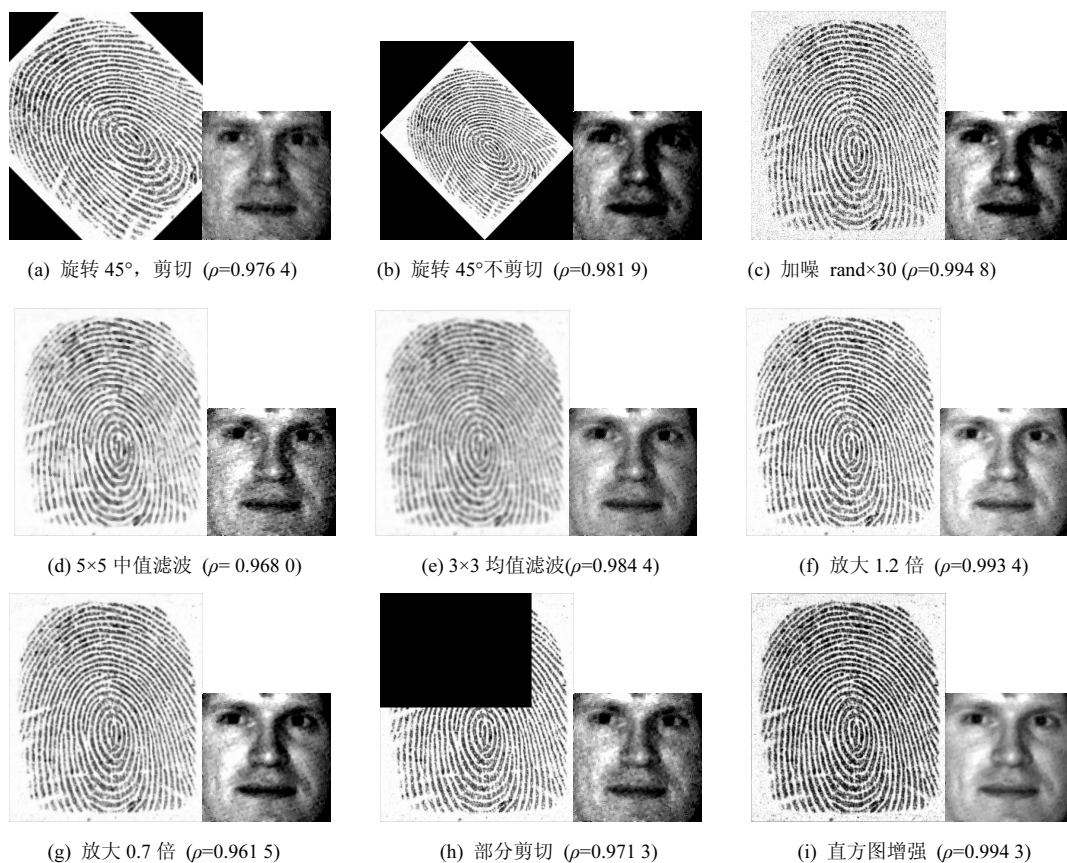


图 5 各类攻击测试

文测试含密指纹图像在不同量化因子条件下, JPEG 压缩对人脸提取的影响, 图 6 展示了具体效果。

JPEG 压缩测试结果表明, 量化质量因子(Q)为 20 时, 相关系数 ρ 保持在 0.97 以上, 而当 Q 为 10 时, ρ 明显下降到 0.934 0。为了保持较好的保真度, 一般 JPEG 压缩的量化质量因子在 70~80 间, 而此时相关系数 ρ 保持在 0.98 以上, 同时也具有很好的视觉效果。

3.2 比较指纹人脸图像的各自识别结果差异

生物模板主要应用于身份识别认证, 含密指纹图像和提取的人脸图像效果如何, 不仅要从视觉和相关度上判断, 也需要测试其识别率, 在同等条件下, 测试观察含密指纹图像和原始指纹图像的识别率差异以及原始人脸图像和提取人脸图像的识别率差异。

实验条件: 选择 Yale 人脸图像库, 每人有 10

幅不同表情的图像。随机选择 5 幅作为训练样本, 另外 5 幅作为测试样本, 分别应用 PCA^[16]和 FLDA^[17]算法测试其识别率, 获得原始人脸图像库的识别率。把 5 幅测试人脸分别作为秘密人脸, 经过隐藏提取, 获取的秘密人脸图像替换原始的图像, 测试其识别率, 统计提取人脸的识别率。指纹识别仅比较未受攻击的原始指纹图像和含密指纹图像的识别率差异, 经比较识别率基本不变。因为含密指纹图像降质不明显, 隐藏并不影响指纹特征的提取, 所以指纹识别率保持一致。表 2 列举了尺寸为 128×128 和 64×64 两类人脸图像在不同攻击下提取后的识别率比较结果, 各类攻击对人脸识别有少部分影响, 识别率降低 5% 左右。假定人脸图像和指纹图像来自同一个人, 双生物特征融合后识别率会高于单一特征的识别率, 因生物特征库限制未做相应测试。



图 6 不同量化质量因子的 JPEG 压缩攻击提取效果

表2 不同攻击条件下提取人脸的识别率比较

Attack	识别率			
	PCA(128)	FLDA(128)	PCA(64)	FLDA(64)
No Attack	68.7%	89.22%	68.1%	87.3%
Rotation (45°)	60.5%	79.4%	61.6%	78.9%
Median Filtering	65.7%	85.3%	63.5%	83.4%
Resizing (1.2)	67.1%	88.5%	62.8%	84.7%
JPEG (Q=40)	64.5%	86.2%	62.7%	83.2%

4 结束语

信息隐藏技术的抗攻击问题一直是其难点，容易受到隐藏容量和提取保真度的限制。本文针对多模生物特征安全传输、存储问题，基于信息隐藏技术提出人脸与指纹图像隐藏保护策略。而且本文提出的算法不仅解决隐藏保护问题，更强调其抗各类攻击能力，尤其在几何攻击方面。目前，几何攻击是信息隐藏技术的一大难题，SVD、归一化和特征定位的结合，可以较好地解决几何攻击问题。本文中提出水印优化检测策略，大大提升了隐藏图像的提取质量，为下一步的特征识别提供质量保障。

参考文献：

- [1] ROSS A, JAIN A K. Information fusion in biometrics[J]. Pattern Recognition Letters, 2003(24): 2115-2125.
- [2] RATHA NK, CONNELL J H, BOLLE RM. Secure data hiding in wavelet compressed fingerprint images[C]//ACM Multimedia. 2002: 127-130.
- [3] JAIN A K, ULUDAG U. Hiding biometric data[J]. Transactions on Pattern Analysis and Machine Intelligence, 2003, 25(11): 1494-1498.
- [4] GUNSEL B, ULUDAG U, TEKALP A M. Robust watermarking of fingerprint images[J]. Pattern Recognition, 2002, 35(12): 2739-2747.
- [5] VATSA M, SINGH R, MITRA P, et al. Comparing robustness of watermarking algorithms on biometrics data[C]//The Workshop on Biometric Challenges From Theory to Practice-ICPR. 2004: 5-8.
- [6] VATSA M, SINGH R, NOORE A. Feature based RDWT watermarking for multimodal biometric system[J]. Image and Vision Computing. 2009(27): 293-304.
- [7] GYUMKIM W, LEE H. Multimodal biometric image watermarking using two-stage integrity verification, Signal[C]//Process. 2009.
- [8] MIAO Q, YING H L, NING D. A novel image hiding approach based on correlation analysis for secure multimodal biometrics[J]. Journal of Network and Computer Applications, 2010(33): 247-257.
- [9] ZHU H Q, LIU M, LI Y. The RST invariant digital image watermarking using Radon transforms and complex moments[C]//Digital Signal Process. 2010.

- [10] LI L D, GUO B L. Localized image watermarking in spatial domain resistant to geometric attacks[C]//International Electronic Communication. 2009: 123-131.
- [11] NIU P P. A feature-based robust digital image watermarking scheme using bandelet transform[J]. Optics & Laser Technology, 2011(43): 437-450.
- [12] PING D, BRANKOV J G, GALATSANOS N P, et al. Digital watermarking robust to geometric distortions[J]. IEEE Transactions on Image Processing, 2005, 14(12):2140-2150.
- [13] 刘瑞祯, 谭铁牛. 基于奇异值分解的数字图像水印方法[J]. 电子学报, 2011, 29(2): 2.
- LIU R Z, TAN T N. SVD based digital watermarking method[J]. Acta Electronica Sinica, 2011, 29(2):1-4.
- [14] 李海峰, 王树勋, 温泉, 等. 基于分块 SVD 和 Zernike 矩的顽健图像水印[J]. 模式识别与人工智能, 2005, 18 (3): 6.
- LI H F, WANG S X, WEN Q, et al. Robust image watermarking based on block SVD and zernike moments[J]. Pattern Recognition and Artificial Intelligence, 2005, 18(3):359-365.
- [15] 冯俐俐, 李昌禧. 指纹中心点的定位和特征匹配方法[J]. 华中科技大学学报(自然科学版), 2002, 30(10): 78-80.
- FENG L L, LI C X. Fingerprint matching algorithm based on finger core[J]. Journal of Huazhong University of Science and Technology(Natural Science Edition), 2002, 30(10):78-80.
- [16] TURK M, PENTLAND A. Eigenfaces for recognition[J]. Journal of Cognitive Neuroscience, 1991, (3): 72-86.
- [17] BELHUMEUR P N, HESPANHA J P, KRIEGMAN D J. Eigenfaces vs fisherfaces: recognition using class specific linear projection[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1997, 19(7): 711-720.

作者简介：



曹玉强（1977-），男，河南南阳人，重庆通信学院讲师，主要研究方向为信息隐藏、数字水印、图像压缩和模式识别。



龚卫国（1957-），男，重庆人，重庆大学教授、博士生导师，主要研究方向为图像处理、模式识别、智能化信息技术及系统。

柏森（1963-），男，四川达州人，博士（后），重庆通信学院教授、硕士生导师，主要研究方向为信息隐藏、掩密通信、图像处理、模式识别。