软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2023,34(2):868−883 [doi: 10.13328/j.cnki.jos.006419]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

一种加密域鲁棒图像哈希算法*

秦 川[1], 郭梦琦[1], 李欣然[1], 钱振兴[2], 张新鹏[2]

[1](上海理工大学 光电信息与计算机工程学院, 上海 200093)

[2](复旦大学 计算机科学技术学院, 上海 200433)

通信作者: 钱振兴, E-mail: zxqian@fudan.edu.cn

摘 要: 随着云计算的发展, 越来越多的多媒体数据存储在云端, 出于安全需要, 往往需要对其加密后再上传至云端进行存储或运算等操作. 针对加密图像, 在不具备图像明文内容的情况下, 为了认证图像内容的完整性和真实性, 提出了一种基于 Paillier 同态加密的鲁棒图像哈希算法. 该算法主要由 3 个部分构成: 图像所有者端图像加密, 云服务器端密文图像哈希计算以及接收者端明文图像哈希生成. 具体地, 图像所有者对图像进行 Paillier 加密, 并将加密图像上传至云服务器, 由云服务器利用 Paillier 密码系统的运算法则执行加密域 DCT 与 Watson 人眼视觉特征等的计算, 并利用密钥控制的伪随机矩阵增加哈希的随机性, 接收者解密并分析接收到的密文哈希, 生成明文图像哈希. 实验结果表明, 所提算法在鲁棒性、唯一性和安全性上具有较理想的性能.

关键词: 图像哈希; 加密域; 鲁棒性; 唯一性; 安全性

中图法分类号: TP309

中文引用格式: 秦川, 郭梦琦, 李欣然, 钱振兴, 张新鹏. 一种加密域鲁棒图像哈希算法. 软件学报, 2023, 34(2): 868–883. http://www.jos.org.cn/1000-9825/6419.htm

英文引用格式: Qin C, Guo MQ, Li XR, Qian ZX, Zhang XP. Robust Image Hashing in Encrypted Domain. Ruan Jian Xue Bao/Journal of Software, 2023, 34(2): 868–883 (in Chinese). http://www.jos.org.cn/1000-9825/6419.htm

Robust Image Hashing in Encrypted Domain

QIN Chuan[1], GUO Meng-Qi[1], LI Xin-Ran[1], QIAN Zhen-Xing[2], ZHANG Xin-Peng[2]

[1](School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China)

[2](School of Computer Science, Fudan University, Shanghai 200433, China)

Abstract: With the development of cloud computing, more and more multimedia data is stored in the cloud. For security needs, it is often necessary to encrypt images before uploading them to the cloud for storage or computing operations. Without knowing the plaintext content of the encrypted image, in order to verify the integrity of the image information and the authenticity of the content, an image hash algorithm based on Paillier homomorphic encryption is proposed. The algorithm is mainly composed of three parts: the image owner encrypts the image, the cloud server generates a ciphertext image hash, and the receiver generates a plaintext image hash. Specifically, the image owner encrypts the image and uploads the encrypted image to the cloud server. The cloud server uses the algorithm of the Paillier cryptosystem to perform calculations of DCT and Watson human visual features in encrypted domain, and uses a key-controlled pseudo-random matrix to increase the randomness of the ciphertext hash, thereby improving the security of the hash. The receiver decrypts and analyzes the received ciphertext hash to obtain the plaintext image hash. Experimental results show that the proposed algorithm has ideal performance in terms of robustness, uniqueness, and security.

Key words: image hashing; encrypted domain; robustness; discrimination; security

随着数码相机、手机等设备成像技术的逐渐成熟, 数字图像的获取变得越来越容易, 其在工作和生活中扮演着越来越重要的角色. 同时, 许多功能强大且易于操作的图像处理工具使得对图像内容进行修改操作的门槛变低,

* 基金项目: 国家自然科学基金 (U20B2051, U1936214)
收稿时间: 2021-04-30; 修改时间: 2021-06-07; 采用时间: 2021-07-14; jos 在线出版时间: 2022-05-24
CNKI 网络首发时间: 2022-11-15

非专业的用户也可以轻松地对图像内容进行修改, 这对数字图像的完整性和真实性产生了威胁[1,2]. 因此, 如何有效识别和认证数字图像成为了亟待解决的重要问题[3].

感知图像哈希是图像认证领域中的热点研究问题. 图像哈希是指用一串固定长度的字符或数字序列来表示图像的感知内容, 可以理解为图像视觉内容的压缩表达, 也称为图像指纹. 图像哈希的生成不会更改图像的内容, 近年来被广泛应用于图像认证、数字水印和图像检索等领域. 已经有许多研究人员提出了有效的技术来加速图像哈希的发展, 早期 Schneider 和 Chang 等人提出了一种基于图像内容的数字签名算法, 并将该算法应用于图像认证[4]. Liu 等人提出了一种基于 Radon 变换和不变特征的鲁棒图像哈希方法[5], 并将其用于图像认证. Tang 等人提出了一种基于局部熵和 DWT 的安全图像哈希方案[6], 该方案被应用于图像篡改的验证. Qin 等人提出了一种使用非均匀采样的图像哈希方案[7]. 该方案在鲁棒性和区分性之间实现了令人满意的折衷.

与此同时, 云计算的出现使得用户可以将大量的图像数据和复杂的图像处理运算交给云服务器来处理, 大大降低了用户的存储和计算负担. 因为多媒体数据中也包含一些隐私内容, 所以这也带来了数据隐私安全的相关问题[8,9]. 保护隐私的传统方法是对数据进行加密, 但是对数据加密以后便无法为用户提供一些常见的明文数据服务, 例如对多媒体数据的搜索, 计算和分析[10,11]. 因此, 加密域中的安全信号处理技术逐渐成为安全外包这一领域的一个重要研究方向. 近年来, 加密域中的安全信号处理技术已经得到了广泛的研究, 并取得了一定的成果. 法国学者 Erkin 是安全信号处理研究领域的领导者和先锋, Erkin 等人对加密域多媒体数据的信号处理进行了很好的综述[12]. 由于尺度不变特征变换 (SIFT) 描述符被广泛应用于图像处理中, Hsu 等人最先提出了用于解决加密域中安全 SIFT 特征表示和提取的方法[13]. 他们利用 Paillier 加密算法的同态特性很好地解决了加密域中的高斯运算和卷积计算, 但是他们的方案没有很好地解决 SIFT 中极值点提取的比较操作问题, 耗费了巨大的存储、计算和通信成本. 为了提高效率和安全性, Hu 等人提出了一种有效且实用的隐私保护计算外包协议, 可以实现海量加密图像数据上的 SIFT 特征提取[14]. 该方案通过随机分割原始图像数据, 设计适用于安全乘法和比较的新颖协议以及由两个独立的云服务器共同进行特征计算, 达到了安全性和有效性的要求. 除此以外, 还有一些针对其他特征的隐私保护方案. Chen 等人提出了一种加密域中的多重分形特征提取和表示方法[15]. 该方案首先使用混沌序列按块对图像进行加扰, 然后通过利用混沌序列的局部随机性和特殊周期性来设计加密图像的安全多分形特征提取. Xia 等人提出了一种安全的 LBP 特征提取算法[16], 在方案中, 通过块改组, 块内改组和保留顺序的像素值替换对图像进行加密. Yang 等人提出了一种基于类同态加密 (SHE) 的隐私保护 Hahn 矩方案, 并将其命名为 PPHM[17]. 该方案具有较低的复杂度和较高的安全性, 同时在图像重建和图像识别方面均具有良好的性能. Wang 等人提出了一种多用户场景下高效隐私保护的基于内容的图像检索方案[18], 该方案利用欧式距离比较技术对图像特征向量进行相似度排序并返回 top-k 结果. 同时, 设计的高效密钥转换协议允许每一个检索用户使用自身的私钥生成查询请求, 并检索不同数据拥有者生成的加密图像. Xiang 等人提出了一种基于同态加密系统的图像鲁棒可逆水印算法[19], 该算法实现了在不对原始图像进行预处理的情况下可直接在加密后的密文图像中嵌入水印, 并可分别在加密域或明文域提取水印和恢复原始密文图像或原始明文图像, 而且嵌入的水印对常见的图像处理操作具有一定的鲁棒性.

加密域中安全信号处理技术的发展在保护了数据隐私安全的同时, 也让更多的明文数据服务得以在加密域中实现[20,21], 图像认证就是其中的一种. 出于安全图像认证的需要, 本文提出了一种加密域鲁棒图像哈希算法, 通过应用同态加密这一安全信号处理技术, 实现了加密域图像哈希的生成. 首先由图像所有者对图像进行预处理和加密并将加密图像传送至云服务器端, 云服务器端对加密图像进行旋转若干特定角度, 以及水平镜像和垂直镜像的操作, 得到包括原始加密图像在内的若干加密版本. 同时引入人眼视觉特性 (human visual system, HVS), 将加密图像分块后分别计算图像 DCT 系数矩阵的变型, 将其与 Watson 权重矩阵和密钥控制的伪随机矩阵进行加密域哈希生成运算, 并将计算结果传送至接收者端. 接收者对加密处理结果解密得到明文域处理结果, 并进行量化判决以产生固定长度的图像哈希. 根据本文所提出的加密域哈希算法, 可以进行图像认证的应用, 比较待认证图像的哈希值与原始图像哈希值, 若它们之间的归一化汉明距离小于预先设定的阈值, 则通过认证, 反之拒绝. 本文工作的主要创新点如下: (1) 提出了一种基于 Paillier 同态加密的鲁棒图像哈希算法, 在保护图像隐私安全的同时, 可用于对加密图像的图像认证; (2) 引入 HVS, 在加密域中通过 DCT 系数矩阵变型与 Watson 权重矩阵和伪随机矩阵的密文

运算, 实现具有人眼视觉特性的密文哈希生成; (3) 本文算法生成的图像哈希对一般的图像内容保持操作具有鲁棒性, 同时还具有较好的唯一性和安全性.

1 加密域鲁棒图像哈希算法

本文提出的加密域鲁棒图像哈希算法流程图如图 1 所示. 该系统主要由图像所有者、云服务器、接收者 3 部分组成.

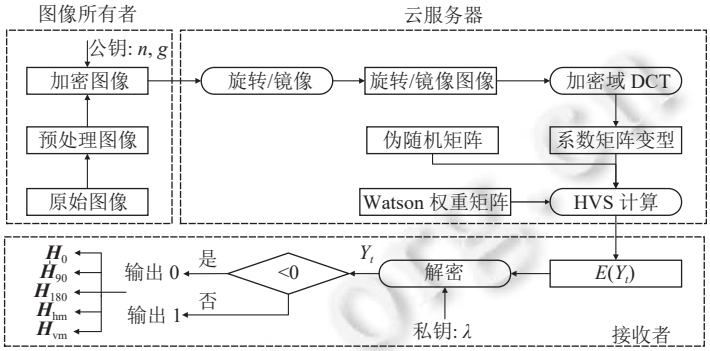


图 1 加密域图像特征提取及哈希构造

1.1 预处理和图像加密

利用公式 (1) 将输入的 RGB 彩色图像 $\boldsymbol{I}_0$ 转换为灰度图像 (若图像已经是灰度, 则不执行此步骤), 然后将灰度图像调整至 $M \times M$ 像素的固定尺寸:

$$\boldsymbol{I}_1 = 0.2989R + 0.5870G + 0.1140B \tag{1}$$

为了保护图像内容隐私, 对预处理后得到的图像 $\boldsymbol{I}_1$ 使用 Paillier 同态加密算法进行加密. Paillier 密码系统是一种部分同态、非对称的加密方案. 首先需要生成公钥 n, g 和私钥 λ. 选取两个大素数 p 和 q, 使其满足 $\psi(pq, (p-1)(q-1)) = 1$, $\psi(\cdot)$ 代表最大公约数运算符, 可以得到:

$$n = p \times q \tag{2}$$

$$\lambda = \varphi((p-1),(q-1)) \tag{3}$$

其中, $\varphi(\cdot)$ 表示最小公倍数运算符. 选择 $g \in Z_{n^2}^*$ ($Z_{n^2}=\{0, 1, \ldots, n^2-1\}$, $Z_{n^2}^* \in Z_{n^2}$), 并且满足:

$$\psi\left(L\left(g^{\lambda} \bmod n^2\right), n\right) = 1 \tag{4}$$

其中, $L(\cdot)$ 定义为 $L(x) = (x-1)/n$, $x \in N^*$. 由此可以得到公钥 n, g 和私钥 λ. 对明文 m ($m \in Z_n$ 且 $m < n$) 运用公钥 n 和 g 进行加密得到密文 c, 见公式 (5):

$$c = E(m) = g^m \times r^n \bmod n^2 \tag{5}$$

其中, $E(\cdot)$ 表示 Paillier 加密函数, r 为随机整数且 $r \in Z_{n^2}^*$. 随机数 r 保证了 Paillier 加密的非确定性, 即对于同一个明文 m, 由于 r 的不同, 其得到的对应密文 c 可能不同. Paillier 解密操作的步骤如下: 对于密文 c, 可以根据公式 (6) 恢复得到原始明文 m:

$$m = D(c) = \left(L(c^{\lambda} \bmod n^2) \times \mu\right) \bmod n \tag{6}$$

其中, $D(\cdot)$ 表示 Paillier 解密函数, $\mu = [L(g^{\lambda} \bmod n^2)]^{-1} \bmod n$. 因此, 根据公式 (5), 可对图像 $\boldsymbol{I}_1$ 进行 Paillier 加密操作得到密文图像 $\boldsymbol{I}$:

$$I(x,y) = E(\boldsymbol{I}_1(x,y)) = (g^{I_1(x,y)} \times r^n) \bmod n^2 \tag{7}$$

图像所有者在对预处理图像进行加密操作之后, 将加密后的图像 $\boldsymbol{I}$ 发送至云服务器端以进行加密域的图像哈希计算.

1.2 加密域图像哈希计算

云服务器接收到来自图像所有者发送的加密图像后, 首先对加密图像 $\boldsymbol{I}$ 分别进行固定角度 (90°, 180°, 270°) 的旋转以及水平镜像和垂直镜像操作, 得到一组加密图像, 包括原始加密图像和旋转、镜像加密图像, 接着在加密域中进行 DCT 计算, 得到 DCT 系数矩阵的变型, 结合 Watson 权重矩阵以及密钥控制的伪随机矩阵计算得到加密域图像处理结果 $E(Y_t)$, 并将其传送至接收者端, 由接收者对其进行解密, 并对解密结果进行量化判决后, 得到图像哈希值.

1.2.1 加密域图像旋转镜像操作

为了使生成的图像哈希对固定角度旋转以及镜像操作具有一定的鲁棒性, 在特征提取前, 云服务器对加密图像 $\boldsymbol{I}$ 进行固定角度 (90°, 180°, 270°) 的旋转以及水平镜像和垂直镜像操作, 可以得到加密图像 $\boldsymbol{I}$ 的 5 个不同版本的加密图像. 设 $P_0\,(x_0, y_0)$ 为原始图像中的某个像素点, $P_1\,(x_1, y_1)$ 为 $P_0\,(x_0, y_0)$ 旋转或镜像操作后得到的图像中对应的像素点. 从原始图像中的 $P_0\,(x_0, y_0)$ 映射到旋转/镜像图像中的 $P_1\,(x_1, y_1)$, 其坐标变换如公式 (8) 所示:

$$\begin{cases} x_1 = y_0, y_1 = -x_0, \text{ if 旋转90°} \\ x_1 = -x_0 + M,\ y_1 = -y_0, \text{ if 旋转180°} \\ x_1 = y_0 + M, y_1 = -x_0 + M, \text{ if 旋转270°} \\ x_1 = -x_0, y_1 = y_0, \text{ if 水平镜像} \\ x_1 = x_0, y_1 = -y_0, \text{ if 垂直镜像} \end{cases} \tag{8}$$

接下来, 云服务器对加密图像 $\boldsymbol{I}$ 及其 5 个旋转镜像版本进行特征提取操作. 下一节将以对加密图像 $\boldsymbol{I}$ 进行特征提取为例进行叙述.

1.2.2 加密域 DCT 系数特征提取

首先, 云服务器将加密图像 $\boldsymbol{I}$ 分成 $(M/8) \times (M/8)$ 个大小为 8×8 的图像块 $\boldsymbol{B}_i$, $i = 1, 2, \ldots, M^2/64$. 再分别对每个图像块 $\boldsymbol{B}_i$ 进行加密域 DCT 的计算. 已知明文域中 DCT 系数矩阵的计算如公式 (9) 所示:

$$F(u,v) = a(u)a(v)\sum_{j=0}^{7}\sum_{k=0}^{7} f(j,k) \times \cos\left(\frac{(2j+1)u\pi}{16}\right) \times \cos\left(\frac{(2k+1)v\pi}{16}\right) \tag{9}$$

其中, 当 $u, v = 0$ 时, $a(u), a(v) = \sqrt{1/8}$; 当 $u, v = 1, 2, \ldots, 7$ 时, $a(u), a(v) = \sqrt{1/4}$. 为在提取特征时不受平均亮度影响, 我们将系数矩阵中的直流系数置零.

由公式 (9) 可知, $a(u)$、$a(v)$、$\cos\left(\frac{(2j+1)u\pi}{16}\right)$ 和 $\cos\left(\frac{(2k+1)v\pi}{16}\right)$ 均不是整数. 如果要在加密域中求取 DCT 系数矩阵, 根据第 1.1 节中 $m \in Z_n$ 且 $m < n$ 的要求, 需要先将这几项量化为整数后再进行运算, 即根据公式 (10) 进行 DCT 系数矩阵变型的计算:

$$F(u,v) = [\xi_1 a(u)a(v)] \times \sum_{j=0}^{7}\sum_{k=0}^{7} f(j,k) \times \left[\xi_2 \cos\left(\frac{(2j+1)u\pi}{16}\right)\right] \times \left[\xi_2 \cos\left(\frac{(2k+1)v\pi}{16}\right)\right] \tag{10}$$

其中, ξ_1、ξ_2 为正整数, 分别表示对 $a(u)a(v)$ 和 $\cos\left(\frac{(2j+1)u\pi}{16}\right)$、$\cos\left(\frac{(2k+1)v\pi}{16}\right)$ 的放大倍数, $[\cdot]$ 函数表示四舍五入取整运算.

由于公式 (10) 中的运算为加法和数乘运算, 因此可以利用 Paillier 密码系统的加法和标量乘法特性进行加密域中的计算. 根据同态特性可知, 在适当的模运算下, 对两个密文的乘积进行解密可以得到对应两个明文的和, 对密文的整数指数幂进行解密可以得到该整数指数与对应明文的乘积. 它的同态性质可由公式 (11)、公式 (12) 表示, 其中 ξ 为整数, 对于两个明文 m_1 和 m_2, 有:

$$D\left((E(m_1) \times E(m_2)) \bmod n^2\right) = (m_1 + m_2) \bmod n \tag{11}$$

$$D\left(E(m_1)^{\xi} \bmod n^2\right) = (m_1 \times \xi) \bmod n \tag{12}$$

由此, 可以得到 DCT 系数矩阵变型的计算公式, 如公式 (13) 所示:

$$E(\boldsymbol{C}_i(u,v))=E\left([\xi_1 a(u)a(v)]\times\sum_{j=0}^{7}\sum_{k=0}^{7}B_i(j,k)\times\left[\xi_2\cos\left(\frac{(2j+1)u\pi}{16}\right)\right]\times\left[\xi_2\cos\left(\frac{(2k+1)v\pi}{16}\right)\right]\right)$$
$$=\prod_{j=0}^{7}\prod_{k=0}^{7}E\left(B_i(j,k)\times[\xi_1 a(u)a(v)]\times\left[\xi_2\cos\left(\frac{(2j+1)u\pi}{16}\right)\right]\times\left[\xi_2\cos\left(\frac{(2k+1)v\pi}{16}\right)\right]\right)\bmod n^2$$
$$=\prod_{j=0}^{7}\prod_{k=0}^{7}E(B_i(j,k))^{[\xi_1 a(u)a(v)]\times\left[\xi_2\cos\left(\frac{(2j+1)u\pi}{16}\right)\right]\times\left[\xi_2\cos\left(\frac{(2k+1)v\pi}{16}\right)\right]}\bmod n^2 \tag{13}$$

其中, $\boldsymbol{C}_i$ 为图像块的系数矩阵的变型, 大小为 8 × 8. 由公式 (13) 得到每个图像块的系数矩阵的变型后, 再将其按图像块在原图像中的位置拼接得到图像的 DCT 系数矩阵的变型 $\boldsymbol{C}$, 大小为 $M \times M$. 需要说明的是, 在计算中, 把 $\xi_1 a(u)a(v)$、$\xi_2\cos\left(\frac{(2j+1)u\pi}{16}\right)$ 和 $\xi_2\cos\left(\frac{(2k+1)v\pi}{16}\right)$ 作为整体来进行计算以减少加密域中的指数运算次数, 从而提高计算效率.

1.2.3 基于 HVS 的密文哈希计算

云服务器计算得到图像系数矩阵变型后, 结合由密钥控制的伪随机矩阵以及 Watson 视觉模型, 进行基于 HVS 的密文哈希计算.

首先, 为了提高生成哈希的安全性, 根据密钥 K 生成 τ 个与 $\boldsymbol{C}$ 大小相同的伪随机矩阵 $\boldsymbol{D}_t$, $t = 1, 2, \ldots, \tau$. 矩阵中元素相互独立, 且服从标准正态分布. 将 $\boldsymbol{D}_t$ 进行取整处理得到 $[\xi_3\boldsymbol{D}_t]$, 并根据公式 (5) 将其加密, 计算公式如公式 (14) 所示:

$$E([\xi_3 D_t])=(g^{[\xi_3 D_t]}\times r^n)\bmod n^2 \tag{14}$$

其中, ξ_3 为正整数. 没有密钥 K 的情况下, 无法得到完全相同的伪随机矩阵, 具有一定的安全性.

基于 Watson 人眼视觉模型引入 DCT 频率敏感度矩阵 $\boldsymbol{A}$, 矩阵中的每个元素的值表示图像分块在没有掩蔽噪声的情况下, 对应位置的 DCT 系数可被察觉的最小修改幅度, 这个值越小, 说明人眼对该频率越敏感, 也就是说该频率系数对图像视觉内容越重要, 其在频率特征值中占的比例应该越大, 因而在计算特征值时可将矩阵 $\boldsymbol{A}$ 中的每个元素的倒数作为对应位置 DCT 频率的权重. 周期延拓矩阵 $\boldsymbol{A}$, 并将延拓后矩阵中的元素取倒数, 得到大小为 $M \times M$ 的 Watson 权重矩阵 $\boldsymbol{Q}$, $\boldsymbol{A}$ 和 $\boldsymbol{Q}$ 如公式 (15) 所示. 同样的, 由于 $\boldsymbol{Q}$ 中元素不是整数, 需要将其化为整数后再进行计算, 对 Watson 权重矩阵 $\boldsymbol{Q}$ 进行取整操作 $[\xi_4\boldsymbol{Q}]$, ξ_4 为正整数.

$$\boldsymbol{A}=\begin{pmatrix}1.40&1.01&1.16&1.66&2.40&3.43&4.79&6.56\\1.01&1.45&1.32&1.52&2.00&2.71&3.67&4.93\\1.16&1.32&2.24&2.59&2.98&3.64&4.60&5.88\\1.66&1.52&2.59&3.77&4.55&5.30&6.28&7.60\\2.40&2.20&2.98&4.55&6.15&7.46&8.71&10.17\\3.43&2.71&3.64&5.30&7.46&9.62&11.58&13.51\\4.79&3.67&4.60&6.28&8.71&11.58&14.50&17.29\\6.56&4.93&5.88&7.60&10.17&13.51&17.29&21.15\end{pmatrix},$$

$$\boldsymbol{Q}=\left(\begin{array}{ccc:c:ccc}0.7143&\cdots&0.1524&&0.7143&\cdots&0.1524\\\vdots&\ddots&\vdots&\cdots&\vdots&\ddots&\vdots\\0.1524&\cdots&0.0473&&0.1524&\cdots&0.0473\\\hdashline&\vdots&&\ddots&&\vdots&\\\hdashline0.7143&\cdots&0.1524&&0.7143&\cdots&0.1524\\\vdots&\ddots&\vdots&\cdots&\vdots&\ddots&\vdots\\0.1524&\cdots&0.0473&&0.1524&\cdots&0.0473\end{array}\right) \tag{15}$$

云服务器利用 Watson 权重矩阵 $\boldsymbol{Q}$ 增大人眼敏感的频率系数在计算图像哈希时所占比重, 并利用伪随机矩阵增加哈希的安全性, 计算得到基于 HVS 的密文哈希计算结果. 计算公式如公式 (16) 所示, 其中, $t = 1, 2, \ldots, \tau$.

$$E(Y_t)=E\left(\sum_{p=1}^{M}\sum_{q=1}^{M}C(p,q)\times[\xi_3 D_t(p,q)]\times[\xi_4 Q(p,q)]\right)$$
$$=\prod_{p=1}^{M}\prod_{q=1}^{M}E\left(C(p,q)\times[\xi_3 D_t(p,q)]\times[\xi_4 Q(p,q)]\right) \bmod n^2$$
$$=\prod_{p=1}^{M}\prod_{q=1}^{M}E(C(p,q))^{[\xi_3 D_t(p,q)]\times[\xi_4 Q(p,q)]} \bmod n^2 \tag{16}$$

至此, 云服务器得到加密域的密文哈希计算结果 $E(Y_t)$, 则密文哈希可以表示为: $E(\boldsymbol{H}_0)=[E(Y_1), E(Y_2),\ldots, E(Y_\tau)]$, 将其解密便可以得到图像的明文哈希值. 基于 HVS 的图像哈希算法能够反映人眼的视觉特性, 增大对人眼敏感的频域系数 (即图像主要内容特征) 在计算图像哈希时的权重.

1.3 解密和明文哈希生成

接收者从云服务器端接收到加密域计算结果 $E(Y_t)$ 后, 对其进行解密操作. 接收者利用私钥 λ 并结合公式 (6) 对 $E(Y_t)$ 进行解密, 得到 Y_t 的值, 如公式 (17) 所示.

$$Y_t=D(E(Y_t))=\left(L\left(E(Y_t)^{\lambda} \bmod n^2\right)\times\mu\right) \bmod n \tag{17}$$

将 Y_t 与 0 进行大小比较, 若 Y_t 大于等于 0, 则 h_t 为 1, 否则, h_t 为 0, 其中 $t=1, 2,\ldots, \tau$, 可以得到原始图像的哈希值 $\boldsymbol{H}_0=[h_1, h_2, \ldots, h_\tau]$. 同理, 对于旋转加密图像和镜像加密图像, 可得到旋转图像哈希值 $\boldsymbol{H}_{90}$, $\boldsymbol{H}_{180}$, $\boldsymbol{H}_{270}$ 以及镜像图像哈希值 $\boldsymbol{H}_{\mathrm{hm}}$, $\boldsymbol{H}_{\mathrm{vm}}$. 完整的图像哈希值表示为 $\boldsymbol{H}=\{\boldsymbol{H}_0\|\boldsymbol{H}_{90}\|\boldsymbol{H}_{180}\|\boldsymbol{H}_{270}\|\boldsymbol{H}_{\mathrm{hm}}\|\boldsymbol{H}_{\mathrm{vm}}\}$(‖表示哈希值的级联), 哈希长度为 6τ 比特, 并且得到的这组哈希能够抵抗固定角度 (90°, 180°, 270°) 的旋转以及水平镜像和垂直镜像操作.

2 实验结果与分析

本节将对得到的明文哈希值进行实验来验证其性能, 实验内容包括哈希长度分析实验、安全性实验、鲁棒性实验、唯一性实验、与其他哈希算法的性能比较实验以及图像认证的应用实验. 所有实验均在 2.40 GHz Core, i5-9600H CPU, 8.00 GB 内存和 Windows 10 系统的计算机上进行, 编程环境为 Matlab 2017b. 图 2(a)–图 2(e) 是 5 幅大小为 256 × 256 的标准测试图像, 依次为 Airplane, Baboon, House, Lena 和 Peppers, 均可从 USC-SIPI 图像数据库[22]中下载得到. 本节将主要采用这 5 幅灰度图像以及彩色图像数据库 (UCID)[23]中 1 338 张图像的灰度版本作为实验测试图.

(a) Airplane (b) Baboon (c) House (d) Lena (e) Peppers

图 2 标准测试图像

2.1 相似度衡量

在本文的实验中, 两个图像哈希: $\boldsymbol{H}_1$、$\boldsymbol{H}_2$ 之间的相似性用归一化汉明距离来衡量, 即 $\boldsymbol{H}_1$ 和 $\boldsymbol{H}_2$ 中不同的分量所占的百分比, 如式 (18) 所示:

$$d=\frac{d_{\mathrm{different}}}{d_{\mathrm{all}}} \tag{18}$$

其中, d_{all} 为 $\boldsymbol{H}_1$(或 $\boldsymbol{H}_2$) 向量中包含元素的个数, $d_{\mathrm{different}}$ 为 $\boldsymbol{H}_1$、$\boldsymbol{H}_2$ 中不同元素的个数, d 为 $\boldsymbol{H}_1$、$\boldsymbol{H}_2$ 之间的归一化汉明距离. 当两个图像哈希之间的归一化汉明距离小于一个设定的阈值 T, 则认为这两个图像是感知相似的, 反之认为这两个图像是感知不同的.

在实验过程中, 安全性实验、鲁棒性、唯一性实验、性能比较实验以及图像认证的应用实验均采用 $\boldsymbol{H}=\{\boldsymbol{H}_0||\boldsymbol{H}_{90}||\boldsymbol{H}_{180}||\boldsymbol{H}_{270}||\boldsymbol{H}_{\mathrm{hm}}||\boldsymbol{H}_{\mathrm{vm}}\}$来计算归一化汉明距离, 旋转和镜像鲁棒性实验采用哈希段 $\boldsymbol{H}_0$、$\boldsymbol{H}_{90}$、$\boldsymbol{H}_{180}$、$\boldsymbol{H}_{270}$、$\boldsymbol{H}_{\mathrm{hm}}$、$\boldsymbol{H}_{\mathrm{vm}}$ 一一比对的方法进行实验.

2.2 哈希长度分析

由于唯一性与图像哈希方案的感知鲁棒性相矛盾, 因此, 为了公平地进行 5 种方案的比较, 将感知鲁棒性和唯一性的综合性能视为区分视觉相似和不同图像的分类能力.

由第 1.3 节可知原始图像的哈希值为 $\boldsymbol{H}_0=[h_1, h_2, \ldots, h_\tau]$, 完整的图像哈希值表示为 $\boldsymbol{H}=\{\boldsymbol{H}_0||\boldsymbol{H}_{90}||\boldsymbol{H}_{180}||\boldsymbol{H}_{270}||\boldsymbol{H}_{\mathrm{hm}}||\boldsymbol{H}_{\mathrm{vm}}\}$, 哈希长度为 6τ 比特. 为了分析图像哈希长度对哈希性能的影响, 利用 ROC 曲线对哈希长度参数 τ 分别为 32、64、96 比特时鲁棒性和唯一性的综合性能进行比较. 两种典型指标, 即真实阳性率 P_{T} 和错误阳性率 P_{F}, 被用于性能评估:

$$P_{\mathrm{T}}=\frac{N_{\mathrm{true}}}{N_{\mathrm{similar}}} \tag{19}$$

$$P_{\mathrm{F}}=\frac{N_{\mathrm{false}}}{N_{\mathrm{different}}} \tag{20}$$

其中, N_{true} 表示正确分类为相似图像的实际相似图像的数量, N_{false} 代表错误分类为相似图像的实际不同图像的数量, N_{similar} 和 $N_{\mathrm{different}}$ 分别为实际相似和实际不同图像的总数. 在图 3 中, x 轴为 P_{F}, y 轴为 P_{T}, P_{F} 描述了唯一性, 而 P_{T} 则反映了感知鲁棒性. 当 P_{T} 相同时, P_{F} 越小, 算法整体性能越好; 当 P_{F} 相同时, P_{T} 越大, 算法性能越好, 即靠近左上角的曲线比远离左上角的曲线具有更好的分类性能. 当 $P_{\mathrm{F}}=0$ 时, $\tau=32$ 比特的曲线对应的 P_{T} 为 0.9794, $\tau=64$ 比特的曲线和 $\tau=96$ 比特的曲线对应的 P_{T} 为 1, 由此可以看出, $\tau=64$ 比特和 $\tau=96$ 比特时算法的分类性能优于 $\tau=32$ 比特时算法的分类性能. 但是 τ 若为 96 比特, 其计算所需的时间和资源也更多, 因此在本文实验中, 将 τ 取为 64 比特.

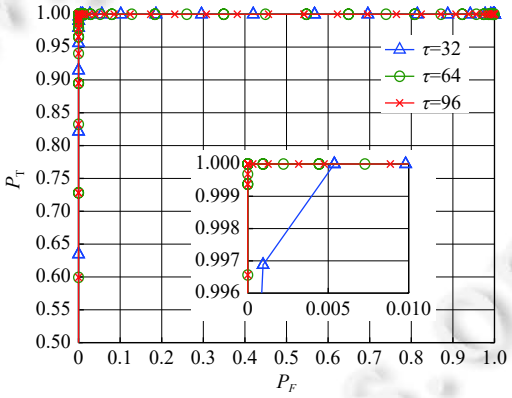
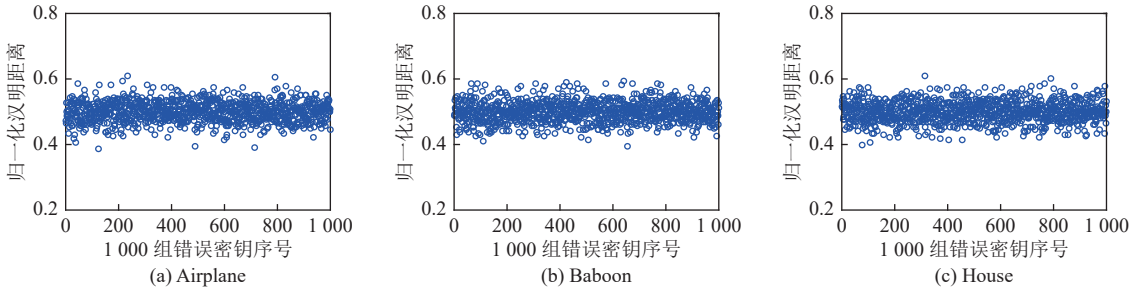


图 3 不同哈希长度的 ROC 曲线比较

2.3 安全性

2.3.1 生成伪随机矩阵的密钥安全性

由第 1 节可知, 基于 HVS 的图像哈希方案中需要由密钥 K 来控制生成伪随机矩阵 $\boldsymbol{D}_t$, 当取不同的密钥 K 来产生 $\boldsymbol{D}_t$ 时, 会得到不同的图像哈希, 攻击者在不知道正确密钥的情况下很难得到正确的哈希. 下面将描述取不同的密钥生成伪随机矩阵所产生的实验结果. 图 4 中展示了本文方案生成伪随机矩阵的密钥安全性, 其中横坐标是 1000 组随机生成的错误的密钥索引, 图 4(a)–图 4(c) 的纵坐标分别是图 2 中的 Airplane、Baboon、House 在正确和错误密钥控制下产生的哈希对之间的归一化汉明距离. 在最理想的情况下, 不同密钥生成的哈希之间的归一化汉明距离为 0.5. 可以观察到, 图 4 中几乎所有 d 都分布在 [0.38, 0.65] 之间, 且围绕 0.5 上下浮动., 这意味着, 在不知道正确密钥 K 的情况下, 攻击者难以伪造图像哈希值.

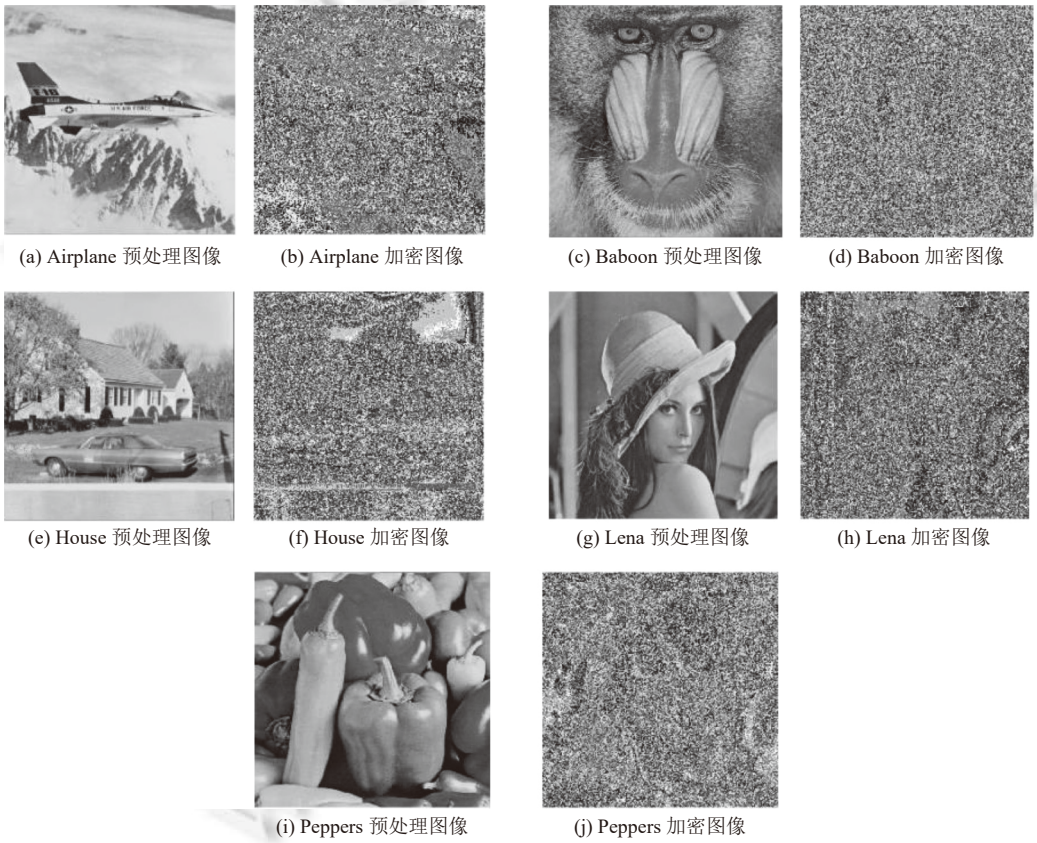


(a) Airplane (b) Baboon (c) House

图 4 正确的密钥和 1 000 组错误的密钥产生的哈希对之间的归一化汉明距离

2.3.2 加密解密过程的安全性

由第 1.1 节的加密公式 (5)、解密公式 (6) 可以知道, 使用公钥 g 和 n 对明文 m 进行加密, 使用私钥 λ 对密文 c 进行解密, 没有正确的私钥 λ, 则无法得到图像的明文信息. 除此以外, 在加密过程中还会产生一个随机整数 r, 它保证了 Paillier 加密方案的非确定性, 因为对于同一个明文 m 来说, 当产生的随机整数 r 不同, 得到的对应密文 c 也不同. 图 5(b)、(d)、(f)、(h)、(j) 为对图 5(a)、(c)、(e)、(g)、(i) 的加密结果图. 注意, 为了能够将加密结果用图像表示出来, 图 5(b)、(d)、(f)、(h)、(j) 中加密图像的像素值是对加密值进行了 256 模运算后的结果. 从图 5 可以清楚地看到, 预处理图像的内容经过加密后被隐藏起来, 从产生的加密结果图中不能得到原图的任何信息, 因此可以有效地保护内容所有者的隐私.



(a) Airplane 预处理图像 (b) Airplane 加密图像 (c) Baboon 预处理图像 (d) Baboon 加密图像

(e) House 预处理图像 (f) House 加密图像 (g) Lena 预处理图像 (h) Lena 加密图像

(i) Peppers 预处理图像 (j) Peppers 加密图像

图 5 基于 Paillier 同态加密的预处理图像的加密结果

2.4 鲁棒性

对图 2 中的 5 幅图像分别进行 10 种常见的图像处理: JPEG 压缩、高斯低通滤波、伽马校正、均值滤波、中值滤波、缩放、椒盐噪声、斑点噪声、特定角度旋转、镜像操作, 以及 5 种组合攻击操作: JPEG 压缩和高斯低通滤波、JPEG 压缩和伽马校正、JPEG 压缩和椒盐噪声、均值滤波和斑点噪声、中值滤波和缩放, 来产生原始图像的感知相似图像. 每种处理的详细参数值设置见表 1.

表 1 15 种内容保持的图像处理操作及其参数设置

图像操作	参数名称	参数值	产生图像数
JPEG压缩	品质因数	30, 40, 50, 60, 70, 80, 90, 100	8
高斯低通滤波	标准差	0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1	8
伽马校正	伽马值	0.8, 0.9, 1, 1.1, 1.2, 1.3, 1.4, 1.5	8
均值滤波	窗尺寸	3, 5, 7, 9, 11, 13, 15, 17	8
中值滤波	窗尺寸	1, 3, 5, 7, 9, 11, 13, 15	8
缩放	缩放比例	0.8, 0.9, 1, 1.1, 1.2, 1.3, 1.4, 1.5	8
椒盐噪声	噪声密度	0.001, 0.002, …, 0.007, 0.008	8
斑点噪声	噪声密度	0.001, 0.002, …, 0.007, 0.008	8
JPEG压缩+高斯低通滤波	品质因数, 标准差	品质因数: 30, 60, 90; 标准差: 0.3, 0.4, …, 1	24
JPEG压缩+伽马校正	品质因数, 伽马值	品质因数: 30, 60, 90; 伽马值: 0.8, 0.9, …, 1.5	24
JPEG压缩+椒盐噪声	品质因数, 噪声密度	品质因数: 30, 60, 90; 噪声密度: 0.001, 0.002, …, 0.008	24
均值滤波+斑点噪声	窗尺寸, 噪声密度	窗尺寸: 3, 9, 15; 噪声密度: 0.001, 0.002, …, 0.008	24
中值滤波+缩放	窗尺寸, 缩放比例	窗尺寸: 1, 7, 13; 缩放比例: 0.8, 0.9 , …, 1.5	24
旋转	旋转角度	90°, 180°, 270°	3
镜像	水平镜像, 垂直镜像	hm, vm	2

对于图 2 中的每个图像, 根据表 1 中每个图像操作生成相似图像, 并计算出哈希值, 然后根据公式 (18) 计算相似图像哈希与原始图像哈希之间的归一化汉明距离 d. 除了旋转和镜像后的相似图像外 (详细描述见后), 每个标准测试图像可以产生 64 个常见图像操作下的相似图像, 以及 120 个组合攻击操作下的相似图像, 即可以得到标准测试图像与相似图像之间的 184 个归一化汉明距离 d, 对于图 2 中的 5 幅原始图像, 可以产生总共 920 个汉明距离. 在图 6 和图 7 的每个子图中, 横坐标是每种图像操作的参数值, 纵坐标是原始图像与对应相似图像哈希对之间的归一化汉明距离 d.

为进一步体现图像哈希方案的鲁棒性能, 接着从 USC-SIPI 图像数据库的 Aerials 中选取 38 张图片, Miscellaneous 中选取 12 张图片, 共 50 张图片进行鲁棒性实验. 选择表 1 中提到的除旋转、镜像外的其他 13 种常见图像处理应用到 50 张图片上, 共 184 种不同参数的攻击, 详细参数设置见表 1. 可得到共 $50 \times (8 \times 8 + 24 \times 5) = 9200$ 张相似图片. 表 2 为每张相似图像与原图像之间归一化汉明距离 d 的数据统计表. 由图 6(a)–图 6(h)、图 7(a)–图 7(e) 和表 2 可以观察到, 相似图像与原始图像之间的 d 一般小于 0.27. 也就是说, 本文的图像哈希方案针对常见的图像处理操作具有较好的鲁棒性.

在旋转和镜像的鲁棒性实验中, 实验图像的哈希值都对应 6 个部分: 图像分别旋转 0°、90°、180°、270°得到的旋转图像的哈希值以及对图像分别进行水平、垂直镜像操作后所得图像的哈希值. 要判断一张实验图像是否是原始图像的旋转或镜像版本, 需要将该实验图像哈希值的 6 个部分与原始图像哈希值的 6 个部分一一比对, 由它们的对应关系来判断实验图像是否是原始图像的旋转或镜像版本. 以旋转 90°的实验图像为例, 将旋转 90°的实验图像的哈希值的 6 个部分, 记为 $\boldsymbol{H}_0^{(1)}$、$\boldsymbol{H}_{90}^{(1)}$、$\boldsymbol{H}_{180}^{(1)}$、$\boldsymbol{H}_{270}^{(1)}$、$\boldsymbol{H}_{\mathrm{hm}}^{(1)}$、$\boldsymbol{H}_{\mathrm{vm}}^{(1)}$, 将原始图像哈希值的 6 个部分记为 $\boldsymbol{H}_0$、$\boldsymbol{H}_{90}$、$\boldsymbol{H}_{180}$、$\boldsymbol{H}_{270}$、$\boldsymbol{H}_{\mathrm{hm}}$、$\boldsymbol{H}_{\mathrm{vm}}$, 首先计算 $\boldsymbol{H}_0^{(1)}$ 与 $\boldsymbol{H}_0$、$\boldsymbol{H}_{90}$、$\boldsymbol{H}_{180}$、$\boldsymbol{H}_{270}$、$\boldsymbol{H}_{\mathrm{hm}}$、$\boldsymbol{H}_{\mathrm{vm}}$ 之间的归一化汉明距离 d, 可以发现 $\boldsymbol{H}_0^{(1)}$ 与 $\boldsymbol{H}_{90}$ 之间的 d 值为 0, 而 $\boldsymbol{H}_0^{(1)}$ 与 $\boldsymbol{H}_{180}$、$\boldsymbol{H}_{270}$、$\boldsymbol{H}_0$、$\boldsymbol{H}_{\mathrm{hm}}$、$\boldsymbol{H}_{\mathrm{vm}}$ 之间的 d 值很大, 都在 0.37 以上, 与上述鲁棒性阈值 $T = 0.27$ 相比, 可以明显的区分开. 接着分别计算 $\boldsymbol{H}_{90}^{(1)}$、$\boldsymbol{H}_{180}^{(1)}$、$\boldsymbol{H}_{270}^{(1)}$、$\boldsymbol{H}_{\mathrm{hm}}^{(1)}$、$\boldsymbol{H}_{\mathrm{vm}}^{(1)}$ 与 $\boldsymbol{H}_0$、

$\boldsymbol{H}_{90}$、$\boldsymbol{H}_{180}$、$\boldsymbol{H}_{270}$、$\boldsymbol{H}_{\mathrm{hm}}$、$\boldsymbol{H}_{\mathrm{vm}}$ 之间的归一化汉明距离 d, 可以发现 $\boldsymbol{H}_{90}^{(1)}$ 和 $\boldsymbol{H}_{180}$, $\boldsymbol{H}_{180}^{(1)}$ 和 $\boldsymbol{H}_{270}$, $\boldsymbol{H}_{270}^{(1)}$ 和 $\boldsymbol{H}_0$ 之间的 d 值均为 0, 而和其他几个哈希部分的 d 值均大于 0.35. 从而可以得到 $\boldsymbol{H}_0^{(1)}=\boldsymbol{H}_{90}$, $\boldsymbol{H}_{90}^{(1)}=\boldsymbol{H}_{180}$, $\boldsymbol{H}_{180}^{(1)}=\boldsymbol{H}_{270}$, $\boldsymbol{H}_{270}^{(1)}=\boldsymbol{H}_0$ 这样一个对应关系. 据此可以判断该实验图像是原始图像旋转了 90°的旋转图像. 图 8(a)–图 8(e) 中的实验图像分别是原始图像旋转了 90°、180°、270°的旋转图像和水平、垂直镜像后的镜像图像, 可以看出哈希具有比较好的旋转和镜像鲁棒性能.

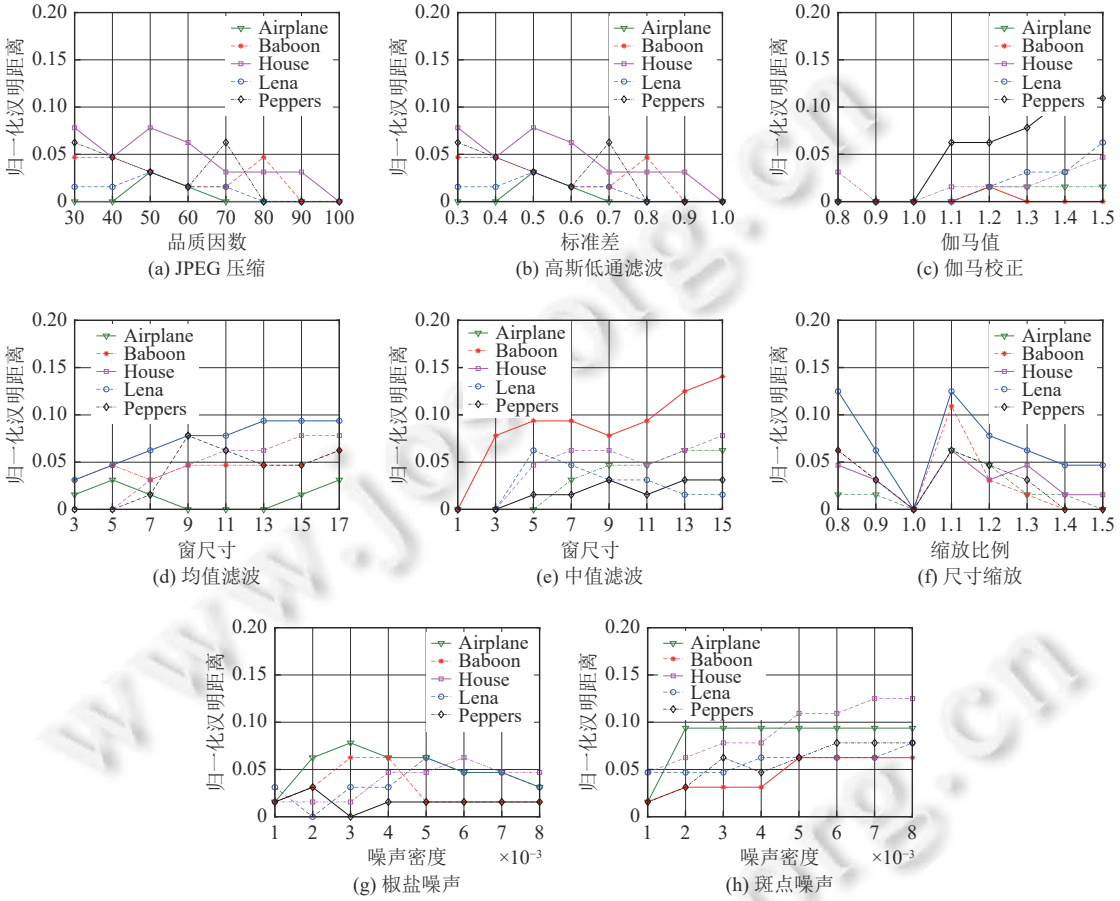


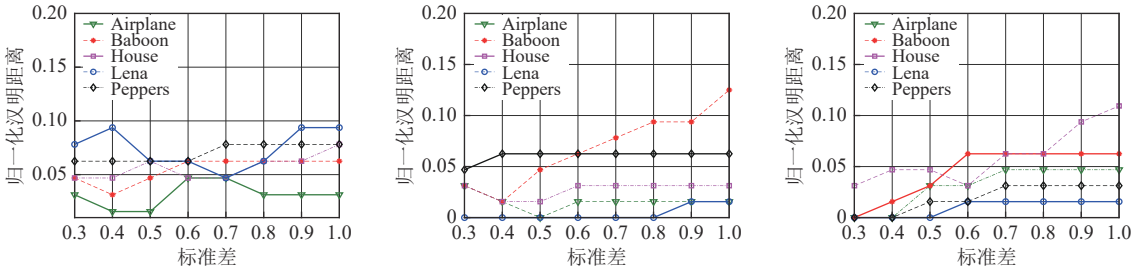
图 6 单一的内容保持图像处理操作下的鲁棒性结果

2.5 唯一性

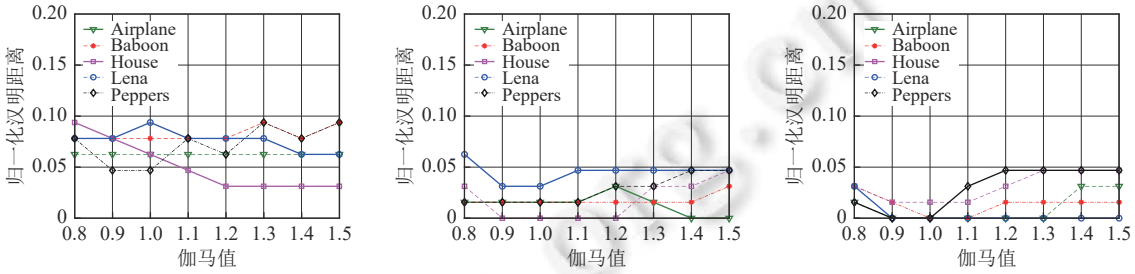
为了评估本文哈希方案辨别不同图像的能力, 在实验中采用了彩色图像数据库 (UCID) 库中包括 1 338 张大小为 512×384 和 384×512 的不同图像. 首先求出 UCID 中的所有 1 338 张图像的哈希值, 然后计算每幅图像的哈希值与其他 1 337 幅图像哈希值之间的归一化汉明距离, 可以得到这 1 338 张视觉上不同的图像的共计 C_{1338}^{2} = 894453 个归一化汉明距离. 图 9 为这 894 453 个归一化汉明距离的直方图, 其中横坐标表示归一化汉明距离 d 的值, 纵坐标代表 d 的相应出现频率. 由图 9 可以观察到, 基于参数估计, 归一化汉明距离的直方图分布大致符合均值 $\mu=0.5$ 和标准偏差 $\sigma=0.0626$ 的正态分布.

从统计上讲, 两个不同图像的碰撞概率 P_{c} 是其归一化汉明距离 d 小于设定阈值 T 的概率, 如公式 (21) 所示:

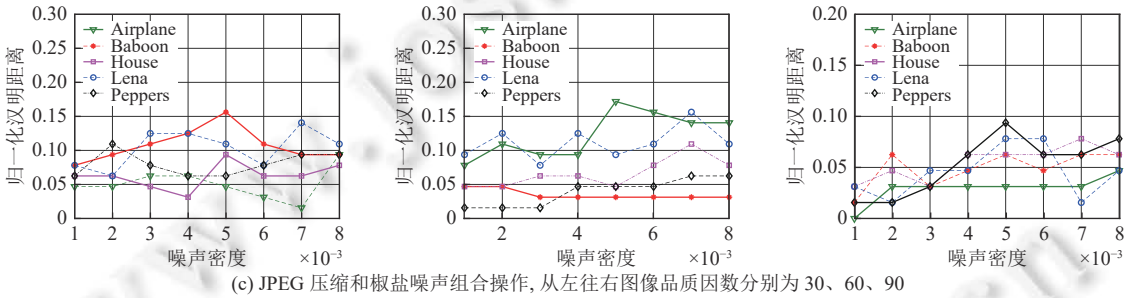
$$P_{\mathrm{c}}(T)=\frac{1}{\sqrt{2\pi}\sigma}\int_{-\infty}^{T}\exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)dx=0.5\times\mathrm{erfc}\left(-\frac{T-\mu}{\sqrt{2}\sigma}\right) \tag{21}$$



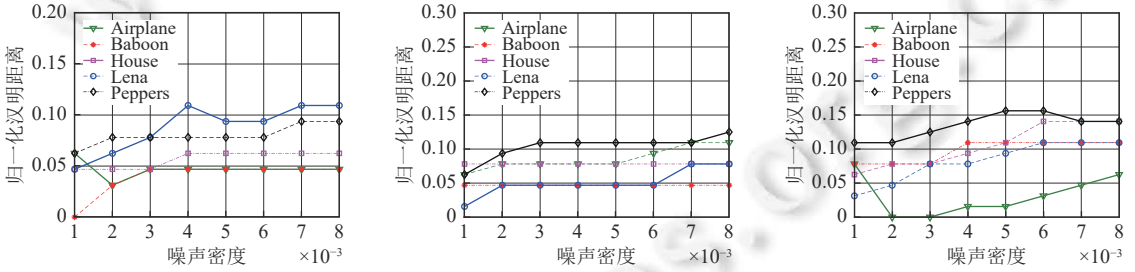
(a) JPEG 压缩和高斯低通滤波组合操作, 从左往右图像品质因数分别为 30、60、90



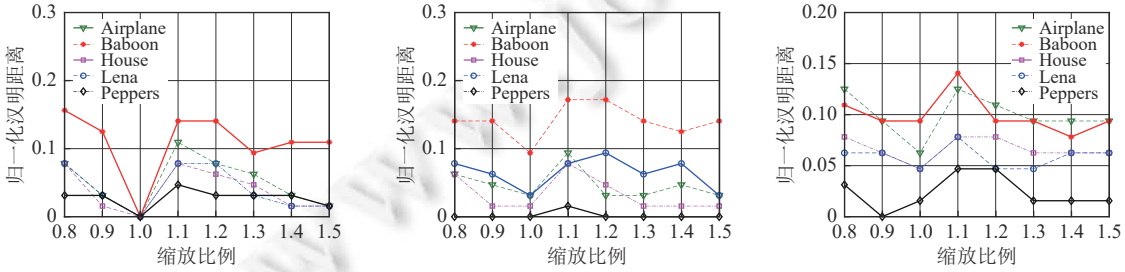
(b) JPEG 压缩和伽马校正组合操作, 从左往右图像品质因数分别为 30、60、90



(c) JPEG 压缩和椒盐噪声组合操作, 从左往右图像品质因数分别为 30、60、90



(d) 均值滤波和斑点噪声组合操作, 从左往右图像窗尺寸分别为 3、9、15



(e) 中值滤波和缩放组合操作, 从左往右图像窗尺寸分别为 1、7、13

图 7　组合的内容保持图像处理操作下的鲁棒性结果

表 2　对图像库中图像做内容保持操作后哈希对间的归一化汉明距离 d 统计信息

图像操作	最小值	最大值	均值	方差
JPEG压缩	0	0.156	0.035	0.029
高斯低通滤波	0	0.266	0.051	0.053
伽马校正	0	0.094	0.016	0.019
缩放	0	0.188	0.040	0.036
均值滤波	0	0.156	0.047	0.031
中值滤波	0	0.141	0.042	0.036
椒盐噪声	0	0.203	0.052	0.038
斑点噪声	0	0.203	0.055	0.042
JPEG压缩+高斯低通滤波	0	0.141	0.071	0.030
JPEG压缩+伽马校正	0	0.098	0.014	0.015
JPEG压缩+椒盐噪声	0	0.269	0.048	0.049
均值滤波+斑点噪声	0	0.245	0.043	0.046
中值滤波+缩放	0	0.261	0.050	0.052

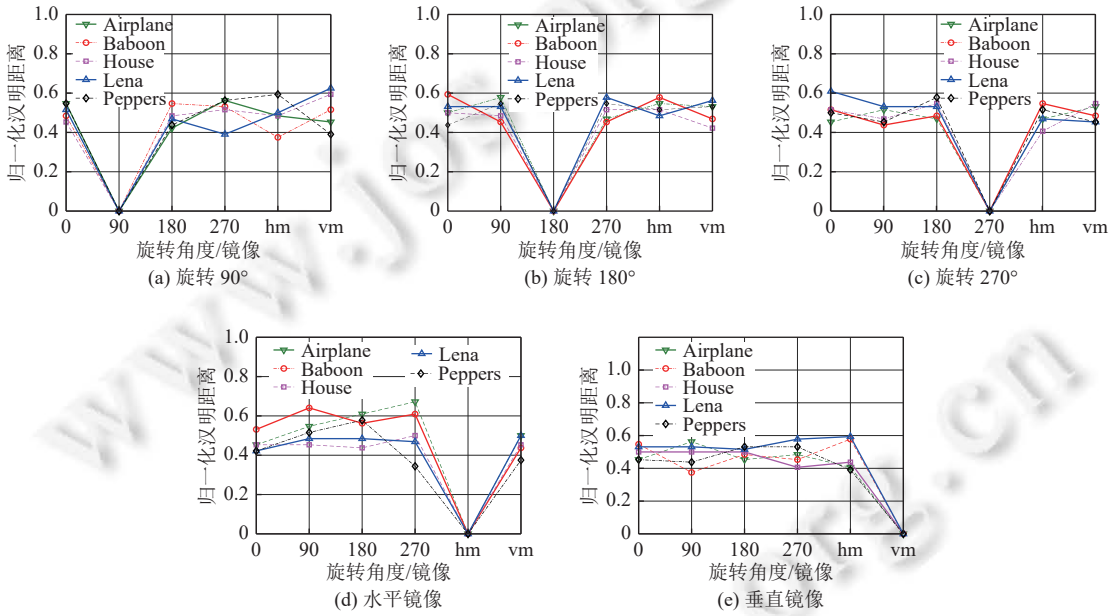


图 8　针对旋转及镜像操作的鲁棒性结果

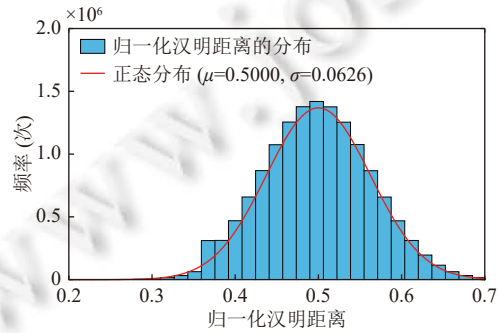


图 9　UCID 图像库中 1 338 张视觉不同图像的哈希对之间的归一化汉明距离分布

公式 (21) 中 exp(·) 表示以自然常数 e 为底的指数函数, 而 erfc(·) 表示互补误差函数. 因此, 可以计算出不同阈值 T 下的碰撞概率 P_c, 如表 3 所示. 显然, 阈值 T 设置得越小, 碰撞概率 P_c 越小. 另一方面, 由于两个视觉相似图像的哈希对之间的归一化汉明距离应该小于阈值 T, 因此, 较小的阈值 T 可能会影响感知鲁棒性. 由第 2.4 节的鲁棒性实验可以知道, 在几种常用的图像操作下, 本文方案的归一化汉明距离 d 几乎都小于 0.27, 当 T 等于 0.27 时, 本文图像哈希方案的碰撞概率为 1.1933×10^{-4}, 对于图像检索和认证的应用来说足够小. 因此, 在本文方案中, 可以将阈值 T 设置为 0.27, 以同时获得感知鲁棒性和抗冲突性两种表现之间的令人满意的折衷.

表 3 不同阈值 T 下的碰撞概率

阈值T	P_c
0.20	8.2427×10^{-7}
0.22	3.8593×10^{-6}
0.24	1.6382×10^{-5}
0.26	6.3072×10^{-5}
0.27	1.1933×10^{-4}
0.28	2.2039×10^{-4}
0.30	6.9943×10^{-4}

2.6 性能比较

为了证明本文哈希性能的优越性, 将本文哈希方案与 4 个典型哈希算法 (WLBP_CA[24]、RP_IVD[25]、RP_NMF[26]、CV_Canny[27]) 进行了比较. 由于唯一性与图像哈希方案的感知鲁棒性相矛盾, 因此, 为了公平地进行 5 种方案的比较, 将感知鲁棒性和唯一性的综合性能视为区分视觉相似和不同图像的分类能力, 即用 ROC 曲线进行性能评估. 图 10 为本文哈希方案与 WLBP_CA[24]、RP_IVD[25]、RP_NMF[26]、CV_Canny[27]哈希方案的 ROC 曲线, 来展示基于感知鲁棒性和唯一性整体性能的分类能力的比较, 其中横坐标和纵坐标分别表示真阳性率 P_T 和假阳性率 P_F. 随机选取 UCID 中 80 张不同的图片, 计算它们哈希值之间的归一化汉明距离, 共 (80×79)/2= 3160 组. 选取 Aerials、Miscellaneous 共 50 张不同图片, 每张图片按照表 1 的前 8 种图像操作, 每种操作 8 个参数变化, 生成 50×8×8=3200 张加噪图片, 计算它们的哈希值与原始图像哈希值之间的归一化汉明距离 d, 共 3200 组, 用来进行对比实验.

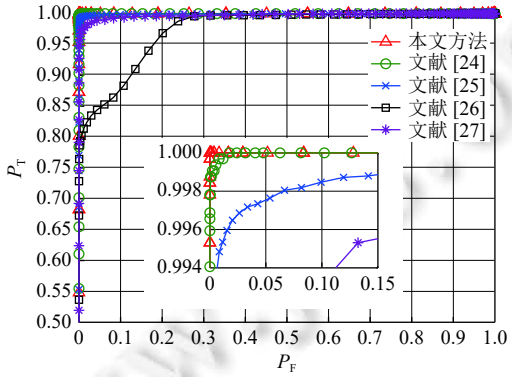


图 10 不同算法的 ROC 性能曲线比较

从图 10 中可以看出, 本文方案的 ROC 曲线比 WLBP_CA[24]、RP_IVD[25]、RP_NMF[26]、CV_Canny[27]方案的 ROC 曲线更接近左上角. 当 $P_T=1$ 时, 本文算法的 P_F 接近于 0, 而文献 [24−27] 的 P_F 分别为 0.017、0.663、0.950 和 0.608. 当 $P_F=0$ 时 , 本文算法的 P_T 为 0.9984, 而文献 [24−27] 的 P_T 分别为 0.9978、0.7701、0.5365 和 0.8569. 由此可见, 本文算法的鲁棒性和唯一性的综合性能优于文献 [24−27].

2.7 图像认证的应用

当图像哈希用于图像认证时, 需要分别计算原始图像的哈希值与潜在篡改版本的哈希值, 通过将二者之间的归一化汉明距离与预定阈值进行比较, 可以判断待认证图像是否被篡改, 若归一化汉明距离大于预定阈值, 则判断待认证图像被篡改, 反之则判断待认证图像未被篡改.

为了展示我们方案的图像认证能力, 我们从 UCID 数据库中选择了 4 幅图像, 并对这 4 幅图像分别进行了不同方式的篡改, 如图 11 所示, (a)、(c)、(e)、(g) 为 4 幅原始图像, (b)、(d)、(f)、(h) 为其对应的篡改版本. 表 4 列出了原始图像哈希与其篡改版本哈希之间的归一化汉明距离, 我们可以发现, 它们的归一化汉明距离都大于阈值 T =0.27, 这意味着篡改操作导致图像哈希发生了显著变化, 我们的方案在图像认证应用上可以达到令人满意的性能.

(a) 原始图像 1 (b) 篡改图像 1 (c) 原始图像 2 (d) 篡改图像 2

(e) 原始图像 3 (f) 篡改图像 3 (g) 原始图像 4 (h) 篡改图像 4

图 11 原始图像和相应的篡改版本

表 4 原始图像哈希与其篡改版本哈希之间的归一化汉明距离

图像	归一化汉明距离
图11(a)和图11(b)	0.2969
图11(c)和图11(d)	0.2813
图11(e)和图11(f)	0.3594
图11(g)和图11(h)	0.2813

3 实验结果与分析

本文提出了一种基于 Paillier 同态加密的图像哈希算法, 实现加密域中图像哈希的生成, 可应用于基于安全云计算的图像认证. 算法在图像哈希生成过程中, 引入了 Watson 矩阵, 使得生成哈希具有人眼视觉特性, 同时由于密钥控制的伪随机矩阵的存在, 使得在不同密钥下会得到不同的图像哈希值, 保证了算法的安全性. 实验结果表明本文哈希算法具有较好的鲁棒性, 并对固定角度旋转以及镜像操作鲁棒, 同时也具有较好的唯一性. 与一些典型的明文域图像哈希算法相比, ROC 曲线表明了本文算法在感知鲁棒性和分类性能方面的优越性. 另外, 安全性实验证明了, 在没有正确的伪随机矩阵生成密钥和加密解密密钥的情况下, 攻击者无法得到正确的图像哈希值. 将来的研究方向包括使算法对于任意角度旋转鲁棒, 在加密域计算效率方面进一步提高等.

References:

[1] Pun CM, Yan CP, Yuan XC. Image alignment-based multi-region matching for object-level tampering detection. IEEE Trans. on

Information Forensics and Security, 2017, 12(2): 377–391. [doi: 10.1109/TIFS.2016.2615272]

[2] Wang XF, Zhou XR, Zhang Q, Xu BC, Xue JR. Image alignment based perceptual image hash for content authentication. Signal Processing: Image Communication, 2020, 80: 115642. [doi: 10.1016/j.image.2019.115642]

[3] Du L, Ho ATS, Cong RM. Perceptual hashing for image authentication: A survey. Signal Processing: Image Communication, 2020, 81: 115713. [doi: 10.1016/j.image.2019.115713]

[4] Schneider M, Chang SF. A robust content based digital signature for image authentication. In: Proc. of the 3rd IEEE Int'l Conf. on Image Processing. Lausanne: IEEE, 1996. 227–230. [doi: 10.1109/ICIP.1996.560425]

[5] Liu YL, Xin GJ, Xiao Y. Robust image hashing using Radon transform and invariant features. Radioengineering, 2016, 25(3): 556–564. [doi: 10.13164/re.2016.0556]

[6] Tang ZJ, Zhang XQ, Dai YM, Lan WW. Perceptual image hashing using local entropies and DWT. The Imaging Science Journal, 2013, 61(2): 241–251. [doi: 10.1179/1743131X11Y.0000000039]

[7] Qin C, Chang CC, Tsou PL. Robust image hashing using non-uniform sampling in discrete Fourier domain. Digital Signal Processing, 2013, 23(2): 578–585. [doi: 10.1016/j.dsp.2012.11.002]

[8] Duan J, Zhou JT, Li YM. Secure and verifiable outsourcing of large-scale nonnegative matrix factorization (NMF). IEEE Trans. on Services Computing, 2021, 14(6): 1940–1953. [doi: 10.1109/TSC.2019.2911282]

[9] Chang V, Ramachandran M. Towards achieving data security with the Cloud Computing adoption framework. IEEE Trans. on Services Computing, 2016, 9(1): 138–151. [doi: 10.1109/TSC.2015.2491281]

[10] Xia ZH, Wang XH, Zhang LG, Qin Z, Sun XM, Ren K. A privacy-preserving and copy-deterrence content-based image retrieval scheme in Cloud Computing. IEEE Trans. on Information Forensics and Security, 2016, 11(11): 2594–2608. [doi: 10.1109/TIFS.2016.2590944]

[11] Jiang LZ, Xu CX, Wang XF, Luo B, Wang HQ. Secure outsourcing SIFT: Efficient and privacy-preserving image feature extraction in the encrypted domain. IEEE Trans. on Dependable and Secure Computing, 2020, 17(1): 179–193. [doi: 10.1109/TDSC.2017.2751476]

[12] Erkin Z, Franz M, Guajardo J, Katzenbeisser S, Lagendijk I, Toft T. Privacy-preserving face recognition. In: Proc. of the 9th Int'l Symp. on Privacy Enhancing Technologies. Seattle: Springer, 2009. 235–253. [doi: 10.1007/978-3-642-03168-7_14]

[13] Hsu CY, Lu CS. , Pei SC. Image feature extraction in encrypted domain with privacy-preserving SIFT. IEEE Trans. on Image Processing, 2012, 21(11): 4593–4607. [doi: 10.1109/TIP.2012.2204272]

[14] Hu SS, Wang Q, Wang JJ, Qin Z, Ren K. Securing SIFT: Privacy-preserving outsourcing computation of feature extractions over encrypted image data. IEEE Trans. on Image Processing, 2016, 25(7): 3411–3425. [doi: 10.1109/TIP.2016.2568460]

[15] Chen GM, Chen Q, Zhu XY, Chen YQ. Encrypted image feature extraction by privacy-preserving MFS. In: Proc. of the 7th Int'l Conf. on Digital Home (ICDH). Guilin: IEEE, 2018. 42–45. [doi: 10.1109/ICDH.2018.00016]

[16] Xia ZH, Jiang LQ, Ma XH, Yang WY, Ji PZ, Xiong NN. A privacy-preserving outsourcing scheme for image local binary pattern in secure industrial Internet of Things. IEEE Trans. on Industrial Informatics, 2020, 16(1): 629–638. [doi: 10.1109/TII.2019.2913217]

[17] Yang TF, Ma JF, Wang Q, Miao YB, Wang X, Meng Q. Image feature extraction in encrypted domain with privacy-preserving Hahn moments. IEEE Access, 2018, 6: 47521–47534. [doi: 10.1109/access.2018.2866861]

[18] Wang XY, Ma JF, Miao YB. Efficient privacy-preserving image retrieval scheme over outsourced data with multi-user. Journal on Communications, 2019, 40(2): 31–39 (in Chinese with English abstract). [doi: 10.11959/j.issn.1000-436x.2019023]

[19] Xiang SJ, Yang L. Robust and reversible image watermarking algorithm in homomorphic encrypted domain. Ruan Jian Xue Bao/Journal of Software, 2018, 29(4): 957–972 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5406.htm [doi: 10.13328/j.cnki.jos.005406]

[20] Paillier P. Public-Key cryptosystems based on composite degree residuosity classes. In: Proc. of the Int 'l Conf. on Advances in Cryptology. Prague: Springer, 1999. 223–238. [doi: 10.1007/3-540-48910-X_16]

[21] Li ZY, Gui XL, Gu YJ, Li XS, Dai HJ, Zhang XJ. Survey on homomorphic encryption algorithm and its application in the privacy-preserving for cloud computing. Ruan Jian Xue Bao/Journal of Software, 2018, 29(7): 1827–1851 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5354.htm [doi: 10.13328/j.cnki.jos.005354]

[22] USC. The USC-SIPI image database. 2019. http://sipi.usc.edu/database/

[23] Schaefer G, Stich M. UCID: An uncompressed color image database. In: Proc. of SPIE 5307, Storage and Retrieval Methods and Applications for Multimedia 2004. San Jose: SPIE, 2003. 472–480. [doi: 10.1117/12.525375]

[24] Qin C, Hu YC, Yao H, Duan XT, Gao LP. Perceptual image hashing based on weber local binary pattern and color angle representation. IEEE Access, 2019, 7: 45460–45471. [doi: 10.1109/ACCESS.2019.2908029]

[25] Tang ZJ, Zhang XQ, Li XX, Zhang SC. Robust image hashing with ring partition and invariant vector distance. IEEE Trans. on Information Forensics and Security, 2016, 11(1): 200–214. [doi: 10.1109/TIFS.2015.2485163]

[26] Tang ZJ, Zhang XQ, Zhang SC. Robust perceptual image hashing based on ring partition and NMF. IEEE Trans. on Knowledge and Data Engineering, 2014, 26(3): 711–724. [doi: 10.1109/TKDE.2013.45]

[27] Tang ZJ, Huang LY, Zhang XQ, Lao H. Robust image hashing based on color vector angle and Canny operator. AEU-Int'l Journal of Electronics and Communications, 2016, 70(6): 833–841. [doi: 10.1016/j.aeue.2016.03.010]

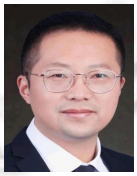
附中文参考文献:

[18] 王祥宇, 马建峰, 苗银宾. 高效隐私保护的多用户图像外包检索方案. 通信学报, 2019, 40(2): 31–39. [doi: 10.11959/j.issn.1000-436x.2019023]

[19] 项世军, 杨乐. 基于同态加密系统的图像鲁棒可逆水印算法. 软件学报, 2018, 29(4): 957–972. http://www.jos.org.cn/1000-9825/5406.htm [doi: 10.13328/j.cnki.jos.005406]

[21] 李宗育, 桂小林, 顾迎捷, 李雪松, 戴慧珺, 张学军. 同态加密技术及其在云计算隐私保护中的应用. 软件学报, 2018, 29(7): 1827–1851. http://www.jos.org.cn/1000-9825/5354.htm [doi: 10.13328/j.cnki.jos.005354]

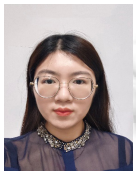
秦川(1980－), 男, 博士, 教授, CCF 高级会员, 主要研究领域为多媒体信息安全, 信息隐藏, AI 安全, 密文域信号处理, 数字取证.



钱振兴(1981－), 男, 博士, 教授, 主要研究领域为多媒体信息安全, 信息隐藏, AI 安全, 密文域信号处理, 数字取证.

郭梦琦(1995－), 女, 硕士生, 主要研究领域为多媒体信息安全, 密文域信号处理.

张新鹏(1975－), 男, 博士, 教授, 主要研究领域为多媒体信息安全, 信息隐藏, AI 安全, 密文域信号处理, 数字取证.



李欣然(1992－), 女, 博士生, 主要研究领域为多媒体信息安全, 信息隐藏, AI 安全.