第41卷第7期 中国科学技术大学学报 Vol. 41, No. 7
2011年7月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Jul. 2011

文章编号:0253-2778(2011)07-0576-06

针对指纹模板的可逆信息隐藏编码方法

胡校成,张卫明,俞能海

(中国科学技术大学多媒体计算与通信教育部-微软重点实验室,安徽合肥 230027)

摘要:通过融合指纹、人脸、口令等用户身份信息来进行多模态认证可以提高身份认证系统的安全性.而利用信息隐藏技术,可以将几种身份信息嵌入到某一种生物模板中实现安全存储.本文介绍了一种以指纹模板为隐藏载体的多模态认证技术,该技术的关键问题是要保证嵌入信息后的指纹图片的质量,以确保匹配的精度.为此,提出了一种将二元信息稀疏化的数据嵌入编码方法,利用这种编码可以有效降低数据嵌入过程中对指纹图片的修改,从而改善载密图片的质量,以达到提高匹配精度的目的.该方法嵌入脆弱水印,用于指纹模板的完整性认证.

关键词:指纹模板;信息隐藏;可逆信息隐藏;反零游程编码

中图分类号:TP309.7 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2011.07.002

A lossless data coding and hiding scheme for fingerprint templates

HU Xiaocheng, ZHANG Weiming, YU Nenghai

(*MOE-MS Key Laboratory of Multimedia Computing and Communication, University of Science and Technology of China, Hefei* 230027, *China*)

Abstract: By merging several kinds of user authentication information such as fingerprints, faces, passwords etc., multi-modal authentication can improve the security of traditional identify authentication systems. Furthermore, via data hiding technology, specific user identities can be imbedded into their biologic templates to ensure safe storage. A multi-modal authentication scheme was introduced, which uses fingerprint templates as the cover. The key problem of this technology is to ensure the quality of the template picture after embedding, which is important for the matching precision afterwards. Both theoretical analysis and experimental results demonstrate that by adopting a coding method which increases the sparseness of the original binary data before embedding, modification of the fingerprint template is lowers effectively, thus ensuring the image quality and matching precision. The method embeds fragile watermarks for the integrity authentication of the fingerprint template.

Key words: fingerprint template; data hiding; lossless data hiding; reverse zero run length (RZL) coding

0 引言

近年来,如何基于生物特征(如指纹、声音、人脸等)进行身份认证成为研究热点.该领域的发展趋势之一是:融合多种生物特征(包括口令)进行多模态身份认证来提高认证过程的安全性.信息隐藏技术作为多种生物特征融合的有效方法之一而受到关注[1-2].

收稿日期:2011-04-28;**修回日期**:2011-06-23

基金项目:中国高技术研究发展(863)计划(2008AA01Z117),国家科技重大专项(2010ZX03004-003)资助.

作者简介:胡校成,男,1988年生,硕士生. 研究方向:信号信息处理和计算机视觉. E-mail: hxc@mail.ustc.edu.cn

通讯作者:俞能海,博士/教授. E-mail: ynh@ustc.edu.cn

文献[3]提出了一种基于信息隐藏的多模态身份认证框架:注册阶段,系统保存用户的生物特征模板(譬如指纹),并将其他的身份信息(如口令或人脸特征)加密嵌入到指纹模板中;验证阶段,采集待验证用户的指纹与数据库中预存的指纹模板匹配,匹配成功后再从指纹模板中提取出其他身份信息来进行第二重身份验证.因此,一方面,用户希望在载体模板中嵌入更多的身份信息来提高认证的安全性;另一方面,要尽量保持载体模板的质量,以确保第一重认证过程的匹配精度.

文献[3]中采用指纹模板作为信息隐藏的载体,指纹模板经过细化后保存为具有单像素边界的二值图像.关于二值图像的信息隐藏方法已有很多[4-8],文献[3]针对单像素边界二值图像提出了一种新可逆信息隐藏方法,该方法在提取出嵌入的信息后可以无损恢复原始载体.与其他已有的二值图像信息隐藏方法比,文献[3]的方法更适用于指纹图像,在给定的嵌入率下,可以保持更好的图像质量.另外,这种可逆隐藏方法还可以用来嵌入脆弱水印,作为指纹模板完整性认证和篡改区域定位的工具.

但是,实际应用中的认证系统对认证准确性有非常高的要求,所以作为载体的生物模板需要保持尽可能高的图像质量.为此,本文针对文献[3]中的可逆信息隐藏方法提出了一种数据嵌入的编码算法,该算法可以有效减少信息嵌入过程对载体模板的修改,从而提高图像质量.

文章主要结构分 4 部分:节 1 介绍基于指纹边界的可逆信息隐藏;节 2 提出利用稀疏编码改进的信息嵌入方法;节 3 是实验数据部分的说明和讨论;节 4 进行总结.

1　基于指纹边界的可逆信息隐藏

1.1　消息嵌入原理

和基于块的方法不同,基于指纹边界的可逆信息隐藏[3]对细化过后的二值指纹图像进行逐像素的处理,首先判定每个像素是否可嵌,只有可嵌入的像素点才被选取嵌入信息.每个像素是否可嵌由以它为中心的 3×3 块的连通模式决定.约定当前像素点及其 8 邻域依次用 P_0,P_1,P_2,P_3,P_4,P_5,P_6,P_7,P_8 标记,,如图 1 所示;用"1"表示前景(黑色)像素,"0"表示背景(白色)像素.

定义每个像素 $C(i,j)$的嵌入规则:

$(i-1,j-1)$ 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　单像素及其 8 邻域标记

Fig. 1　Notation of a single pixel and its eight neighbors

$$C(i,j)=\overline{P}_0\cdot\left(\prod_{w=1}^{4}\overline{P}_{2\cdot w-1}\right)\cdot\sum_{w=1}^{4}\left(P_{2\cdot w}*P_{2\cdot w+2}\right) \tag{1}$$

式中,$P_{10}=P_2$;$\overline{P}$是对 P 的逻辑取反.若上式结果 $C(i,j)=1$,则表示像素点 P_0 是可嵌点.简单直观地表示,如图 2 所示共有 4 种可嵌入模式,如果当前像素点 P_0 处于其中一种模式(指纹骨架的边界点),则表示它是可嵌的,否则不可嵌.

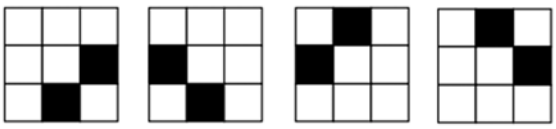


图 2　可嵌入像素点的 4 种模式

Fig. 2　Four patterns satisfy the embeddability criterion

1.2　消息嵌入过程

给定一幅细化后的指纹图像,对于特定长度的待嵌入消息,嵌入过程如下:

①首先从细化后的二值指纹图像中按照一定规则选取像素点,如利用密钥驱动的随机数发生器选择像素点;

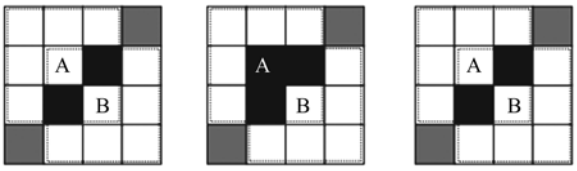
②判断选取像素点的可嵌入性,若其可嵌,则嵌入 1 比特消息;

③重复①到②直到所有消息比特被嵌入.

由图 2 易知,在嵌入消息之前,所有的可嵌入像素点均表示"0"(白色),如果需要嵌入 1 比特"1",只要将相应的像素点翻转成"1"(黑色)即可.值得注意的是,对于可嵌入像素点的修改会影响对应 3×3 块中其他像素点的可嵌入性.例如,如图 3 所示,(a)表示原图中一个 4×4 块中的像素分布,初始时我们知道像素点 A 和像素点 B 都是可嵌入的,假设像素点 A 嵌入消息比特"1",造成 A 像素的修改,这时像素点 B 变得不可嵌入;而当像素点 A 嵌入消息比特"0"后,则像素点 B 依然可嵌.

这样的嵌入过程只是在图 2 所示的 4 种模式上添加一些边界像素,而指纹图像的骨架特征可以保

持得很好.



(a) 初始时像素A和B均为嵌入点 (b) 当像素A嵌入“1”后像素B变得不可嵌入 (c) 当像素A嵌入“0”后像素B仍然可嵌

图 3 数据嵌入说明

Fig. 3 Illustration of data embedding process

1.3 消息提取过程

提取过程分两步,指纹图像重建和数据提取.首先我们的原始图 F 是经过细化处理过的,边界宽度为单像素,不存在像素边界(如图 4 所示的情形).也就是说对于嵌入信息后的指纹图片 T,只要出现图 4 的模式,通过把中心像素点清零,即可恢复原始的指纹图片 F.

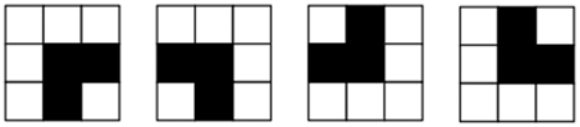


图 4 像素点嵌入比特“1”后的模式

Fig. 4 Pixel patterns after bit “1” embedded

得到重建的原始图片 F 后,通过下面步骤提取嵌入的消息:

①选取于 F 中的某个像素点 $F(i,j)$.

②我们通过式(1)来计算其 $C(i,j)$.如果 $C(i,j)=1$,则从中提取 1 比特消息 $m=T(i,j)$,同时修改 $F(i,j)=T(i,j)$(因为后面像素的可嵌入性依赖于 $F(i,j)$是否被修改过);否则不提取.

③当所有的像素点均被处理后,连接提取的比特即可以得到嵌入的消息.

2 针对指纹边界的消息嵌入编码

我们用嵌入率和修改率评价嵌入方法的性能.嵌入率定义为消息长度与载体图像大小的比值;修改率定义为被修改像素个数与载体图像大小的比值.上面提到的基于指纹边界的信息隐藏方法[3],最大嵌入率可以达到 0.4 以上,对于尺寸为 512×512 的载体,可嵌入的消息长度超过 10^4 比特.因为嵌入的消息通常是加密后的伪随机序列,“1”的比率为 1/2,所以其修改率总是嵌入率的 1/2.而在实际应用中,指纹图像中嵌入的口令信息数据量较小(约 160 比特),即使加入其他用户身份信息,譬如人脸特征等,数据量也可控制在一千到几千比特内,即实际需要的嵌入率较小.而对于较小的嵌入率我们可以通过编码方法降低修改率,从而提高匹配精度.

下面,我们提出一种可以有效降低修改率的数据嵌入编码方法.由于载体指纹图像中的可嵌入点均为“0”,因此我们假设在一条“全零载体”上嵌入消息,为了减少修改,我们要减少在载体上写“1”的比率.

记 N 长全零载体为 $\boldsymbol{x}=(x_1,x_2,\cdots,x_N)$,其中 $x_i=0,1\leqslant i\leqslant N$.待嵌入的二元消息序列记为 $\boldsymbol{m}=(m_1,m_2,\cdots,m_L)$.消息嵌入过程需要使用两个指针,分别记为 $P1$ 和 $P2$,其中 $P1$ 用来标记最后一个被修改的载体的位置,$P2$ 用来标记已嵌入的消息长度.我们提出的编码方法是变率码,其嵌入率由参数 $k(k\geqslant 1)$控制.

2.1 嵌入过程

首先将两个指针置零,即 $P1=0$, $P2=0$.然后读取第 $P2+1$ 个消息比特 m_{P2+1},根据 m_{P2+1}的取值采用两种不同的嵌入方式:

①如果 $m_{P2+1}=0$,令 $P1=P1+2^k$, $P2=P2+1$,这种情况仅一个比特 m_{P2+1}被嵌入,占用了 2^k 个载体,但是没有载体被修改.

②如果 $m_{P2+1}=1$,读取接下来的 k 个消息比特 $(m_{P2+2},\cdots m_{P2+k+1})$,将这个 k 维向量表示成一个十进制整数,记作 D,则 $D\in[0,2^k-1]$.令 $P1=P1+D+1$, $P2=P2+k+1$,并将载体 x_{p1}翻转为“1”.这种情况,$k+1$ 个消息比特$(m_{P2+1},m_{P2+2},\cdots m_{P2+k+1})$被嵌入,占用了 D 个载体,仅有一个载体 x_{p1} 被修改.

对于两种情况,我们都将前 $P2$ 比特消息嵌入到了前 $P1$ 个载体中,接着读取第 $P2+1$ 个消息比特,重复上述步骤,直到消息被全部嵌入或 $N-P1<2^k$.嵌入消息后的载密对象记作 $\boldsymbol{y}=(y_1,y_2,\cdots,y_N)$.

2.2 提取过程

提取消息时,首先令指针 $P1=0$, $P2=0$.以 $P1+1$为起点,在载密对象 $\boldsymbol{y}$ 中连续读取 2^k 个元素 $(y_{P1+1},y_2,\cdots,y_{P1+2^k})$.根据向量$(y_{P1+1},y_{P1+2},\cdots,y_{P1+2^k})$是否包含“1”,分两种情况处理:

①如果$(y_{P1+1},y_{P1+2},\cdots,y_{P1+2^k})$中所有的元素都为“0”,提取第 $P2+1$ 个消息比特 $m_{P2+1}=0$,并令 $P1=P1+2^k$, $P2=P2+1$.

②如果向量$(y_{P1+1},y_{P1+2},\cdots,y_{P1+2^k})$中存在“1”,设第一个“1”出现的位置为 $P1+i$,则整数

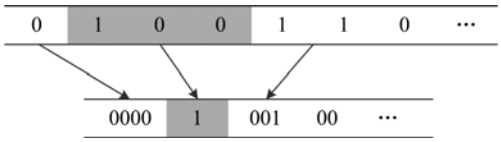
$i-1\in[0,2^k-1]$可以用 k 比特二进制数表示，记为 $(i-1)_{bi}$. 提取第 $P2+1$ 个消息比特 $m_{P2+1}=1$，以及接下来的 k 个消息比特 $(m_{P2+2},\cdots m_{P2+k+1})=(i-1)_{bi}$，然后令 $P1=P1+i$，$P2=P2+k+1$.

以相同的方式在剩余的载体 $(y_{P1+1},\cdots,y_N)$ 提取消息，直到消息长度等于预设的消息长度，或者 $N-P1<2^k$ 并且在最后的 $N-P1$ 载密对象中不存在“1”.

2.3　嵌入和提取过程实例

下面用一个简单的例子说明消息的嵌入和提取过程.

取编码参赛 $k=2$，消息序列和对应的载体修改过程见图 5.



第一行为消息，第二行为修改后的载体

图 5　消息嵌入过程

Fig. 5　Message embedding process

嵌入过程：

Step 1　读到的第一个消息比特为“0”，所以指针后移 4 个位置，不做任何修改.

Step 2　读取第二个比特，为“1”，所以接着读取后续的两个比特“00”，转化为十进制表示“0”，0+1=1，所以指针向后移 1 个位置，并将相应载体修改为“1”.

Step 3　读取下一个消息比特，为“1”，所以接着读取后续的两个比特“10”，转化为十进制表示“2”，2+1=3，所以指针向后移 3 个位置，并将相应载体修改为“1”……

提取过程：

Step 1　从载密序列中读取连续 4 个符号，发现前四个符号不包含“1”，所以提取一个消息比特“0”，并将指针指到位置 4.

Step 2　从第 5 个位置开始读取连续 4 个符号，发现包含符号“1”，所以先提取一个消息比特“1”；因为“1”出现在连续 4 个符号的第 1 个位置上，计算 1-1=0，0 的二进制表示为“00”，所以再提取两个消息比特“00”，并将指针后移 1 位，指到第 5 个位置.

Step 3　从第 6 个位置开始读取连续 4 个符号，发现包含符号“1”，所以先提取一个消息比特“1”；因为“1”出现在连续 4 个符号的第 3 个位置上，计算 3-1=2，2 的二进制表示为“10”，所以再提取两个消息比特“10”，并将指针后移 3 位，指到第 8 个位置……

3　实验结果

图 6 所示为 5 幅 512×480 的二值细化指纹图像，这 5 幅图像代表了主要的指纹图像类别：tented arch，arch，right loop，left loop 和 whorl[10]. 我们以这几张图片为载体，用文献[3]的方法和本文的编码方法嵌入消息，考察各种嵌入率对应的修改率和峰值信噪比(PSNR)指标. 二值图像 PSNR 值利用下面的公式(2)和(3)计算：

$$\mathrm{MSE}=\frac{1}{\mathrm{M}\times\mathrm{N}}\sum_{i=1}^{M}\sum_{j=1}^{N}(b_{ij}-b'_{ij})^2\times 255 \quad (2)$$

$$\mathrm{PSNR}=10\log_{10}\frac{(255)^2}{\mathrm{MSE}}\mathrm{dB} \quad (3)$$

式中，M，N 为图像的宽和高；b_{ij} 和 b'_{ij} 为原始图像和载密图像对应的像素值.

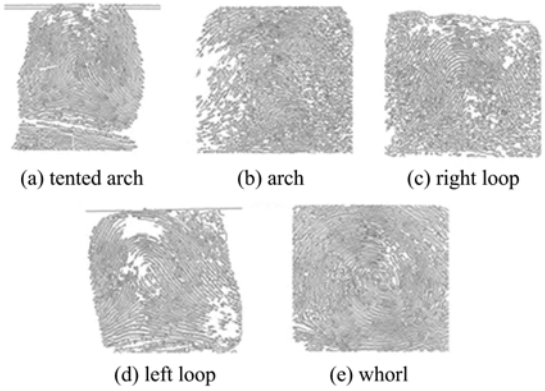


图 6　5 种指纹图像模板

Fig. 6　Five fingerprint image templates

在试验中，编码参数 k 分别取 0，1，2，3，4，5，6，7. 其中 $k=0$ 表示非编码的情况，即嵌入率最大的情况. 如图 7 所示，随着 k 值增大，编码对应的嵌入率减小. 码的嵌入率是离散分布的，我们可以通过组合不同参数的码来得到连续的嵌入率. 比如在图 7(a)中，$k=0$ 时编码嵌入率为 0.042，$k=1$ 时嵌入率为 0.038，若所需嵌入率在 0.038 和 0.042 之间，可以将消息分成两部分，一部分采用 $k=1$ 的码嵌入，另一部分采取 $k=2$ 的码嵌入，从而既达到了容量要求，又保持了较小的修改率和较大的峰值信噪比.

除了与文献[3]的原始方法比较，我们还与文献[9]中的编码方法做了比较试验. 文献[9]提出的是一种以视频为载体的可逆信息隐藏方法，但其本质上也是在一全零载体上嵌入消息，为了减少修改，文

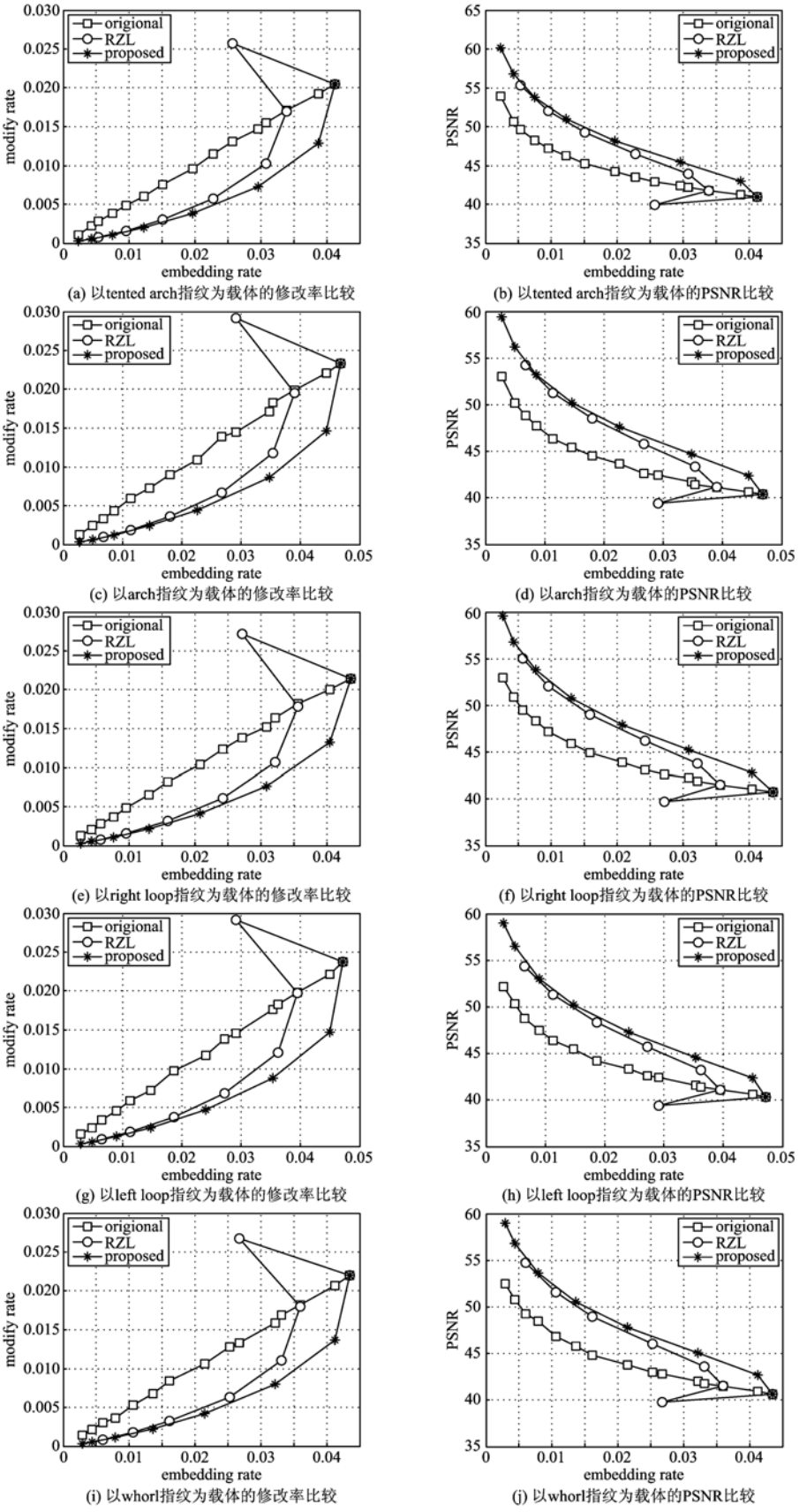


图 7　以 5 种指纹图片为载体,对 3 种嵌入方法的修改率和 PSNR 的比较

Fig. 7　Modify rate and PSNR comparison of three embedding schemes on the five fingerprint templates

献[9]提出了“reverse zero run length(RZL)”编码.本文的方法可以看成是对 RZL 编码的改进.

如图 7 所示,与文献[3]的方法比,对于各种指纹图像,RZL 编码[9]和本文的编码方法都可以有效降低修改率,从而提高峰值信噪比.但是本文的编码方法较之 RZL 编码修改率更低,尤其是对嵌入率较大的情况,改进尤为显著.

另外,我们在指纹图像 tented arch 模板中,用 3 种嵌入方法分别均匀嵌入7 000比特消息(表 1),然后比较载密图像的视觉差异.对比放大之后的图片(图 8)可以看出,文献[3]中的原始嵌入方法在指纹图像的边界处产生了许多拐角,使用 RZL 编码可以使拐角减少,而本文的编码方法增加的拐角最少,因而与载体图匹配的效果最好.

表 1　均匀嵌入 7000 比特消息时不同嵌入方法对载体修改率对比结果

Tab. 1　Cover modify rate comparison of different schemes while 7000 bit message embedded evenly

	载体修改率
原始嵌入方法	0.014 4
RZL 嵌入方法	0.014 2
改进的嵌入方法	0.007 1

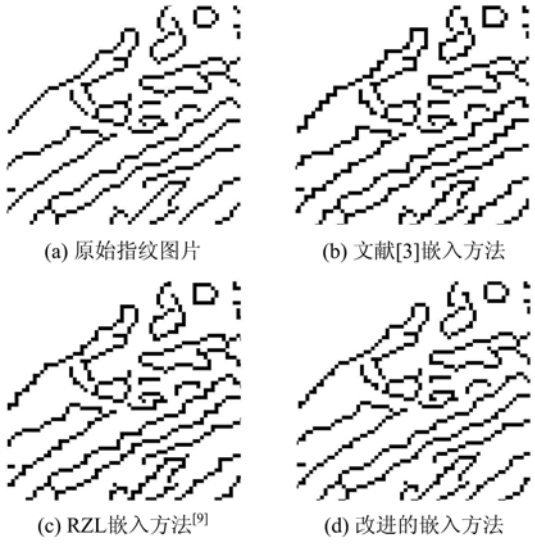


图 8　以 tented arch 指纹模板为载体,用 3 种方法嵌入 7000 比特消息后图像的放大视觉质量对比

Fig. 8　Magnified visual quality comparison of three embedding schemes on the tented arch fingerprint template with a 7000 bit embedding length

4　结论

本文针对一种基于指纹边界的可逆信息隐藏的方法,提出了一种信息嵌入编码算法,该算法可以显著减少嵌入过程对载体的修改,从而提高载密图像的质量.将本文方法应用于基于指纹的多模态认证系统,可以提高指纹匹配的精度,保证认证的准确性.

然而,本文提出的信息嵌入方法在减小载体修改率的同时,使得嵌入方法容错能力有一定的下降,较少的比特位的错误有可能导致后面一连串比特位提取出错.在后续的工作中,我们将考虑结合冗余校验和纠错编码方法来提升嵌入编码的容错能力.

参考文献(References)

[1] Jain A K, Uludag U. Hiding biometric data[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2003, 25(11): 1 494-1 498.

[2] Vatsa 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, 2010:1 293-1 298.

[4] Wu M, Liu B. Data hiding in binary image for authentication and annotation[J]. IEEE Transactions on Multimedia, 2004, 6(4): 528-538.

[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] Yang H, Kot A C. Orthogonal data embedding for binary images in morphological transform domain-a high-capacity approach [J]. IEEE Transactions on Multimedia, 2008, 10(3): 339-351.

[7] HoY 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.

[8] Xuan G, Shi Y Q, Chai P, et al. Reversible binary image data hiding by run-length histogram modification [C]//Proceedings of the 19th International Conference on Pattern Recognition. New York: IEEE Press, 2008: 1-4.

[9] Wong K, Tanaka K, Takagi K, et al. Complete video quality-preserving data hiding[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2009, 19(10):1 499-1 512.

[10] Candela G T, Grother P J, Watson C I, et al. A pattern level classification automation system for fingerprints: NIS-TIR 5647 [R]. NIST, 1995.