针对索引图像的人脸区域分级加密算法

韩 琦, 王志芳, 牛夏牧, 李 琼
(哈尔滨工业大学计算机科学与技术学院, 黑龙江哈尔滨 150001)

摘 要: 人脸是一种典型的图像感兴趣区域, 面向视觉感知的分级人脸区域图像加密增强了图像加密的针对性和灵活性. 本文针对索引图像的特点, 提出了一种基于颜色索引表加密和空间位置加密的人脸区域分级图像加密算法. 通过不同的密钥对颜色索引表和图像矩阵分别加密, 实现了对索引图像人脸区域的两级加密. 第一级加密后保留了少量图像中人脸的感知信息, 可以用做快速查找和识别, 第二级加密后的图像则不包含任何原图像的感知信息. 进而结合公钥密码体制, 构造了一个实用的两级加密图像安全传输方案.

关键词: 分级加密; 索引图像; 感兴趣区域; 感知信息
中图分类号: TP309.2 文献标识码: A 文章编号: 0372-2112 (2008) 12A-025-05

A Face Region Hierarchical Encryption Algorithm for Palette Images

HAN Qi, WANG Zhi-fang, NIU Xia-mu, LI Qiong
(*School of Computer Science and Technology, Harbin Institute of Technology, Harbin, Heilongjiang 150001, China*)

Abstract: Face is a typical region of interest of image. The face region hierarchical encryption based on the vision perceptual enhances the pertinence and flexibility of image encryption. A novel face region encryption algorithm of palette image is proposed by involving the palette encrypting and pixels' position encrypting. Different keys are used to encrypt the palette and the pixels' position, and the hierarchical encryption of palette image is achieved. The first level (lightweight) encryption will keep part of the perceptual information of the original face region and could be used for fast identifying. The second level encryption will eliminate all the perceptual information and achieve a high level security. Further, by combining the public key cryptosystem, a two level secure image transmitting scheme is constructed.

Key words: hierarchical encryption; palette image; region of interest; perceptual information

1 引言

由于图像本身特有的大数据量、大冗余等特点, 图像加密技术渐渐发展为有别于一般数据加密的一个新的研究领域[1]. 从图像格式的角度, 当前图像加密的研究主要集中在两个方向: 一是将数字图像看作像素颜色值的二维或三维矩阵(分别对应灰度图像和彩色图像), 通过像素空间位置置乱、颜色值置乱或者变换域置乱的方式对图像进行加密[2,3]; 二是针对 JPEG 等压缩图像格式, 在编码过程中对相关的系数进行置乱以实现图像的加密[4].

图像作为感知信息的重要载体之一, 其所承载的信息更多的体现为供使用者观看的视觉感知信息[5], 这与文本、代码等载体是不同的, 因此数字图像的加密问题也有其独特的特点和需求. 对于大多数包含人脸内容的图像, 需要保护的信息往往集中在人脸区域. 在图像上直接应用经典的加密算法, 一方面难以做到格式透明, 另一方面加密后的图像仍然可能保留大量感知信息, 因此有必要对基于视觉感知特性的图像加密技术进行深入研究. 同时, 由于人类感知机制的渐进性和模糊性, 图像加密可以引入分级加密的概念以拓展其功能和适用范围, 即对图像的感知信息进行分级的掩蔽, 经过轻量级加密的图像仍然能够传递物体轮廓、位置等信息, 但是掩蔽了感兴趣的细节区域[3,6], 这对于在数字版权管理系统(DRM)中实现多级授权、浏览保护等是非常有意义的.

本文针对一类广泛应用的图像格式——索引图像(palette images), 提出了一种基于颜色索引表加密和像素空间加密的多级人脸区域图像加密算法, 基于对人脸区域的识别和标定, 实现了索引图像中人脸区域的两级加密, 在第一级加密中保留少量的人脸感知信息, 而第二级则对感知信息进行完全加密. 进而基于该算法, 结合公钥密码体制, 构造了一套实用的图像加密传输方案.

收稿日期: 2008-09-30; 修回日期: 2008-12-08
基金项目: 国家自然科学基金(No. 60832010, No. 60671064, No. 60703011); 国家 863 高技术研究发展计划(No. 2007AA01Z458); 高等学校博士学科专项科研基金(No. 20070213047)

2 相关工作

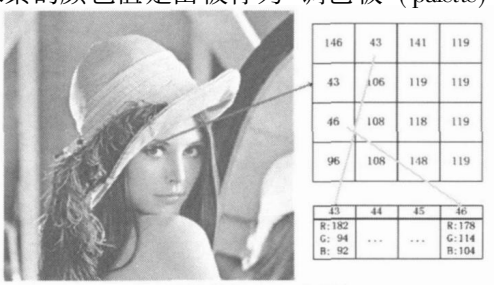
2.1 图像加密技术

从加密对图像数据文件格式影响的角度, 图像加密算法分为格式透明和格式不透明两类. 早期使用密码学方法进行图像加密, 往往会把整个图像数据文件进行加密[7], 使得加密后的文件无法以图像的方式被读取和显示, 这就是所谓的格式不透明. 基于 Arnold 变换的图像置乱处理方法最早实现了格式透明的图像加密[1], 即图像文件的结构得以保留, 可以直接被读取和显示, 但是显示出的图像则是无法感知和辨认的加密图像. 随后研究者提出多种置乱的方法, 其中包括置乱顺序和置乱模式两个方面, 很多算法都借助混沌系统的随机性产生置乱顺序, 而置乱模式则出现了换位、折叠等不同方法[1]. 这些图像加密方法都是直接针对图像矩阵的元素位置和值进行操作, 没有考虑到实际图像格式的差异.

文献[4]等关注了常见压缩格式的图像加密问题, 通过对 JPEG、JPEG2000 等编码流程的分析, 对其中一些环节的参数进行加密, 从而实现针对压缩格式透明的图像加密. 由于图像本身的感知特性, 分级加密成为图像加密有别于一般数据加密的特有的加密方式[3], 针对涉及到信息安全的图像分发、识别等应用中, 分级加密有着重要的应用.

2.2 索引图像

索引图像作为一种有效的图像存储格式得到了广泛的应用, 很多常用图像格式都使用了颜色索引的方式来减少存储数据量, 如 bmp、gif、tif、png 等格式. 索引图像像素的颜色值是由被称为“调色板”(palette) 的颜色索引表定义的, 图像矩阵中的值并不是真实的颜色值, 而是该颜色在调色板中的索引值. 相对于用 RGB 三个分量值表示一个像素点颜色的真彩色图像而言, 索引图像所能表达的颜色数量比较少(取决于调色板的大小), 但是索引图像存储容量小的优点使得索引图像在 Internet 等很多方面得到了广泛的应用. 索引图像和真彩色图像在数据表示方式上的差别如图 1 所示.



(a) 索引图像的颜色表示方法

(b) 真彩色图像的颜色表示方法

图1 索引图像和真彩色图像

在很多图像处理操作中, 往往直接把索引图像转换为真彩色图像进行处理, 再把处理后的图像转换回索引图像, 对于颜色索引表中没有的颜色则用最接近的颜色代替. 但是对于图像加密等应用, 这样的转换造成的颜色值的微小误差会导致解密失败. 文献[8]等研究了基于颜色索引表的隐写方案, 但是针对索引图像的加密技术尚未见到公开报道.

2.3 人脸区域定位

准确的人脸区域定位是对图像中感兴趣区域进行加密的前提条件, 人脸定位已经在人脸识别、目标跟踪等领域得到了广泛的应用. 根据所使用的特征, 人脸定位的算法可以分为基于特征和基于图像两大类[8], 不同的算法在速度、准确性、图像适应性等方面各有优劣. 考虑到本文算法的需求, 我们选择了基于类 haar 特征的级联分类器方法进行人脸区域定位[9], 该算法的基本思想是通过一系列弱分类器的级联实现对人脸这一复杂对象的分类, 而每一个弱分类器仅对一种简单的类 haar 特征进行区分. 如图 2 所示, 待检测图像窗口将依次通过一系列弱分类器, 在任何一个分类器处没有通过就被直接跳过, 而通过全部分类器的窗口则被认为包含人脸. 由于不包含人脸的图像区域不必经过所有的分类器, 因此可以获得较高的算法效率.

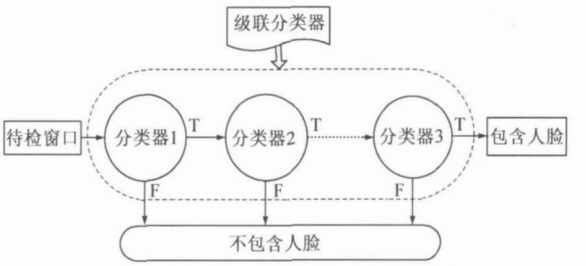


图2 基于级联分类器的人脸区域检测

3 索引图像分级加密算法

3.1 算法流程

针对索引图像的特点, 本文提出了一种索引图像的分级加密算法, 算法流程如图 3 所示. 原始的索引图像 $\boldsymbol{I}_0$ 的数据表示分为两部分: 图像矩阵 $\boldsymbol{M}_0$ 和颜色索引表 P_0, 加密后的图像 $\boldsymbol{I}_e$ 也由 $\boldsymbol{M}_2$ 和 P_2 两部分组成, 这样, 在格式上加密前的图像和加密后的图像是一致的, 可以用同样的工具打开显示 $\boldsymbol{I}_o$ 和 $\boldsymbol{I}_e$. 加密过程包括

两个方面, 图像矩阵 $\boldsymbol{M}$ 的加密和颜色索引表的加密(事实上, 这里所指的加密即有密码学中所说的数据加密, 也有图像加密中常用的置乱). 颜色索引表经过一次置乱和一次加密, 这主要是考虑到抵抗颜色索引表的替换攻击. 图像矩阵由置乱后的颜色索引表重新构造索引, 然后再通过置乱消除感知信息.

图像的分级加密体现在对图像矩阵和颜色索引表的分别解密上. 如果用户只拥有 Key_3, 则可以得到正确的图像矩阵 $\boldsymbol{M}_1$, 但无法得到正确的颜色索引表, 因此只能显示少量的轮廓信息; 而当用户拥有 Key_2 和 Key_3 时, 就可以完全解密得到 $\boldsymbol{M}_1$ 和 P_1. $\boldsymbol{M}_1$ 和 P_1 虽然在数据形式上与 $\boldsymbol{M}_0$ 和 P_0 不同, 但所表示的图像和原图像 $\boldsymbol{I}_o$ 完全一致. 同时, Key_1 的所有者可以在原图像的参与下通过 P_1 对加密图像的来源真实性进行认证.

3.2　颜色索引表加密

在图3的算法中, 对颜色索引表的加密进行了两次加密, 第一次是对颜色索引表中颜色位置进行了一次置乱, 第二次是对颜色索引表的颜色值进行了加密. 第一次置乱的目的在于消除颜色索引表的一般性, 提高加密算法抵抗替换颜色索引表攻击的能力. 一般情况下, 颜色索引表的生成由通用的图像处理软件生成, 因而生成的颜色索引表有一定的规律, 色彩相近的图像有可能得到相近的颜色索引表, 替换颜色索引表攻击就是通过替换加密后的索引图像的颜色索引表对原始图像的内容进行猜测和还原. 为了抵抗这种攻击, 首先用 Key_1 对待加密索引图像 $\boldsymbol{I}_o$ 的颜色索引表进行一次置乱处理, 得到新的颜色索引表 P_1, 和原来的颜色索引表 P_0 相比, 只是每个颜色值的顺序不同. 同时, 需要重新构造对图像矩阵中的颜色索引值, 使之指向的颜色值保持不变. 记 $P_o=\{c_1, c_2, \cdots, c_n\}$, 则置乱处理的算法描述如下:

(1) 通过 Key_1 和一个 ID 信息 d 生成一个 n 维的实数数组 $R=\{r_1, r_2, \cdots, r_n\}$;

(2) 对数组 R 按照大小顺序排序, 并记录各个元素在原数组中的位置, 得到一个元素为 1 到 n 的随机排列的数组 $S=\{s_1, s_2, \cdots, s_n\}$;

(3) 以数组 S 中元素的做下标, 重新排列颜色索引表 P_0 中的颜色值, 得到新的颜色索引表 P_1.

对颜色索引表的第二次加密使用了现代密码学的经典方法, 将颜色索引表 P_1 的二进制表示形式当作一般的数据流, 使用 RC4 流加密算法进行加密, 得到加密后的颜色索引表 P_2, 使用到了密钥 Key_2.

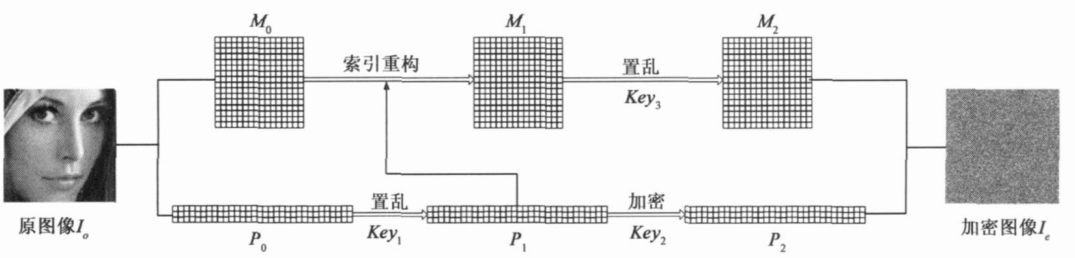


图3　索引图像分级加密算法流程

3.3　像素位置加密

只加密颜色索引表, 不对图像矩阵进行置乱, 得到的是第一级的加密图像, 这一级的加密图像仍然保留了部分感知信息, 但图像已不再具有可用性, 如图4所示.

为了实现完全加密, 对图像矩阵中像素的空间位置进行了置乱, 采用和索引表置乱类似的方法, 通过 Key_3 得到一个长度为 $p \times q$ 的实数数组(p 和 q 是图像的高和宽, 单位为像素), 进而得到1到 $p \times q$ 的随机排列, 以该排列为下标对图像像素的空间位置进行置乱, 从而实现了第二级的图像加密, 得到加密图像已经完全消除了原图在视觉上的感知信息, 如图5所示.

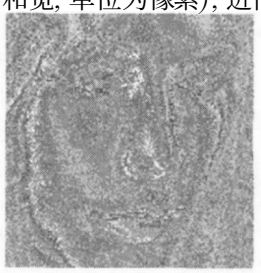


图4　保留部分感知信息的第一级加密图像

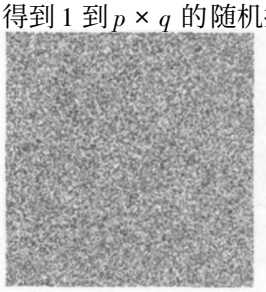


图5　第二级加密图像

3.4　基于公钥体制的图像安全传输方案

在前面介绍的索引图像分级加密算法基础上, 给出一种基于公钥密码系统的图像安全传输及认证方案. 假设有通信双方 Alice 和 Bob 需要以加密的方式传送图像, 攻击者 Mallory 试图截获并破解传送的秘密图像, 另外还有友好者 Carol 和 Dave, 他们可以在一定程度上知晓 Alice 和 Bob 的通信内容, 但不允许获得完整的图像内容. 该应用场景可以通过下面的示意图进一步阐述: 在公钥密码体制下, 设计了一套基于索引图像分级加密的安全图像传输方案. 在该方案中, Alice、Bob、Carol、Dave 彼此拥有对方的公钥, Mallory 暂时无法获得任何人的公钥. Alice 向 Bob 发送图像的过程可以用图7描述.

Bob 接收到加密图像后, 用 Alice 的公钥做算法中 Key_3 的恢复置乱的像素位置, 同时用自己的私钥解密

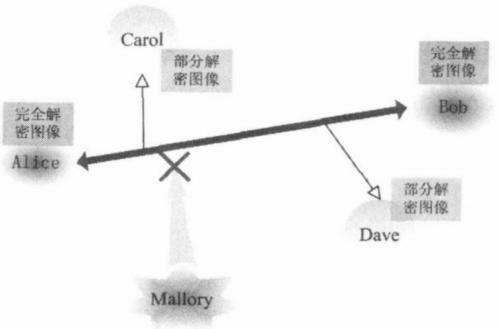


图6 分级安全图像通信场景

颜色索引表, 得到完整的解密图像. 友好者 Carol 和 Dave 可以通过自己掌握的 Alice 的公钥做 Key_3, 得到类似图 4 所示的部分解密图像. 而攻击者 Mallory 无法获得任何一个密钥, 也就无法直接获得解密图像, 即使通过一定手段获得了 Alice 的公钥, 仍然只能得到部分解密图像. Alice 用自己的私钥做 Key_1 对原始的颜色索引表进行加密, 一方面可以避免 Mallory 进行颜色索引表替换攻击, 另一方面在必要的时候, 可以通过原始图像和 Bob 解密后的颜色索引表 P_2 进行图像来源的真实性认证或者版权的证明, 认证的过程可以简要描述为:

(1) Bob 用自己的私钥解密颜色索引表 P_2, 得到可以正确显示图像的颜色索引表 P_1;

(2) Alice 使用其私钥恢复置乱的颜色索引表 P_1, 得到原始的颜色索引表 P_0;

(3) 比对原始图像的颜色索引表和 P_0. 如果不一致, 则可以认定是攻击者假冒 Alice 的名义向 Bob 发送的图像; 如果一致, 则可以用来声明 Alice 的版权.

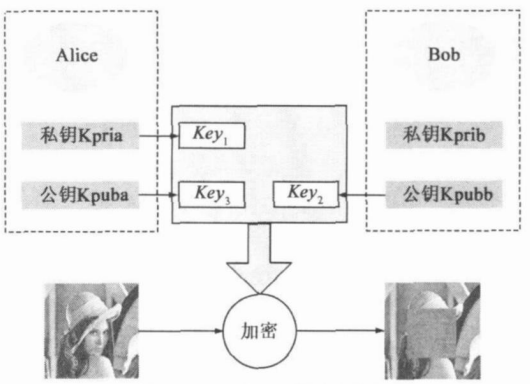


图7 Alice向Bob发送图像

这种需要原图参与的来源认证主要用于发生纠纷时的裁决, 如果引入数字水印技术, 即把 Alice 用其私钥加密的 ID 信息嵌入图像或者颜色索引表[7], Bob 就可以通过 Alice 的公钥实现盲认证.

4 仿真实验

仿真实验按照 3.4 节的通信场景, 选择了 lena 和 peppers 两个索引图像作为实验样本. 其中, lena 针对人脸区域进行感兴趣区域加密, 而 peppers 则进行全图加密. 图 8 给出了原图、部分加密图和完全加密图.

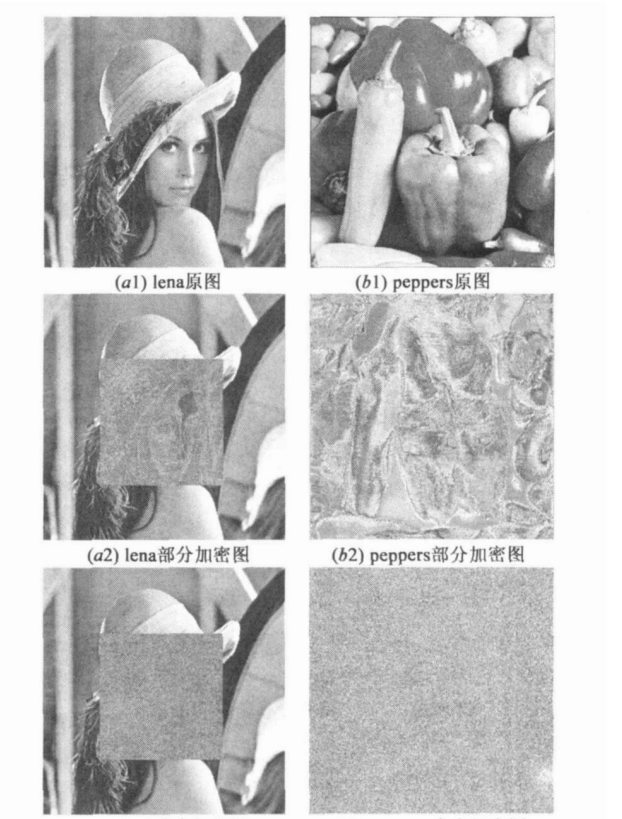


图8 部分仿真实验结果

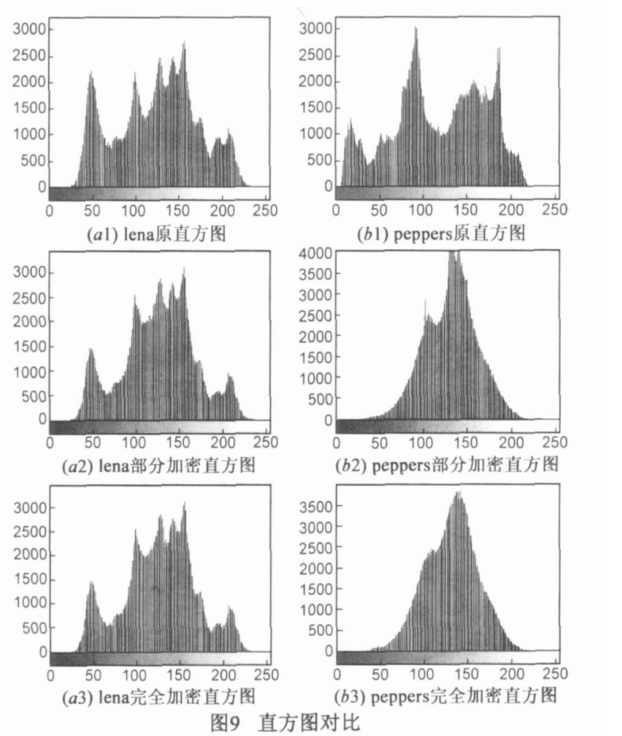


图9 直方图对比

图 8 所示为图 7 中对应图像的亮度直方图, 通过图 9(b1)-9(b3)可以看出, 加密后的图像消除了原图像直方图的主要特征, 满足全图加密的安全需求. 而在图 9(a1)-9(a3)中, 由于是对原图进行感兴趣区域加密, 直方图只有一些细节有所变化.

5 结论

针对人脸区域的分级加密由于其独特的针对性和灵活性, 成为图像加密技术中值得深入研究的新方向. 索引图像由于其特殊的数据表示结构, 使得大多数针对真彩色图像的加密算法无法直接应用. 而同时其颜色索引表的使用又为图像分级加密提供了可能. 本文针对索引图像的人脸区域加密问题提出了一种基于颜色索引表加密和像素空间位置加密的分级加密算法, 实现了图像中人脸感知信息的分级保护. 进而结合公钥密码体制, 提出了一种安全图像传输方案, 充分利用公钥密码体制的特点, 使不同的接受者可以获得不同程度的图像信息. 仿真实验证明了算法的有效性和安全性.

参考文献:

[1] 李昌刚, 韩正之. 图像加密技术新进展[J]. 信息与控制, 2003, 32(4): 339- 343.
Li Chang-gang et al. The new evolution of image encryption techniques[J]. Information and Control, 2003, 32(4): 339- 343. (in Chinese)

[2] Philip P Dang, Paul M Chau. Image encryption for secure internet multimedia applications[J]. IEEE Transactions on Consumer Electronics, 2000, 46(3): 395- 403.

[3] Dominik Engel, Elias Pschernig, et al. An analysis of lightweight encryption schemes for fingerprint images[J]. IEEE Transactions on Information Forensics and Security, 2008, 3(2): 173- 182.

[4] Subramania Sudharsanan. Shared key encryption of JPEG color images[J]. IEEE Transactions on Consumer Electronics, 2005, 51(4): 1204- 1211.

[5] 牛夏牧, 焦玉华. 感知哈希综述[J]. 电子学报. 2008, 36(7): 1405- 1411.
Niu Xiar mu et al. An overview of perceptual hashing[J]. Acta Electronica Sinica, 2008, 36(7): 1405- 1411. (in Chinese)

[6] Anil Kr. Yekkala, Narendranath Udupa, et al. Lightweight encryption for images[A]. Proceedings of International Conference on Consumer Electronics[C]. Las Vegas: IEEE, 2007. 1- 2.

[7] M-H Yang, D J Kriegman, et al. Detecting faces in images: A survey[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002, 24(1): 34- 58.

[8] 胡云, 伍宏涛, 张涵钰等. 大容量索引图像水印方案的设计与实现[J]. 北京邮电大学学报, 2005, 28(1): 26- 29.
Hu Yun, et al. A digital watermarking scheme in huge index image[J]. Journal of Beijing University of Posts and Telecommunications, 2005, 28(1): 26- 29. (in Chinese)

[9] Qi Han, Qiong Li, et al. Eyes tracking in a video sequence based on haar like features and skin color[A]. 2007 Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing[C]. Kaohsiung: IEEE, 2007. 608 - 611.

作者简介:

韩　琦　男, 1981 年生于河南省平顶山市. 2002 年和 2004 年分别获得哈尔滨工业大学学士和硕士学位. 现为哈尔滨工业大学博士研究生, 研究方向为信息安全、机器视觉.
E-mail: hanqi_xf@hit.edu.cn.

王志芳　女, 1979 年生于河南省平顶山市. 2003 年获河南大学学士学位, 2005 年获哈尔滨工业大学硕士学位. 现为哈尔滨工业大学博士研究生, 研究方向为图像处理、模式识别.