基于内容的多模态可逆密写方法

齐 妙 代江艳 王建中 于晓熹 张 明
(东北师范大学计算机科学与信息技术学院 长春 130117)
(智能信息处理吉林省高校重点实验室 长春 130117)

摘 要 为了提高生物认证信息在网络传输过程中的安全性,提出一种基于内容相关性分析的多模态双重可逆密写方法。与现存大多数方法不同,为了充分利用载体图像丰富的内容和提高方法的隐藏性能,首先采用最小二乘回归方法分析掌纹图像与人脸图像之间的内容相关性,即用人脸图像表示掌纹图像,未被表示的部分掌纹图像被嵌入到相应的人脸图像中,另外,重构系数作为密钥存储;然后,为了不引起攻击者的注意,将得到的含密人脸图像嵌入到随机选取的自然载体图像中;最后,将得到含有掌纹信息和人脸信息的含密图像进行传输。提出的方法实现了生物认证信息的双重可逆信息隐藏,而且哈希函数和密钥的使用提高了该方法的安全性。大量实验结果表明该,方法具有很好的安全性、不可见性和很高的嵌入容量。特别地,采用双重隐藏机制进一步增强了生物认证信息的安全性,确保了多模态生物认证的有效性。

关键词 密写,内容相关,双重可逆信息隐藏,多模态生物认证
中图法分类号 T391.4 **文献标识码** A

Content-based Reversible Steganographic Method for Multimodal Biometrics

QI Miao DAI Jiang-yan WANG Jian-zhong YU Xiao-xi ZHANG Ming
(School of Computer Science and Information Technology, Northeast Normal University, Changchun 130117, China)
(Key Laboratory of Intelligent Information Processing of Jilin Universities, Changchun 130117, China)

Abstract A novel dual reversible steganographic method based on content correlation analysis is proposed for enhancing the security of biometric information transmitted in the network. Different from the existing approaches, in order to make good use of abundant content of the cover image and improve the performance of data hiding, least square (LS) regression method was adopted to exploit the content correlation between the palm image and the face image firstly. In other words, the face image was used to represent the palm image, and the unrepresented part of the palm image was embedded into the corresponding face image. Besides, the reconstruction coefficients were taken as the secret key for security. Then, the stego-face image was hidden into a nature cover image by the same method for causing much less attention of attackers randomly. Finally, the stego-cover image containing palm information and face information were transmitted. The presented method realizes dual reversible data hiding for biometrics and its security is also employed with a hash function and a secret key. The proposed method exhibits good security, invisibility and high capacity. Specially, dual reversible data hiding further improves the security of transmitted biometric information and ensures the validity for multimodal biometric identification.

Keywords Steganographic, Content correlation, Dual reversible data hiding, Multimodal biometric identification

1 引言

近年来,随着现代通信技术的飞速发展和计算机互联网技术的迅速普及,生物认证作为一种准确而且可靠的认证识别技术得到广泛的应用。生物认证信息,例如掌纹、人脸、数字签名、语音和虹膜等的信息量很大,其在传输过程中极易引起网络攻击者的怀疑,因此很容易遭到攻击者的仿制和攻击。如果生物认证信息在传输过程中遭到拦截,攻击者可能会更改生物认证信息的内容或滥用拦截到的生物认证信息进行非法活动,这样就会严重影响生物识别系统的安全性、准确性和可靠性,进而威胁到生物认证信息所有者的生命财产安全。Schneier[1]指出只有保证生物认证数据的有效性,才能使生物认证系统正常工作。所以,保证生物认证信息在网络传输过程中的完整性和安全性是亟待解决的问题。

到稿日期:2012-02-01 返修日期:2012-04-30 本文受吉林省科技发展计划项目青年科研基金(201201070,201201063),东北师范大学校内青年基金(10QNJJ004),吉林大学符号计算与知识工程教育部重点实验室项目(93K172012K13)资助。

齐 妙(1981—),女,博士,讲师,主要研究方向为信息安全、生物认证,E-mail:qim801@nenu.edu.cn;代江艳(1985—),女,博士生,主要研究方向为信息安全、模式识别;王建中(1981—),男,博士后,讲师,主要研究方向为模式识别;于晓熹(1987—),女,硕士生,主要研究方向为信息安全、模式识别;张 明(1978—),女,博士,讲师,主要研究方向为计算机图形图像处理。

目前，国内外许多研究学者已经提出了一些信息隐藏方法来保护生物认证信息的安全性和完整性，例如水印和密写方法[2-6]。其中一类方法是采用数字水印的思想将水印嵌入到生物认证图像中或者直接将一个或多个生物特征隐藏到另外的生物认证图像中。文献[2]分别使用了4种现有的水印方法，将虹膜编码嵌入到灰度人脸图像中，实现了多模态生物认证，并通过人脸和虹膜的认证准确率和鲁棒性评价了每种方法的性能。文献[3]结合DWT和LSB方法将人脸模板嵌入到灰度指纹图像中，该方法能够抵抗几何攻击和频域攻击，保护了人脸模板和指纹图像的完整性。文献[4]介绍了一种多模态生物图像水印方法，该方法通过隐藏的拇指特征分别对人脸和指纹进行安全性和完整性验证。这类方法虽然能够抵抗某些类型的攻击但隐藏的容量并不大，而且其使用生物认证图像作为载体，极易遭到拦截甚至破坏。另一类方法引进密写的思想，将秘密信息隐藏到不引人注意的载体中。为了提高传输过程中的安全性，文献[5]将生物数据嵌入到3种不同类型的载体图像中来分散攻击者的注意力。文献[6]首先使用生物密钥对虹膜模板进行加密，然后使用DWT方法将其隐藏到不相关的载体图像中。实验结果表明这些方法虽然取得了很好的不可见性和鲁棒性，但是载体承载容量不高。

现有的多模态信息隐藏方法中，大多数都是将一个或多个生物认证信息嵌入到另一幅生物认证图像或自然场景图像中，嵌入容量并不大，而且，这些方法是不可逆的。也就是说，它们不能完全恢复载体图像。在嵌入过程中，这些方法可能改变宿主生物认证图像固有的特征，以致影响生物认证系统的性能。因此，若隐藏方法不能完全恢复宿主的生物认证图像，则会阻碍进一步的认证工作。为了克服这个弊端，许多学者集中研究了可逆的信息隐藏方法[7-11]，这类方法主要用于医学图像、军事图像、遥感图像以及法律认证图像等的完整性和真实性认证。例如，文献[8]基于扩差法，提出了一种大容量的可逆信息隐藏方法，用于医学图像的内容认证。

综上所述，大多数信息隐藏方法都是直接将秘密信息隐藏到载体图像中，载体图像的冗余信息并没有得到充分的利用，导致载体承载容量不高。特别地，现有的生物认证图像隐藏方法多数以生物信息作为传输载体而且不可逆，其很容易引起攻击者的注意，而且不能保证载体生物认证信息的完整性。为了提高生物认证系统的安全性和信息隐藏的容量，本文提出了一种基于内容相关的多模态可逆隐藏方法，即使用可逆的密写方法保护待传输的多模态生物认证图像。在发送端，对于给定的一对多模态图像（本文以掌纹和人脸图像为例），首先使用最小二乘（Least Square，LS）回归方法对掌纹图像和对应的人脸图像进行相关性分析，即用人脸图像的内容表示掌纹图像，不能被表示的掌纹图像作为秘密图像，并采用文献[10]提出的隐藏算法将其嵌入到人脸图像中；然后，将得到的含密人脸图像使用相同的方法隐藏到不易引人注意的自然场景的载体图像中；最后，将得到的含密载体图像通过网络进行传输。在接收端，首先通过执行嵌入过程的逆过程实现含密人脸图像的提取和载体图像的恢复；然后提取秘密图像，并利用恢复的人脸图像重构掌纹图像来产生完整的掌纹图像；最后，使用得到的掌纹图像和恢复的人脸图像进行多模态生物认证。大量的实验表明，在相关分析过程中，掌纹图像的大部分内容能够被人脸图像所表示，即人脸本身隐含了掌纹图像的大量信息。不见性和隐藏容量的对比结果显示，本文提出的方法具有更好的隐藏性能；而且，通过双重的信息隐藏可进一步提高生物信息的安全性，实现对网络传输中的多模态生物信息的完整性保护，保证生物认证的有效性和可靠性。

本文第2节详细地描述方法；第3节给出实验结果及分析；最后总结全文。

2 基于内容相关性的可逆密写方法

本文将掌纹图像和人脸图像作为秘密传输的生物认证图像，隐藏的目的是保护它们的完整性和安全性，保证多模态生物认证的有效性。本文提出的基于内容的可逆密写方法流程如图1所示。

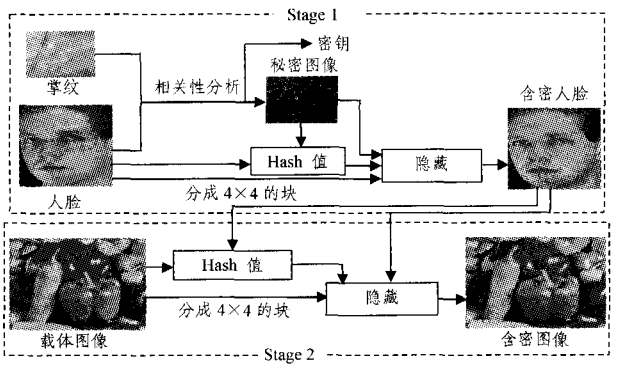

图1 基于内容的可逆密写方法流程图

2.1 相关性分析

为了提高信息隐藏性能，文献[12]采用回归的方法分析了生物认证信息和宿主的相关性，即利用宿主图像的丰富信息表示生物认证图像。鉴于相关分析的优势，本文对掌纹图像和人脸图像进行相关分析以提高嵌入的隐藏性能。给定一幅掌纹图像 P $(m\times n)$ 与其对应的人脸图像 F $(M\times N)$，相关性分析的过程如下：

第1步 将掌纹图像 P $(m\times n)$ 分成不重叠的大小为 $m_1\times n_1$ 的块，并将每一块重新排列成一个列向量，则 $P_B=\{p_1,\cdots,p_{t1}\}$，$t1=1,\cdots,\lfloor m/m_1\rfloor\times\lfloor m/n_1\rfloor$。

第2步 将人脸图像 F $(M\times N)$ 分成大小为 $m_1\times n_1$ 的不重叠的块，并将每一块重新排列成一个向量，则有 $F_B=\{f_1,f_2,\cdots,f_{t2}\}$，$t2=1,\cdots,\lfloor M/m_1\rfloor\times\lfloor N/n_1\rfloor$。

第3步 采用LS回归方法建立回归模型：

$$Y=F_BA,A=(F_B^TF_B)^{-1}F_B^TY \tag{1}$$

式中，A 为重构系数，Y 表示重构的掌纹图像。

第4步 残差掌纹图像 E 计算如下：

$$E=P-Y \tag{2}$$

本文方法中，残差掌纹图像 E 作为一部分秘密信息嵌入，第3步得到的重构系数 A 作为密钥存储。该密钥具有很高的安全性，即对于攻击者来说，密钥是不可预测的，并且很难被破译。图2给出了相关性分析的结果，由图2(c)可见，重构的掌纹图像拥有原始掌纹图像的大部分能量，而秘密图像（图2(d)）的所有像素值都很小，这意味着残差图像的能量比原始掌纹图像低很多。为了可视化残差图像 E，图2(d)显示的是 E 的绝对值放大8倍的形式。

(a) 原始人脸图像　(b) 原始掌纹图像　(c) 重构的掌纹图像　(d) 由(b)和(c)得到的残差图

图 2　相关分析的结果

2.2　秘密信息生成

2.2.1　额外信息

为了验证接收到的图像的真实性和完整性，需要嵌入额外信息。本文采用 Hash 函数生成额外信息。Hash 函数具有很强的敏感性，任何输入的变化都会导致强烈的输出变化。利用这一特性检测接收到的含密图像是否被篡改。得到的二进制 Hash 值 H 的长度为 32 比特。

2.2.2　残差掌纹图像转换

如 2.1 节所述，残差掌纹图像作为秘密信息被嵌入到人脸图像中(图 1 中的 Stage 1)。为了方便嵌入，将残差图像转换成二进制序列。根据大量实验统计分析，残差图像中所有像素值的绝对值都小于 31，因此，秘密图像的每个像素都可以用 6 位二进制位表示，其中第 1 位是符号位，其它 5 位是数值位。如果像素值是负数，符号位置为 1，否则置为 0。这样得到的待隐藏的二进制序列 B_1 长度为 $m\times n\times 6$。

2.2.3　含密人脸图像转换

为了保证生物认证图像在网络传输过程中的安全性，由图 1 虚线框中的 Stage 2 可知，需要将含有掌纹差图像的人脸图像进一步隐藏到不引人注意的载体图像中。同样地，将含密人脸图像中的每个像素用 8 位二进制位表示，则大小为 $M\times N$的图像经过变换后得到的一个二进制序列 B_2 的长度为$M\times N\times 8$。

2.3　秘密信息的嵌入

在发送方，采用双重嵌入策略，秘密信息的嵌入分为两个阶段：第一阶段是将掌纹差图像和人脸图像得到的 Hash 值 H_1 与掌纹差图像的二进制序列 B_1 嵌入到人脸图像中，得到含密人脸图像；第二个阶段是将含密人脸图像与自然场景的载体图像得到的 Hash 值 H_2 与含密人脸图像的二进制序列 B_2 嵌入到该自然场景载体图像中，最终得到含密图像。根据文献[10]的思想，得到本文的嵌入算法，详细描述如下：

第 1 步　将人脸图像 F 分成大小为 4×4 的无重叠的块 $F\_Block=\{F_1,F_2,\cdots,F_{num}\}$，根据预先定义的阈值 T 以及各块的方差，判断各个块的嵌入容量参数 k。

第 2 步　使用 Hash 函数对掌纹差图像 E 和人脸图像 F 进行操作，得到 Hash 值 H_1。

第 3 步　通过下面的公式将二进制序列 S_1(包括 B_1 和 H_1)嵌入到人脸图像中，得到含密人脸图像 F'。以第 i 个块 F_i 为例：

$$\begin{cases} y_{i0}=kq_{i0}-a_{h,k}(F_i) \\ y_{i1}=kq_{i1}-a_{h,k}(F_i)+w_1 \\ \quad\cdots\cdots \\ y_{ih}=kq_{ih}-a_{h,k}(F_i)+w_h \end{cases} \tag{3}$$

$$a_{h,k}(F_i)=\left\lfloor \frac{2(k-1)\sum_{j=0}^{h}q_{ij}+(k-1)h}{2(h+1)} \right\rfloor$$

式中，$F_i=(q_{i0},q_{i1},\cdots,q_{ih})\in Z$ 为图像块 F_i 中的像素值，$S_1=(w_1,\cdots,w_n)\in Z_2$ 表示待嵌入的秘密信息，$F_i'=(y_{i0},y_{i1},\cdots,y_{ih})\in Z$ 表示嵌入秘密信息后的图像块 F_i'，本文 h 取 15。

第 4 步　使用 Hash 函数对含密人脸图像 F' 和自然载体图像 C 进行操作，得到 Hash 值 H_2。

第 5 步　采用第 3 步中的嵌入方法将二进制序列 S_2(包括 H_2 和 B_2)嵌入到自然载体图像 C 中，得到最终的含密图像 C'。

2.4　秘密信息的提取和认证

在接收方，接收到的含密图像是不引人注意的自然场景图像，保证了其在传输过程中的安全性。秘密信息的提取过程是嵌入过程的逆过程，而且不需要原始载体图像的参与。与秘密信息的嵌入过程相对应，在接收方，秘密信息的提取也分为两个阶段。第一个阶段，通过接收到的含密图像，可以得到含密人脸图像的二进制序列 B_2'和 Hash 值 H_2'，同时还可以得到恢复的自然载体图像；为了验证提取的内容的完整性，首先将 B_2'转换成相应的含密人脸图像 F'，然后使用 Hash 函数对 F'和恢复的自然图像进行操作，得到新的 Hash 值 H_2''，通过比较 H_2'和 H_2''验证含密图像在网络传输过程中是否遭到破坏。如果它们匹配成功，则表明提取的秘密信息是真实的；否则，认为含密图像遭到了破坏，要求发送方重新发送图像。第二个阶段的提取和认证过程与第一个阶段类似。最后，利用密钥和恢复的人脸图像得到重构的掌纹图像，并和掌纹差图像相加得到掌纹图像与恢复的人脸图像，进行多模态生物认证。

3　实验与分析

本文在多模态生物认证图像数据库上进行实验，通过不可见性和认证的准确性来测试该方法的性能。

3.1　实验数据

本文使用 Olivetti 实验室(ORL database http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html)的人脸数据库和香港理工大学(http://www4.comp.polyu.edu.hk/ _biometrics)的 PolyU 掌纹数据库建立了一个多模态人脸-掌纹数据库。实验中，使用来自 ORL 数据库中 40 个人的 400 幅人脸图像对本文的方法进行测试，图像大小是 160×140。每个人有 10 幅图像，其中 5 幅用来训练，其他 5 幅作为秘密信息传输。与人脸数据库相一致，从 PolyU 掌纹数据库中随机地选择 40 个人的 400 幅掌纹图像，每人 10 幅图像，图像大小为 32×32。训练与测试的样本数目与人脸图像相同。另外，假设与人脸图像相对应的掌纹图像是来自同一个人的。多模态生物认证的部分图像如图 3 所示。图 3(a)是取自 ORL 数据库中的 6 个人的人脸图像，图 3(b)是对应于图 3(a)中的 6 个人的掌纹图像。

(a) ORL数据库

(b) PolyU数据库

图 3　部分多模态生物认证图像

在本文中，由于生物认证图像的信息量比较大，因此，选用纹理比较丰富的且与生物认证图像无关的自然场景图像[13,14]作为载体图像，如图 4 所示。

(a) Lena　(b) F16　(c) Pepper

图 4　载体图像(512×512)

3.2　性能评估

本文从安全性、不可见性和隐藏容量 3 个指标评估算法的性能。

3.2.1　安全性评估

首先，将多模态生物认证信息隐藏到不易引起注意的宿主中来分散攻击者的注意。

其次，相关分析后将部分的掌纹图像作为秘密信息传输在网络中，即使被提取出来也不能作为有效数据进行非法活动。

最后，采用双重的隐藏策略进一步地提高了该算法的安全性。

3.2.2　不可见性评估

在本小节的实验中，使用峰值信噪比(PSNR)对提出的方法的不可见性进行评估。通常，认为 PSNR 高于 30dB 时，秘密图像具有较好的不可见性。由于本文的方法分为两个阶段：实现掌纹差图像和含密人脸图像的隐藏，因此，在分析图像的不可见性和隐藏容量时，也从这两个阶段分别进行分析。

在 Stage 1 中，本文用两种方法的对比实验证明了所提方法的有效性和优越性。一种是提出的基于内容相关性的可逆密写方法(称为实验 1)，另一种是未使用相关性分析直接将含密人脸图像隐藏到载体图像中(称为实验 2)。也就是说，在实验 2 中没有考虑掌纹图像和人脸图像之间的内容相关性，其隐藏过程与实验 1 相同。

图 5 给出了 Stage 1 中两种方法的 PSNR 值对比结果。从图 5 可以看出，这两种方法的 PSNR 值都高于 35dB，这表明两种方法都具有很好的不可见性。经过统计对比，实验 1 中 200 幅含密人脸图像的 PSNR 平均值是 37.1903dB，比实验 2 中的 PSNR 高约 1dB。

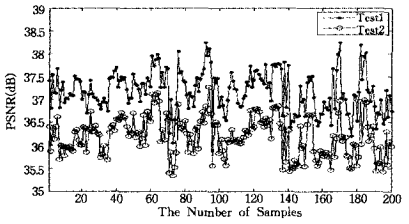

图 5　人脸图像的 PSNR 对比结果

本方法在 Stage 1 中优越的不可见性归因于基于内容的相关性分析。作为相关性分析的结果，秘密图像的能量平均比原始掌纹图像低 35 倍左右，而且秘密图像的大部分二进制序列位的值为 0。因此，在隐藏过程中，改变的像素值的数目很少。此外，实验 1 的隐藏容量比实验 2 少 2/8，因为实验 1 中掌纹原图像的大部分信息由人脸图像承载，剩余的部分信息只用 6 位二进制位表示即可。实验表明，本方法在不可见性和隐藏容量之间做了很好的折中。

在 Stage 2 中，从 3 幅载体图像中随机选择一幅作为传输含密人脸图像的载体，由于在这一阶段的隐藏过程中并没有使用相关性分析，而且两种方法的隐藏容量相同，因此，这两种方法得到的 PSNR 值几乎没有差异。统计实验结果得出，3 种含密载体的 PSNR 平均值为 34.42dB。

此外，为了评价在 Stage 2 中隐藏方法的不可见性，使用实验 3(直接将掌纹图像和人脸图像嵌入到载体图像中)与实验 1 进行了对比，见表 1。可见，本文的方法具有较好的不可见性。

表 1　实验 1 和实验 3 的不可见性比较

	实验 1	实验 3
载体图像大小(像素)	512×512	512×512
平均 PSNR (dB)	34.42	34.26

3.2.3　隐藏容量

含密图像的嵌入容量计算方法如下：

$$bpp=\frac{N_s}{M_c\times N_c} \tag{4}$$

式中，N_s 是嵌入的秘密信息的二进制位数，$M_c\times N_c$ 是载体图像的大小，bpp 表示每个像素嵌入的二进制位数的比特率。

在嵌入容量方面，本小节与经典方法进行了对比。由表 2 可知，该方法中载体的嵌入容量明显高于其它 3 种方法。

表 2　嵌入容量比较

	载体 (Pixel)	秘密信息(Bit)	位/像素(bpp)
Vatsa et al.[2]	1024×768	1000	0.0013
Vatsa et al.[3]	512×512	16384	0.0625
Shih et al.[16]	512×512×3	86016	0.1094
本文方法	512×512	185408	0.7073

对于隐藏内容相同的情况下，本文提出的双重隐藏方法需要的载体比直接隐藏方法所需载体的尺寸更小。下面以图 2 中的一对人脸和掌纹图像为例(图 2(a)和(b))，分析实验 1 和实验 3 在嵌入这组相同的秘密图像的情况下所需要的载体大小，具体如表 3 所列。可见，这两种方法中，相同的嵌入容量需要的载体大小不同，即不同的载体承载的嵌入容量不同。表 3 说明实验 1 需要较小的载体图像即可实现秘密信息的嵌入，载体图像的减小可降低网络传输中的网络负载，提高网络传输性能。

表 3　相同嵌入容量所需载体大小的比较

载体	实验 1	实验 3
Lena	420×420	430×430
F16	388×388	396×396
Pepper	424×424	432×432

3.3　真实性认证和多模态生物认证

多模态生物认证是融合人脸和掌纹的认证结果的一种综合评价指标，通过多模态生物认证结果评价本文方法的性能。实验中，采用局部线性判别嵌入(LLDE)[15]算法提取人脸图像的特征，使用二维主成分分析(2DPCA)[16]提取掌纹图像的特征。在决策阶段，使用最小距离规则(MDR)[17]决定一对人脸和掌纹图像的类别，MDR 定义如下：

$$S_i=\min_{t=1}^{n}(F_t^i)/\max_{j=1}^{n\times N}(F_j)+\min_{t=1}^{n}(P_t^i)/\max_{j=1}^{n\times N}(P_j),i=1,\cdots,N \tag{5}$$

式中，S_i 的最小值表示训练样本和测试样本之间的最大相似性，F_t^i 表示第 i 个人的第 t 个特征向量使用曼哈顿距离的人

脸匹配得分，N 是样本总数，P_i^j 表示掌纹的匹配得分。

在网络传输的过程中，生物认证图像的安全性和完整性是进行有效生物认证的重要保证，一旦在传输过程中遭受到攻击，识别的准确性就会受到影响。

为了保证生物认证图像的有效性，本文在进行生物认证之前对接收的含密图像进行验证。例如，在发送端，将残差掌纹图像和原始人脸图像输入到 Hash 函数，得到的二进制序列作为额外信息嵌入到人脸图像中。在接收端，使用 Hash 值实现对含密人脸图像的认证。首先，从含密人脸图像中提取秘密信息恢复原始人脸图像，然后由提取的残差图像和恢复的人脸图像生成新的 Hash 值，最后比较提取的和新生成的两组 Hash 值。如果它们匹配成功，则说明接收到的含密图像是真实的，可以进一步进行生物认证；否则，要求发送端重新发送含密图像。在本实验中，接收端接收到的图像在没有受到任何攻击的情况下，多模态生物认证的识别率为 99.5%。

图 6 举例说明对接收端接收到的图像进行内容认证的过程。图 6 中，(a)和(b)分别是原始载体图像和含密人脸图像，(c)是含密载体图像，(d)和(e)分别为从(c)中提取的含密人脸图像和恢复的载体图像，(h)是对(c)进行篡改后得到的图像，提取的含密人脸图像和恢复的载体图像分别如(i)和(j)所示。从图 6 可以看出，在没有攻击的情况下，发送方嵌入的 Hash 值与接收方得到的 Hash 值是一致的，这表明接收方接收的图像的内容是真实的；然而，接收方接收的图像遭到很小的篡改之后(如图 6(h)所示)，发送方生成的 Hash 值与接收方得到的 Hash 值显示出明显的差异，这说明接收到的含密图像在传输过程中遭到了攻击，接收到的图像内容是不真实的。进一步地，接收方提取的含密人脸图像和恢复的载体图像也不是真实的，也就没有必要对含密人脸图像中的秘密信息进行提取。为了保证接收的含密图像的真实性和完整性，发送方需重新发送含密图像。

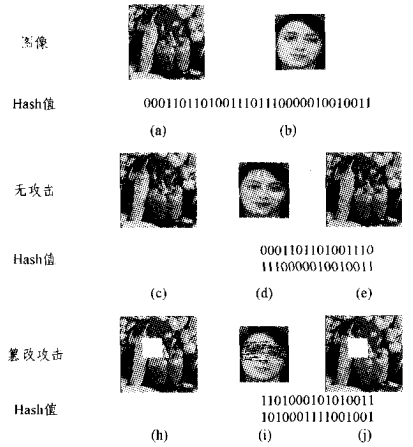

图 6　内容认证举例

结束语　本文提出了一种基于内容的可逆密写方法保护传输的多模态生物认证信息的安全性。在本方法中，最小二乘回归方法对掌纹图像和对应的人脸图像进行相关性分析，目的是充分利用人脸图像丰富的信息尽可能地对掌纹图像进行表示，提高隐藏的性能。作为相关性分析的结果，带有很少能量的残差图像作为秘密信息嵌入到人脸图像中。为了进一步提高生物认证图像传输的安全性并降低其在网络传输中的复杂性，采用双重隐藏机制，将得到的含密人脸图像随机地隐藏到不引人注意的自然载体图像中，以提高最终传输内容在网络中的安全性。此外，由于传输载体的随机选择性和重构系数的复杂性，使得密钥具有很高的秘密性并且很难被破译。而且，通过相关性分析，掌纹图像被分成两部分进行安全传输：主能量部分(使用密钥和载体图像重构的图像)和残差部分(秘密图像)。攻击者得到其中的任何一部分都无法进行犯罪活动。特别地，本文从安全性、不可见性和隐藏容量 3 个指标评价了所提算法的有效性和可行性，大量的实验结果说明了提出的方法能够实现对多模态生物认证信息的安全保护。

参 考 文 献

[1] Schneier B. The Uses and Abused of Biometrics[J]. Comm. ACM, 1999, 42: 136

[2] Vatsa M, Singh R, Mitra P, et al. Comparing robustness of watermarking algorithms on biometrics data[C]// Proceedings of the Workshop on Biometric Challenges from Theory to Practice-ICPR Workshop. 2004: 5-8

[3] Vatsa M, Singh R, Noore A, et al. Robust biometric image watermarking for fingerprint and face template protection[J]. IEICE Electronics Express, 2006, 3(2): 23-28

[4] Kim W, Lee H K. Multimodal biometric image watermarking using two-stage integrity verification[J]. Signal Processing, 2009, 89: 2385-2399

[5] Jain Anil K, Umut U. Hiding Biometric Data[J]. IEEE Transaction on pattern anslysis and machine intelligence, 2003, 25: 1494-1498

[6] Khan M K, Zhang J S, Tian L. Chaotic secure content-based hidden transmission of biometric templates[J]. Chaos, Solitons and Fractal, 2007, 32: 1749-1759

[7] Chang C C, Kieu T D. A reversible data hiding scheme using complementary embedding strategy[J]. Information Sciences, 2010, 180: 3045-3058

[8] Al-Qershi Q M, Khoo B E. High capacity data hiding schemes for medical images based on difference expansion[J]. The Journal of Systems and Software, 2011, 84: 105-112

[9] Kim K S, Lee M J, Lee H Y, et al. Reversible data hiding exploiting spatial correlation between sub-sampled images[J]. Pattern Recognition, 2009, 42: 3083-3096

[10] Peng Fei, Li Xiao-long, Yang Bin. Adaptive reversible data hiding scheme based on integer transform[J]. Signal Processing, 2012, 92: 54-62

[11] 曾宪庭，李卓，平玲娣. 基于块参照像素的无损信息隐藏算法[J]. 计算机科学，2012，39(2)：47-51

[12] Qi Miao, Dai Jiang-yan, Shi Yan-jiao, et al. Video Hiding Method based on Regression and Visual Attention Model for Secure Face Identification[J]. ICIC Express Letters, 2011, 5(10): 3701-3706

[13] Chan C K, Cheng L M. Hiding data in images by simple LSB substitution[J]. Pattern Recognition, 2004, 37: 469-474

[14] Tsai Y Y, Wang C M. A novel data hiding scheme for color images using a BSP tree[J]. Journal of System and Software, 2007, 80: 429-437

[15] Li Bo, Zheng Chun-hou, Huang De-shuang. Locally linear discriminant embedding: An efficient method for face recognition [J]. Pattern Recognition, 2008, 41: 3813-3821

[16] Shih F Y, Wu Scott Y T. Combinational image watermarking in the spatial and frequency domains[J]. Pattern Recognition, 2003, 36: 969-975

[17] Qi Miao, Lu Ying-hua, Du Ning, et al. A Novel image hiding approach based on correlation analysis for secure multimodal biometrics[J]. Journal of Network and Computer Applications, 2010, 33: 247-257