DOI:10.11721/cqnuj20130421

一种基于单像素指纹边界的信息隐藏技术*

秦 勤,李 莉
(河南工程学院 计算机学院,郑州 451191)

摘要:利用信息隐藏技术提高身份认证系统的安全性是一种有效方法,通过将用户身份信息中的指纹、人脸以及口令融合进行多模态认证提高身份认证安全性。而将口令信息嵌入到指纹图像中实现口令信息的隐藏及存储,既能够满足安全认证的需要,又能够保证口令存储的安全性能。本文首先介绍了基于指纹图像为载体的口令信息隐藏技术,然后将细化后指纹图像按单元块进行像素划分,再将口令信息按照 Hash 函数嵌入到单元中心像素点上,相当于构成一个二元信息稀疏矩阵。该方法不仅保证了指纹图像的质量,还确保了指纹图像骨架脊线的质量,从而确保了指纹识别的精度。最后,通过实验结果表明,本文提出的基于单像素指纹边界的信息隐藏技术能够较好地将信息嵌入到指纹图像中,具有较低修改率的同时提高了 *PSNR* 峰值信噪比量,而且与其它方法相比,本文提出的方法对指纹识别正确率影响较小。

关键词:指纹图像;细化;口令信息;嵌入
中图分类号:TP399 **文献标志码**:A **文章编号**:1672-6693(2013)04-0109-04

随着微型电子技术以及信息技术的迅速发展,信息安全逐渐成为人们日益重视的一个热门话题。用户身份认证是保证用户个人信息安全的一个最基本的屏障,近年来,关于如何将一些典型的生物特征(如指纹、人脸、声音等)应用于身份认证技术中,成为提高信息安全领域中的一个研究热点。将多个生物特征以及用户口令融合在一起,进行多模态的身份认证可以提高认证的安全性。同时,在多模态身份认证信息融合过程中,信息隐藏技术是一种有效的方法[1-2]。

文献[3]提出了一种将信息隐藏于指纹模板中的身份认证框架。该方法首先采集原始用户指纹图像,将指纹图像进行细化,使指纹图像中只具有单像素边界值,即二值图像;其次获取用户的口令或人脸局部特征等用户信息,将这些信息嵌入到细化后的单边界二值指纹图像中;最后,在身份认证的过程中,用户在成功匹配指纹后,需要输入口令信息完成第二次认证。与其它关于二值图像的信息隐藏方法[4-5]相比,文献[3]提出信息隐藏方法在保证指纹图像质量的情况下,达到了指纹的完整性认证,提高了身份认证的安全性。文献[6]对这种认证方法进行了改进,但是存在有像素点交叉的现象,本文针对文献[3]提出的信息隐藏身份认证方法,提出了基于指纹图像的信息嵌入隐藏算法,该算法能够有效地将用户口令等安全信息融合进指纹图像中,解决了信息嵌入指纹图像时出现的像素点交叉现象,在不影响指纹图像质量的情况下,提高了身份认证的安全性。

1 基于单像素指纹边界的信息隐藏技术

将信息嵌入指纹图像中,首先需要将采集入库的指纹图像进行滤波细化处理[7],目的是构造指纹特征库,为指纹匹配识别建立原始指纹数据库。其次是判定细化处理后的指纹图像中的像素点是否可以嵌入信息,只有可以嵌入信息的像素点才会被选取。每一个像素点是否为可嵌入信息的决定因素是:该像素点为中心的 3 * 3 邻居像素点为前景色的个数与位置分布。约定当前像素点为中心点 P_0,与其相邻的 8 个像素点分别标记为 P_1,P_2,…,P_8;并且每一个像素点的取值均为 0 或 1,即 $P_i \in \{0,1\}$。其中"0"代表指纹图像中的背景像素(用白色表示),"1"代表指纹图像中的前景像素(用黑色表示)。其结构图如图 1 所示。

一个指纹图像中的像素点 $P(i,j)$是否可以嵌入信息,其判定条件为

$$P(i,j)=\overline{P_0}\cdot\left(\prod_{w=1}^{4}\overline{P}_{2*w-1}\right)\cdot\sum_{w=1}^{4}(P_{2*w}*P_{2*w+2}) \tag{1}$$

* **收稿日期**:2012-08-13 **修回日期**:2012-10-12 **网络出版时间**:2013-07-20 19:23
资助项目:河南省科技厅基础与前沿项目(No. 122102310442);河南省教育厅自然科学研究重点项目(No. 12B520011)
作者简介:秦勤,女,讲师,硕士,研究方向为计算机网络,E-mail:xindaqinqin@126.com
网络出版地址:http://www.cnki.net/kcms/detail/50.1165.N.20130720.1923.201304.109_018.html

$(i-1,j-1)$ P_1	$(i-1,j)$ P_2	$(i-1,j+1)$ P_3
$(i,j-1)$ P_8	(i,j) P_0	$(i,j+1)$ P_4
$(i+1,j-1)$ P_7	$(i+1,j)$ P_6	$(i+1,j+1)$ P_5

图1 像素点及其邻居点标记

(1)式中,$\overline{P_0}$是P_0的逻辑取反值,其中当$w=4$时,$P_{2*w+2}=P_{10}=P_2$,并且$P(i,j)\in\{0,1\}$,当$P(i,j)=0$时,表示当前像素点P_0是不可嵌入信息点;反之当$P(i,j)=1$时,表示当前像素点P_0是可嵌点。作者往往希望获取到指纹图像点是那些可嵌入信息的像素点,对于不可嵌入信息的像素点关心较少,在上式的计算过程中,共有4种模式能使得$P(i,j)=1$,即有4种像素点分布模式能使得像素点P_0是可嵌入信息的。这4种模式如图2所示。若当前像素点P_0处于图2中任一模式时,则表示它是可以嵌入信息的点。

2 消息嵌入过程

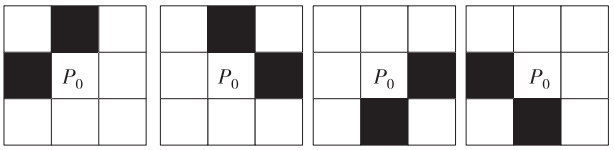


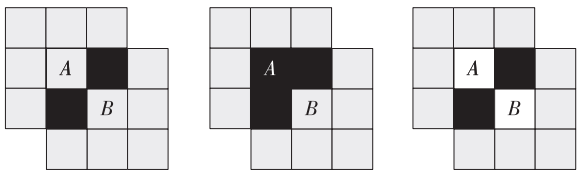
图2 像素点可嵌入信息的4种模式

将细化后的指纹图像,使用上述方法获取到其中的可嵌像素点,将一定长度的消息数据嵌入到指纹图像中的嵌入过程如下。

1) 将细化后的指纹图像可嵌入信息的像素点进行标记,使用Hash函数产生与待嵌入消息数据长度等量的像素点个数,这些使用Hash函数选中的可嵌像素点具有一定的随机性,使得恶意伪造身份的入侵攻击具有一定的难度,从而提高了信息的安全性和隐蔽性。

2) 将消息数据按位嵌入到第1)步选取出来的像素点中,具体为:当消息数据为"0"时,当前像素点P_0的值不变,当消息数据为1 bit"1"时,便将当前像素点P_0的值变为1,同时,将其像素点颜色进行翻转,将背景色白色置为前景色黑色。重复此过程直到所有消息数据全部嵌入。

在上述消息嵌入过程中,存在一种情况是:当前像素点的邻居点极有可能是另一个可嵌入信息的中心点,如图3中(a)所示,A、B均为或嵌入信息的像素点,如果像素点A嵌入1 bit信息"1"后,则像素点B会出现不可嵌入现象,如(b)所示;如果A点嵌入1 bit信息"0"后,B像素点则不受干扰,仍然为可嵌入像素点。这是由于中心像素点的邻居点交叉引起的,如果忽略此问题会造成指纹图像的骨架特征受到改变,可能会引起指纹图像的特征点发生变化,会对指纹图像的识别造成一些影响,因此消息数据嵌入到指纹图像中时,出现的像素点交叉问题需要解决。



(a)A与B均为嵌入点 (b)A嵌入信息"1"后,B为不可嵌入点 (b)A嵌入信息"0"后B可嵌入

图3 消息数据嵌入时的像素点交叉现象

定义一幅指纹图像的嵌入率为消息长度与指纹图像的大小的比值;修改率是被修改的像素点个数与指纹图像大小像素点个数的比值。在实际的应用中,嵌入的用户信息大多是用户口令,口令本身的数据量较小(一般情况下约为160 bit)[6],文献[6]中指出,对于一幅尺寸为512 * 512像素的指纹图像,可嵌入信息量超过了10 000 bit,因此,将用户口令嵌入到指纹图像载体中,相当于构造一幅稀疏矩阵。在不影响嵌入率与修改率的情况下,将指纹模板图像的像素点划分成3 * 3像素的一个小单元unit,定义一个3 * 3像素的unit小单元为嵌入信息的最小单位,如此按块划分可以解决上述像素点交叉的现象,同时可嵌入信息量超过了1 000 bit,完全能够容纳常规口令160 bit数据量。将指纹图像按块划分嵌入点的示意图如图4所示。

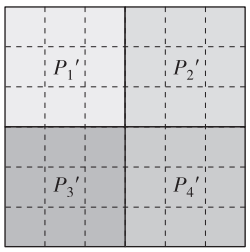


图4 将图像按块划分示意图

将指纹图像按块划分嵌入点的好处是解决了像素点交叉现象,同时避免了信息的嵌入对指纹单像素边界脊线的影响,降低了嵌入口令信息对指纹识别率的影响。

3 口令信息提取过程

将口令信息嵌入到指纹图像中，用户完成第一步认证后，需要进行口令认证过程，口令认证要将嵌入到指纹图像中的口令提出来进行匹配计算，如果一致则完成认证，如果不匹配，则拒绝认证。提取口令信息过程分为两步，重构 Hash 函数找出嵌入口令信息的像素点位置与口令信息数据提取。根据上文所述，将一幅 512 * 512 个像素的细化处理指纹载体图像 F 按 3 * 3 个单元小方块划分后，将有约 37 * 37 个单元像素块，根据(1)式可以计算出像素单元中心点 $P(i,j)$是否可嵌；选取可嵌入信息点的像素单元，即 $P(i,j)=1$，为了提升信息融合的安全性，采用 Hash 函数产生嵌入信息的像素单元位置，因此，重新构造 Hash 函数能够确定嵌入信息的像素单元的位置。确定出嵌入信息单元像素位置后，将信息数据提取分为 2 种情况：当单元像素的类型是图 2 中所示的某一种时，说明嵌入的信息数据是 1 bit “0”；当单元像素的类型是图 5 中所示的某一种时，说明嵌入的信息数据是 1 bit “1”。

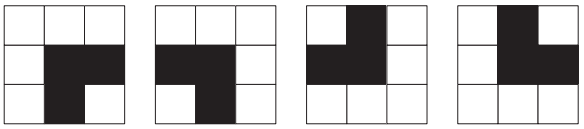


图 5　单元像素点中心点嵌入信息 1 后的模式

4 实验结果

图 6 中(a)图所示为一幅原始指纹图像，(b)图为经过滤波增强与特征提取以及细化处理后的指纹图像[8]，以此指纹图像为载体，用文献[3]的方法和本文提出的方法对口令信息数据进行嵌入，对比分析 2 种方法的嵌入率和峰值信噪比(PSNR)指标，其中单边界指纹二值图像 $PSNR$ 值可以利用(2)、(3)式计算得出。

(a)原始图像　　(b)处理后的图像

图 6　一种指纹图像的模板

$$MES=\frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}(b_{ij}-b'_{ij})^2*255 \tag{2}$$

$$PSNR=10\log_{10}\frac{255^2}{MES}dB \tag{3}$$

上式中，M 与 N 分别代表指纹图像的宽和高；b_{ij} 与 b'_{ij} 分别代表原始指纹图像和嵌入信息指纹图像对应的像素值。

在实验中，将本文提出的信息隐藏技术与文献[3]中提出的方法进行对比分析，评价指标分别用 2 种方法的 $PSNR$ 值比较和口令信息隐藏对于指纹正确匹配率的影响。通过 $PSNR$ 值的对比，可以判断出信息隐藏技术对于指纹图像峰会信噪比的影响情况，而通过信息隐藏对于指纹正确匹配率的实验可以直观地观察得出信息隐藏技术对于指纹模板图像的骨架脊线线条的影响度，较好的信息隐藏技术不会对指纹骨架脊线线条造成过多的影响，从而不会影响到指纹的正确识别率。图 7 和图 8 分别是采用文献[3]中的信息隐藏技术和本文提出的信息隐藏方法的实验结果图。

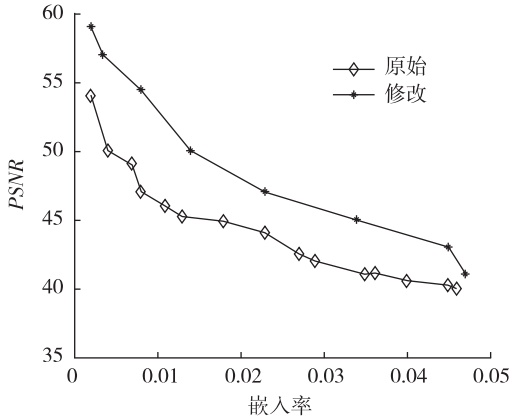


图 7　PSNR 对比分析图

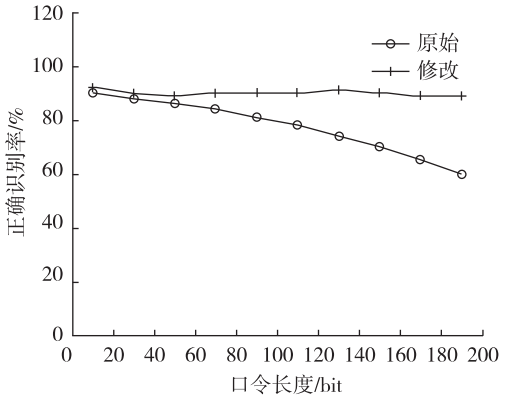


图 8　口令信息的隐藏对指纹匹配率影响

从图 8 中可以看出,与文献[3]的方法相比,本文的信息隐藏方法有较低的修改率,提高了 *PSNR* 峰值信噪比量,并且从图中可以看出,在口令信息嵌入量较大的情况下,本文提出的信息隐藏方法的性能更加显著。从图 8 可以清晰得出,采用本文提出的信息隐藏方法对指纹正确识别率影响较小。

5 总结

本文旨在提供一种身份认证安全方法,针对基于指纹图像为载体的信息隐藏技术为研究对象,提出了一种信息嵌入到指纹图像脊线的方法,该方法将细化后的指纹图像进行单元化处理,解决了信息嵌入到指纹图像像素点的过程中出现的像素点交叉现象,同时避免了因信息(口令、声音或人脸等)嵌入指纹图像后对图像骨架脊线造成的影响,该方法中使用 Hash 函数对可嵌入像素点和口令信息进行分散化处理,提高了口令信息的隐蔽性和安全性。最后,由实验结果可以看出,本文提出的基于单像素指纹边界的信息隐藏技术能够较好地将信息嵌入到指纹图像中,具有较低修改率的同时提高了 *PSNR* 峰值信噪比量,而且与其它方法相比,本文提出的方法对指纹正确识别率影响较小。

参考文献:

[1] Jain A K, Uludag U. Hiding biometric data[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2003, 25(11): 1494-1498.

[2] Vatasa M, Singh R, Noore A. Feature based RDWT watermarking for multimodal biometric system[J]. Image and Vision Computing, 2009, 27(3): 293-304.

[3] Li S, Kot A C. Privacy protection of fingerprint database using lossless data hiding[C]//Proceedings of the 2010 IEEE International Conference on Multimedia and Expo. New York: IEEE Press, 2010: 1293-1298.

[4] Ho Y A, Chan Y K, Wu H C, et al. High-capacity reversible data hiding in binary images using pattern substitution[J]. Computer Standards and Interfaces, 2009, 31(4): 787-794.

[5] Yang H, Kot A C, Pattern-based data hiding for binary image authentication by connectivity-preserving[J]. IEEE Transactions on Multimedia, 2007, 9(3): 475-486.

[6] 胡校成,张卫明,俞能海. 针对指纹模板的可逆信息隐藏编码方法[J]. 中国科学技术大学学报, 2011, 41(7): 576-581.
Hu X C, Zhang W M, Yu N H. The reversible information hiding fingerprint template coding method[J]. The University of Science and Technology of China, 2011, 41(7): 576-581.

[7] 朱宁,施荣华,吴科桦. 一种新的点模式指纹匹配方法[J]. 计算机工程与应用. 2006, 42(5): 74-76.
Zhu N, Shi R H, Wu K H. A new fingerprint point pattern matching method[J]. Computer Engineering and Applications, 2006, 42(5): 74-76.

[8] 汤婷,吴小培,项明. 指纹图像增加与特征提取 [J]. 计算机技术与发展, 2009, 19(1): 81-87.
Tang T, Wu X P, Xiang M. Fingerprint image and feature extraction[J]. Computer Technology and Development, 2009, 19(1): 81-87.

An Information Hiding Technique Based on Fingerprint Boundary of Single Pixel

QIN Qin, LI li

(Department of Computer Science and Engineering, Henan Institute of Engineering, Zhengzhou 451191, China)

Abstract: It is an effective method to improve the security of the identity authentication system by making use of information hiding technology, which integrates user identity information in the fingerprint, face and password with multi-mode authentication to increase authentication security. Password information embedded into the fingerprint images to hide and store the password information, which not only meet the needs of safety certification, but also ensure the safety performance of password storage. This article firstly describes the password information hiding technology that is with fingerprint image as carrier. And then we divided the refined fingerprint images by the pixels cell block, and then mapped the password information to the pixels of the cell center with the hash function, which is equivalent to constitute a binary sparse matrix. This method not only guarantees the quality of the fingerprint image, but also ensures the quality of the fingerprint image skeleton ridge line, to ensure the accuracy of fingerprint identification. Finally, with the experimental results, the information hiding technique based on fingerprint boundary of single pixel proposed in this paper can well embedded information into the fingerprint images, which has lower modified ratio and at the same time proves PSNR. And compared with other methods, the proposed method in this paper has little effect on the fingerprint identification accuracy.

Key words: fingerprint image; refine; password information; embed

(责任编辑 游中胜)