基于有序等价划分的冗余空间转移图像加密安全性分析

陈 帆[1],屈凌峰[1],原长琦[2],和红杰[1]
(1. 西南交通大学信息科学与技术学院,四川成都 611756; 2. 北京电子技术与应用研究所,北京 100091)

摘 要: 现有的冗余空间转移(RST)图像加密算法有效提高了加密图像可逆数据隐藏的隐藏容量和抵抗现有已知明文攻击的能力. 在分析 RST 图像加密三个密钥特性和定义有序等价集的基础上,提出一种基于有序等价划分的已知明文攻击方法. 对得到的明-密图像对(原始图像及其加密图像),首先基于直方图距离比较重建原始图像的位平面置乱图像(BPSI),然后对 BPSI 的每个图像块,在加密图像划分得到的有序等价集中查找并推断该图像块的块置乱密钥(BSK). 推导给出了 BSK 估计准确率与分块大小、图像块个数和有序等价集个数的关系. 实验结果表明,对 512×512 的测试图像,当分块大小不小于 4×4 时,BSK 估计准确率超过 0.95;不同 BSK 估计准确率得到解密图像的视觉效果表明,即使 BSK 估计准确率低至 0.50,也可能导致原始图像的内容信息泄露.

关键词: 可逆信息隐藏; 图像加密; 有序等价划分; 冗余空间转移
中图分类号: TP391 **文献标识码:** A **文章编号:** 0372-2112 (2021)04-0665-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.12263/DZXB.20200126

Ordered Equivalence Division Based Cryptanalysis of Redundant-Space-Transfer Image Encryption

CHEN Fan[1], QU Ling-feng[1], YUAN Chang-qi[2], HE Hong-jie[1]
(1. *School of Information Science and Technology, Southwest Jiaotong University, Chengdu, Sichuan* 611756, *China*;
2. *Beijing Institute of Electronics Technology and Application, Beijing* 100091, *China*)

Abstract: The existing redundant-space transfer (RST) image encryption method adopted in the reversible data hiding in encrypted images scheme improved the embedding capacity and the ability against the existing known plaintext attacks. To address the RST image encryption, based on the analysis of three key characteristics of RST image encryption and the definition of ordered equivalence set (OES), the ordered equivalence division-based known plaintext attack method is proposed. For the obtained plain-cipher image pair, i. e., original image and its corresponding encrypted image, the bit-plane scrambling image (BPSI) of the original image is first reconstructed based on the histogram distance comparison. And then for each block in the BPSI, the block scrambling key (BSK) of it is searched and inferred in the OESs obtained by dividing all blocks of encrypted image. We make an analysis on the relation of the SK estimation accuracy with block size, image block number and ordered equivalence set number. Experimental results demonstrate that the BSK estimation accuracy is not less than 0.95 when block size is not less than 4×4 for the test images of 512×512 pixels. Also, the visual effect on the decrypted images obtained from the BSK estimation accuracy of 0.51 to 0.94 shows that the content information of the original image may be leaked even when the BSK estimation accuracy is as low as about 0.50.

Key words: reversible data hiding; image encryption; ordered equivalent division; redundant space transfer

1 引言

随着通信、云计算和大数据等技术的发展,图像、视频等各种数字媒体保存在开放或半开放云环境中,为用户存储、管理和远程访问数据提供了便利. 不过,iCloud 艳照门、Snapchap 照片等泄密事件发生,也使用

收稿日期:2020-01-20;修回日期:2020-11-15;责任编辑:李勇锋
基金项目:国家自然科学基金(No. 61872303, No. U936113)

户对所有权与管理权分离的云存储产生安全顾虑[1~3]. 云存储数字媒体的内容安全、隐私保护和便捷管理等需求,推动着加密域可逆信息隐藏(Reversible Data Hiding,RDH)技术的发展[2,4,5]. 近年来加密图像 RDH 技术在可逆性、隐藏容量、解密图像质量等方面取得了较多研究成果. 以隐藏容量为例,从早期算法不足 0.01bpp (bit per pixel)[4],逐步提高至 0.3 bpp[5,6] 和 0.5bpp[7,8],接近或超过 1bpp [9~11]. 同时,图像加密方法是直接影响加密图像 RDH 技术的隐藏容量和图像内容安全. 传统像素置乱[12]、像素异或与置乱[13]等图像加密方法生成的加密图像,很难隐藏附加数据以及得到近似的解密图像. 因此,加密图像 RDH 算法需要设计特殊的图像加密算法.

现有 RDHEI 算法中,流密码按位异或 (Bitwise XOR,BXOR)图像加密的速度快、生成的加密图像类随机噪声且位平面间相互独立[5]. 这些特点为通过修改图像的部分位平面实现附加信息嵌入、同时利用图像相关性对含密-加密图像的解密与恢复提供了可能. 因此,BXOR 图像加密被现有加密图像 RDH 算法[8,9] 采用. 不过,如果攻击者得到相同密钥生成的多幅加密图像,利用自然图像的局部相关性,能以较高的概率估计出密钥流[14]. 也就是说,密钥流重用条件下,BXOR 很难抵抗文献[14]提出的唯密文攻击. 为提高安全性,研究者提出 BXOR 与置乱相结合的图像加密算法[6,7] 以提高算法抵抗唯密文攻击的能力,不过算法的嵌入容量较低. 最近,Liu 等[10] 提出一种基于冗余信息转移(Redundant Space Transfer, RST)图像加密的 RDH 算法,提高抵抗唯密文攻击能力的同时,还有效提高了算法隐藏容量,一些平滑图像的嵌入容量接近甚至超过 2bpp. 这主要是由于 RST 图像加密依次将位平面、块和块内像素置乱加密相结合,实现了对像素值和像素位置双重保护,同时还将原始图像冗余信息转移至加密图像. RST 图像加密有效提高了算法抵抗已知攻击的能力,包括唯密文攻击[14] 和各种针对图像置乱的已知明文攻击[15~17].

不过,我们研究发现,RST 图像加密在已知明文攻击下仍存在图像内容泄露的隐患. 为验证 RST 图像加密存在的安全隐患,本文提出一种针对 RST 图像加密的已知明文攻击方法. 攻击者只要得到明-密图像对,就能以较高概率估计置乱密钥流,从而可获取相同密钥生成的其它加密图像的内容信息. 本文的主要贡献如下:(1) 定义图像直方图距离,设计基于直方图距离的位平面置乱密钥的准确估计方法;(2) 定义有序块和有序等价集,提出一种基于有序等价划分的块置乱密钥估计算法,推导给出块置乱密钥估计准确率与块大小、有序等价集个数和图像块个数的关系;(3)设计可能的安全策略以提高 RST 图像加密算法的安全性.

2 对 RST 图像加密的已知明文攻击

首先分析 RST 图像加密算法的特性,然后依次给出在攻击者已知明文-密文图像对(O,Z)的条件下,本文提出的估计位平面置乱密钥和估计块置乱密钥的方法.

2.1 RST 图像加密特性

置乱加密广泛应用于分组密码[18]、图像加密算法等构造中[19]. RTS 图像加密算法由三重置乱加密构成,置乱单位依次为位平面、图像块和块内像素.

Step1 基于 Π^1 的位平面置乱 将大小为 $m\times n$ 的原始灰度图像 $O=\{P_b\mid b=1,2,\cdots,8\}$ 以位平面为单位置乱加密得到位平面置乱图像(BPSI: Bit-Plane Scrambled Image)X.

$$X=\sum_{b=1}^{8}P_{\pi^1(b)}\times 2^{b-1} \tag{1}$$

其中,$\Pi^1=\{\pi^1(1),\cdots,\pi^1(8)\}$ 为密钥,文献[10]对 Π^1 限制如下,

$$\pi^1(b)\in\begin{cases}\{6,7,8\}, & \text{if } 1\leqslant b\leqslant 3\\ \{1,2,3,4,5\}, & \text{if } 3\leqslant b\leqslant 8\end{cases} \tag{2}$$

Step2 基于 Π^2 的图像块置乱 将 BPSI X 划分大小为 $s\times s$ 的 N 个不重叠图像块$\{X_i\}$,利用密钥 $\Pi^2=\{\pi^2(1),\cdots,\pi^2(N)\}$ 得到块置乱图像(BSI: Block Scrambled Image)$Y=\{Y_i\}$,

$$Y_i=X_{\pi^2(i)} \tag{3}$$

s 要大于 1 以实现原始图像“块内冗余信息”转移至加密图像.

Step3 基于 Π^3 的块内像素置乱 对 BSI 的每个图像块 Y_i,以像素为单位置乱加密得到加密图像 $Z=\{Z_i\}$.

RST 图像加密算法会产生安全隐患的原因在于:(1) Π^1 的密钥空间较小($3!\times 5!=720$)且像素的0/1比例不变;(2) Π^3 为弱密钥,由于块内像素置乱不改变原始图像的低频信息(块均值下采样不变),很难实现对图像内容的保护;(3) 图像块 Y_i 和 Z_i 的有序块相同.

$$\overrightarrow{Y_i}=\overrightarrow{Z_i} \tag{4}$$

图像块的有序块定义如下.

定义 1 有序块 对图像块(以 Y_i 为例) $Y_i=\{y_{i,j}\mid j=1,2,\cdots,s^2\}$,块内所有像素按像素值大小排序,得到的新图像块称为该图像块的有序块,$\overrightarrow{Y_i}=\{\overrightarrow{y_{i,j}}\mid j=1,2,\cdots,s^2\}$,

$$\overrightarrow{y_{i,1}}\leqslant\overrightarrow{y_{i,2}}\leqslant\cdots\leqslant\overrightarrow{y_{i,s^2}} \tag{5}$$

$$\forall j\in[1,s^2],\exists j'\in[1,s^2]\quad \text{s.t.}\quad \overrightarrow{y_{i,j}}=y_{i,j'} \tag{6}$$

$$\sum_{j=1}^{s^2} \overrightarrow{y_{i,j}} = \sum_{j=1}^{s^2} y_{i,j} \tag{7}$$

上述三个特性使攻击者根据明文图像 O 和密文图像 Z 准确推出密钥 Π^1,进而估计出 Π^2 成为可能.

2.2　基于直方图距离的 Π^1 估计

为找到密钥 Π^1 的判断条件并证明其合理性,首先给出直方图距离的定义.

定义 2　直方图距离　设 I_1 和 I_2 为两幅图像,相应直方图表示为 $H^{I_1}=\{h_i^{I_1}\mid i=0,1,\cdots,255\}$ 和 $H^{I_2}=\{h_i^{I_2}\mid i=0,1,\cdots,255\}$,则图像 I_1 和 I_2 的直方图距离(Histogram Distance)定义为

$$D_H(I_1,I_2)=\sum_{h=0}^{255}(\mid h_i^{I_1}-h_i^{I_2}\mid>0) \tag{8}$$

显然,RST 图像加密中得到的 BPSI X 与加密图像 Z 的直方图距离 $D_H(X,Z)=0$. 因为密钥 Π^2 和 Π^3 的块置乱和块内像素置乱不会改变像素的值. 根据上述特性,本文设计的基于直方图距离的 Π^1 估计与 BPSI X 重构步骤如算法 1 所示.

算法 1　基于直方图距离的 Π^1 估计与 X 重构

根据明-密图像对(O,Z),估计 Π^1 并重构 X
Input:明文图像 O,加密图像 Z;
Output:置换密钥 Π^1,位平面置乱图像 X;
(1)根据排列组合生成 720 种置换密钥 Π_k^1;
(2)计算加密图像 Z 的直方图 $H^z=\{h_i^z\}$;
(3)For 每个密钥 $\Pi_k^1(k=1,2,\cdots,720)$ do
　(3.1) 根据式(3)计算 O 的 BPS X^k;
　(3.2)计算 X^k 的直方图 $H=\{h_i\mid i=0,1,\cdots,255\}$;
　(3.3) 按式(8)计算第 k 个直方图距离 $H(k)=D_H(Z,X^k)$;
End For
(4)If H 中存在唯一 0 元素 $H(a)$
　{估计成功,返回 $\Pi^1=\Pi_a^1$; $X=X^a$};
Else {估计失败,Return};
End If

2.3　基于有序等价划分的 Π^2 估计

为估计 Π^2,首先给出有序等价集及有序等价划分的定义.

定义 3　有序等价集　设大小相同的 δ 个图像块构成的有限集$\mathbb{B}=\{B_i\mid i=1,\cdots,\delta\}$,满足下面两个条件之一,则称$\mathbb{B}$为有序等价集.

(1)$\mathbb{B}$为单元素集,即 $\delta=1$;
(2)$\forall B_i,B_j\in\mathbb{B}$,满足$\overrightarrow{B_i}=\overrightarrow{B_j}$.

定义 4　图像的有序等价划分　设大小 $m\times n$ 图像 Z 划分为互不重叠图像块 $Z=\{Z_i\mid i=1,2,\cdots,N\}$,图像块大小为 $s\times s$. 将 N 个图像块划分为满足以下 4 个条件的 w 个有序等价集$\mathbb{B}_j$,所有$\mathbb{B}_j$构成的集合称为图像 Z 的有序等价划分,记为$\mathbb{B}$,

$$\mathbb{B}=\{\mathbb{B}_1,\cdots,\mathbb{B}_j,\cdots,\mathbb{B}_w\} \tag{9}$$

其中,四个条件如下:

(1)$\mathbb{B}_j(j\in[1,w])$非空,即 $\delta_j>0$;
(2)$\mathbb{B}_1\cup\cdots\cup\mathbb{B}_w=Z_1\cup\cdots\cup Z_N$;
(3)$\forall j\neq j'\in[1,w]$,$\mathbb{B}_j\cap\mathbb{B}_{j'}=\varnothing$;
(4)$\forall Z_i\notin\mathbb{B}_j,Z_{i'}\notin\mathbb{B}_j$,则$\overrightarrow{Z_i}=\overrightarrow{Z_{i'}}$不成立.

对给定图像和块大小,根据定义 4 能得到唯一的图像有序等价划分. 这是因为:(1) 对任一图像块有且仅能属于一个有序等价集$\mathbb{B}_j$;(2)所有有序等价图像块,属于同一个有序等价集. 图像有序等价集划分步骤如算法 2 所示.

算法 2　图像有序等价集划分算法

已知图像 Z 和图像块个数 N,得到$\mathbb{B}$和 w
Input:图像 Z,图像块个数 N;
Output:图像等价集$\mathbb{B}=\{\mathbb{B}_1,\cdots,\mathbb{B}_w\}$;
(1)将 Z 划分为 N 个图像块 $Z=\{Z_i\mid i=1,\cdots,N\}$;
(2)初始化$\mathbb{B}_1=\{Z_1\}$,$w=1$,$\delta_1=1$;
(3)For 对每个图像块 $X_i(i>1)$) do
　If $\exists$ $\mathbb{B}_j(j\in[1,w])$,其包含的图像块与 Z_i 有序等价
　　$\mathbb{B}_j=\mathbb{B}_j\cup\{Z_i\}$; $\delta_j=\delta_j+1$;
　Else
　　$w=w+1$; $\delta_w=1$; $\mathbb{B}_w=\{Z_i\}$;
　End If
End For
Return $\mathbb{B}$和 w (有序等价集个数);

根据算法 2 得到加密图像 Z 的有序等价划分$\mathbb{B}=\{\mathbb{B}_1,\cdots,\mathbb{B}_j,\cdots,\mathbb{B}_w\}$. 对 BPSI X 的任一图像块 $X_i(i\in[1,N])$,其相应密文块 $Z_{i'}$是通过置乱块内像素得到的,因此 X_i 与 $Z_{i'}$一定有序等价. 同时,根据定义 4 可知,对每个 $Z_{i'}(i'\in[1,N])$,有且仅存在唯一$j'\in[1,w]$值,使得 $Z_{j'}\in\mathbb{B}_{j'}^Z$. 算法 3 给出了基于有序等价集划分的块置乱密钥估计算法的详细步骤.

由算法 3 可知,对每个图像块 X_i,通过得到加密图像 Z 的有序等价划分,置乱密钥的搜索空间从图像块个数 N 降低为与之等价的有序等价集$\mathbb{B}_{j'}$中的图像块个数 $\delta_{j'}$. 因此,图像块置乱密钥 Π^2 的密钥空间从 $N!$ 降低至,

$$\mathbb{S}_{(\Pi^2)}=\prod_{j=1}^{w}(\delta_{j'})! \tag{10}$$

其中,$\prod(\cdot)$表示连乘积. 显然,w 越大,$\delta_{j'}$的最大值越小,密钥空间越小.

由算法 3 的步骤(3.2)可知,图像块 X_i 的置乱密钥 $\pi^2(i)$只可能是$\mathbb{B}_{j'}$中某个图像块的序号. 随机选择$\mathbb{B}_{j'}$中的一个图像块作为块 X_i 置换密钥的估计值$\Pi^2(i)$,其正确估计的概率为 $1/\delta_{j'}$. 由于图像块个数 N 等于所有 δ_j

的累加和,因此,算法 3 得到的密钥估计正确率等于 w 个有序等价集估计正确率的加权和,

$$\rho = \sum_{j=1}^{w} \frac{\delta_j}{\sum_{j=1}^{w} \delta_j} \times \frac{1}{\delta_j} = \sum_{j=1}^{w} \frac{1}{N} = \frac{w}{N} \tag{11}$$

也就是说,图像块置乱密钥估计正确率 ρ 与图像块个数 N 成反比,与图像有序等价划分的元素个数 w 成正比.

算法 3 基于有序等价集的估计 Π^2 算法

根据图像(X,Z)和图像块个数 N,估计 Π^2

Input:BPS 图像 X,加密图像 Z,N;

Output:估计置换密钥 Π^2;

(1)将 X 和 Z 分别划分为 N 个图像块$\{X_i\}$和$\{Z_i\}$;

(2)根据算法 2 得到图像 Z 有序等价集划分$\mathbb{B}$,$\mathbb{B}=\{\mathbb{B}_1,\cdots,\mathbb{B}_w\}$;

(3)For 图像 X 中的每个图像块 X_i do

(3.1) 在$\mathbb{B}$中查找与 X_i 等价的$\mathbb{B}_{j'}$;

(3.2)Π^2 的估计值等于$\mathbb{B}_{j'}$中最后一个图像块的序号;

(3.3) If $\delta_{j'}=1$

从$\mathbb{B}$删除$\mathbb{B}_{j'}$;

Else

从$\mathbb{B}_{j'}$删除最后一个块;$\delta_{j'}=\delta_{j'}-1$;

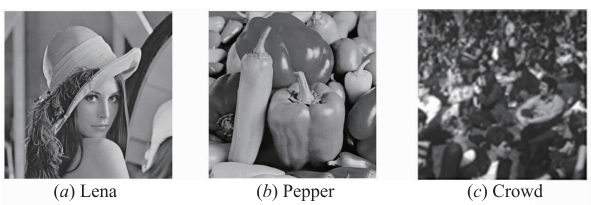
End If

End For

(4)Return Π^2;

3 实验结果及分析

选取常用的 6 幅大小为 512×512 且纹理复杂度不同的灰度图像 Lena、Pepper、Crowd、Baboon、Village 和 Man 作为测试图像,如图 1 所示.



(a) Lena (b) Pepper (c) Crowd

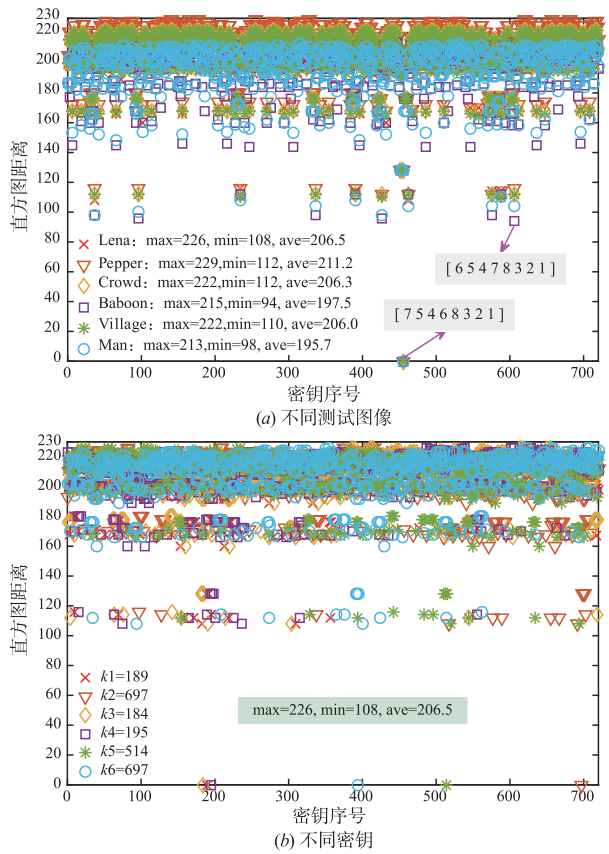
(d) Baboon (e) Village (f) Man

图1 6幅测试图像

本部分实验分析包括:(1)算法 1 估计密钥 Π^1 并重建 X 的概率及时间复杂度;(2)算法 3 得到的密钥 Π^2 估计正确率与块大小、纹理复杂度等的关系分析与验证.

3.1 Π^1 估计

由算法 1 可知,当密钥正确时得到的位平面置乱图像 X^k 与加密图像 Z 的直方图距离一定等于 0. 穷举位平面置乱密钥 Π^1 的所有可能取值,直方图距离 D_H 中一定存在 0 元素且唯一. 为验证不同条件下加密图像与 BPSI 的直方图距离 $D_H(X_{(j)},Z)$ 的统计分布,分别测试不同图像和不同密钥(相同图像)条件下的直方图距离统计分布如图 2 所示.



(a) 不同测试图像

(b) 不同密钥

图2 不同条件下加密图像Z与BPSI X的直方图距离

图 2(a)为 6 幅测试图像的 D_H 统计分布,其中加密图像的 Π^1 序号为456,该序号下对应的 Π^1 为{7 5 4 6 8 3 2 1}. 由图 2(a)可看出,6 幅图像在序号 456 的 D_H 为 0,其它点的 D_H 均大于 0. 图 1 中 6 幅测试图像 D_H 的均值依次为 206.5,211.2,206.3,197.5,206.0 和 195.7. 图 2(b)为 Lena 图像 6 个不同密钥(序号分别为 189,697,184,195,514 和 394)的 D_H 分布. 除了给定密钥点 D_H 等于 0 外,其它点的 D_H 均大于 0. 六个不同密钥对应的直方图距离 D_H 具有相同的最大值,最小值和均值,这主要是由于位平面置乱不会改变原始图像每个直方图的高度.

由图 2(a)和(b)还可看出,不同图像和不同密钥条件下存在少许 D_H 取值在 100 附近,偏离了 D_H 的分

布均值. 这是由于这些密钥与正确 Π^1 密钥的取值接近,但仍然远大于 0. 综上,对不同图像或密钥,当且仅当位平面置乱密钥 Π^1 相同时得到的 BPSI X 与 Z 的直方图距离等于 0,否则直方图距离大于 0. 因此,算法 1 一定能得到密钥 Π^1 并重构出 BPSI X.

算法 1 恢复位平面置乱顺序的攻击过程为穷举攻击,其时间复杂度与 Π^1 的密钥空间成正比. 算法 1 的 For 循环包括三个计算操作:位平面置乱、图像直方图和直方图距离. 设一次循环的时间为 $T_{<for>}$,则算法 1 的时间复杂度为,

$$O_{(\Pi^1)} = 720 \times T_{<for>} \tag{12}$$

在笔记本电脑 LG Gram Core i7-8550U (CPU), DDR4-2400MHz 16GB,MATLAB 2019b 实验环境,对 512×512 测试图像,执行算法 1 得到重构 BPSI X 的时间约为 38.048s. 也就是说,一次循环时间约等于 8.024/720 =0.0528s. 即使对位平面置乱不加限制,512×512 图像穷举攻击重构 BPSI 的时间约为 $T_{<for>} \times 8! = 2129$s,是完全可行的.

3.2　Π^2 估计准确率分析

由式(11)可知,本文算法得到 Π^2 的正确率 ρ 与图像块个数 N 成反比,与有序等价集个数 w 成正比. 对给定图像,N 依赖于分块大小 s,w 与有序等价集中等价块的多少有关,即依赖图像内容. 对 6 幅测试图像和不同分块大小 s,分别测试图像有序等价划分的等价集个数 w. 图 3 给出了 6 幅图像在不同块大小时的 $\rho(\rho = w/N)$ 值.

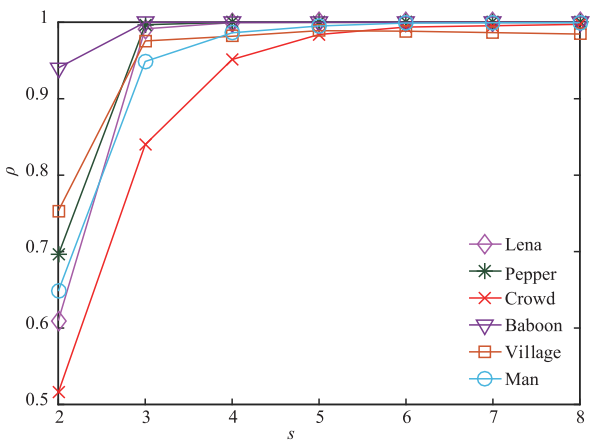


图3　不同条件下密钥Π^2估计准确率理论值

由图 3 可看出,理论的密钥估计准确率 ρ 随分块大小 s 的增加而提高. 当分块大小为 5×5 时,6 幅图像的 ρ 值都接近或等于 1,即 w 与 N 近似相等. 文献[10]块大小为 4×4(s 越大,图像加密算法的冗余转移性能越好,隐藏容量越大),此时 6 幅图像得到 Π^2 的正确率 ρ 分别为 0.9996,1,0.9514,1,0.9818 和 0.9863,均大于 0.95. 随着图像块的变小,存在有序等价块的概率变大,尤其是纹理复杂度低的平滑图像. 当 $s=2$ 时,6 幅图像的 ρ 值依次为 0.6087, 0.6959, 0.5157, 0.9404, 0.7532 和 0.6483.

为直观展示密钥估计正确率与图像内容信息泄露的关系,采用相同密钥生成 6 幅测试图像和 Couples 图像的加密图像. 首先,攻击者在得到一对明-密图像(O, Z)的条件下,分别根据 6 幅测试图像的明-密图像对,采用本文攻击方法得到密钥 Π^1 和 6 种不同正确率的 Π^2 估计值. 6 幅图像得到的 Π^2 估计正确率依次为:0.51 (Crowd),0.61 (Lena),0.65 (Man),0.69 (Pepper),0.75 (Village) 和 0.9404 (Baboon). 然后,利用上述 6 种密钥估计值,解密"加密 Couples 图像",得到 6 幅近似解密 Couples 图像,如图 4 所示.

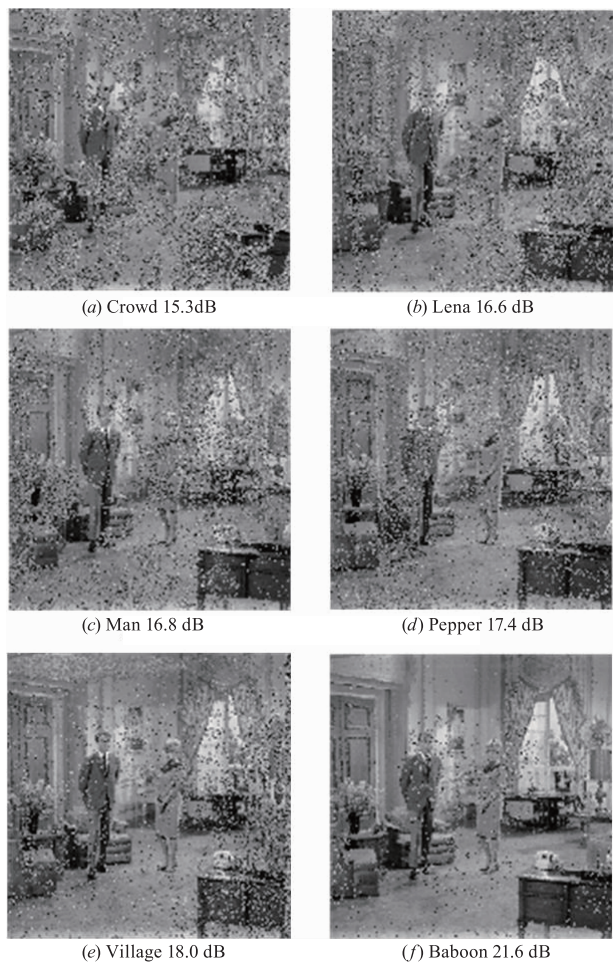


图4　不同明-密图像对估计密钥的解密Couples图像

近似解密 Couples 与原始 Couples 的 PSNR 依次为 15.3dB,16.6dB,16.8dB,17.4dB,18.0dB 和 21.6dB. 显然,密钥估计正确率越高,加密图像 Z 的内容信息泄露越严重. 此外,尽管图 4(a)中存在较多的噪声块,但能明显看出两个人的存在及其位置. 换句话说,块置乱密钥估计正确率即使低至 0.5 左右,也可能导致相同密钥

生成加密图像原始内容信息泄露.

综上可知,RST 图像加密算法存在加密图像内容信息泄露的安全风险.

4 安全策略

为不降低加密图像 RDH 的隐藏容量,安全策略应不影响 RST 图像加密算法的冗余转移性能. 根据文献[10]3.2.2 节的位平面压缩方法可知,只要图像加密前、后每个位平面的二值块中 0/1 个数不变,就不会影响 SMC(Sparse Matrix Compression)[10]压缩性能. 一种安全提升策略:以原始图像位平面的二值块为单位置乱加密,生成二值块置乱图像(Binary Block Scrambled Image,BBSI),再根据本文 2.1 节 Step 3 对 BBSI 进行块内像素置乱得到加密图像. BBSI 生成算法描述如下:

将大小 $m\times n$ 的原始图像 O 的 8 个位平面 P_b^O 分为 $s\times s$ 的二值块,根据 b 值将二值块 P_b^O 扫描为两个有序序列 $P_{b,i}^O(b=1,2,\cdots,8;i=1,2,\cdots,N)$,

$$\begin{cases} S^M=\{P_{6,1}^O,P_{6,2}^O,\cdots,P_{6,N}^O,P_{7,1}^O,\cdots,P_{8,N}^O\} \\ S^L=\{P_{1,1}^O,P_{1,2}^O,\cdots,P_{1,N}^O,P_{2,1}^O,\cdots,P_{5,N}^O\} \end{cases} \tag{13}$$

其中,S^M 和 S^L 分别为三个高位平面和 5 个低位平面的二值块序列,其长度分别为 $3N$ 和 $5N$. 利用密钥分别置乱序列 S^M 和 S^L 得到对应的置乱加密序列,按式(13)扫描的逆过程,即可重构得到 BBSI Y.

上述 BBSI 生成算法将位平面与图像块两个独立的置乱加密,合并为一个对图像位平面的"二值块置乱加密",去掉了置乱加密的中间结果 BPSI. 在保证二值块 SMC 压缩性能的前提下,既破坏了"构建与加密图像直方图距离为 0 的 BPSI"的条件,又扩大 RST 图像加密算法的密钥空间. 改进的 Liu[10]加密算法的密钥空间为 $(5N)!\times(3N)!\times(s^2)!$,远大于文献[10]加密算法的密钥空间 $720\times(N!)\times(s^2)!$.

5 结论

图像加密域可逆数据隐藏是云存储环境中协调图像内容安全、隐私保护和便捷管理的关键技术之一. 图像加密作为实现图像内容安全和隐私保护的关键步骤,对图像加密算法设计提出了更高的要求. 本文分析了文献[10]的冗余空间转移(RST)图像加密算法的安全性,指出该算法在已知明文攻击条件下存在图像内容信息泄露的风险. 其原因在于:RST 图像加密的位平面置乱密钥空间小,结合块内像素置乱有序等价性和弱密钥性,攻击者通过有序等价划分,以较高的概率估计块置乱密钥. 设计了一种以图像位平面的"二值块"为单位置乱加密安全策略,以兼顾 RST 图像加密算法的安全性和冗余转移性能. 上述研究为设计更安全的、适用于 RDHEI 技术的图像加密算法设计提供技术积累与参考.

参考文献

[1] 俞能海,郝卓,徐甲甲,等. 云安全研究进展综述[J]. 电子学报,2013,41(2):371-381.
YU Neng-hai, HAO Zhuo, XU Jia-jia, et al. Review of cloud computing security [J]. Acta Electronica Sinica, 2013,41(2):371-381. (in Chinese)

[2] ZHANG W,WANG H,HOU D,et al. Reversible data hiding in encrypted images by reversible image transformation [J]. IEEE Transactions on Multimedia,2016,18(8):1469-1479.

[3] 马燕. 苹果确认用户 iCloud 遭入侵隐私安全体系或存漏洞[OL]. https://tech.qq.com/a/20180309/003008.html,2018-03-09.

[4] SHI Y Q,LI X,ZHANG X,et al. Reversible data hiding: Advances in the past two decades[J]. IEEE Access,2016,4:3210-3237.

[5] ZHANG Xin-peng. Separable reversible data hiding in encrypted image[J]. IEEE Transactions on Information Forensics and Security,2012,7(2):826-832.

[6] HUANG F,HUANG J,SHI Y. New framework for reversible data hiding in encrypted domain[J]. IEEE Transactions on Information Forensics and Security,2016,11(12):2777-2789.

[7] 鄢舒,陈帆,和红杰. 异或-置乱框架下邻域预测加密域可逆信息隐藏[J]. 计算机研究与发展,2018,55(6):1211-1221.
YAN Shu,CHEN Fan,HE Hong-jie. Reversible data hiding in encrypted image based on neighborhood prediction using XOR-Permutation encryption [J]. Journal of Computer Research and Development,2018,55(6):1211-1221. (in Chinese)

[8] CAO X,DU L,WEI X,et al. High capacity reversible data hiding in encrypted images by patch-level sparse representation[J]. IEEE Transactions on Cybernetics,2016,46(5):1132-1143.

[9] PAULINE P,WILLIAM P. An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images[J]. IEEE Transactions on Information Forensics and Security,2018,13(7):1670-1681.

[10] LIU Z,PUN C. Reversible data hiding in encrypted images by redundant space transfer [J]. Information Sciences,2018,433-434:188-203.

[11] 王继军,孙泽锐,李国祥. 图像抛物线插值空间大容量可逆信息隐藏算法[J]. 电子学报,2019,47(1):139-146.
WANG Ji-jun,SUN Ze-rui,LI Guo-xiang. High capacity reversible data hiding algorithm based on parabolic interpolation space[J]. Acta Electronica Sinica,2019,47(1):

139 – 146. (in Chinese)
[12] LI S, LI C, CHEN G, et al. A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks[J]. Signal Processing: Image Communication, 2008, 23(3): 212 – 223.
[13] 林青,王延江,王珺. 基于超混沌系统的图像加密算法[J]. 中国科学:技术科学,2016,46(9):910 – 918.
LIN Q, WANG Y J, WANG J. The image encryption scheme with optional dynamic state variables based on hyperchaotic system[J]. Scientia Sinica (Technologica), 2016, 46(9): 910 – 918. (in Chinese)
[14] KHELIFI F. On the security of a stream cipher in reversible data hiding schemes operating in the encrypted domain [J]. Signal Processing, 2018, 143: 336 – 345.
[15] LI C, LO K T. Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks [J]. Signal Processing: Image Communication, 2009, 91 (4): 949 – 954.
[16] LI S, LI C, LO K T, et al. Cryptanalysis of an image scrambling scheme without bandwidth expansion [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2008, 18(3): 338 – 349.
[17] JOLFAEI A, WU X, et al. On the security of permutation-only image encryption schemes[J]. IEEE Transactions on Information Forensics and Security, 2016, 11 (2): 235 – 246.
[18] 王念平. 一类分组密码变换簇抵抗线性密码分析的安全性评估[J]. 电子学报,2020,48(1):137 – 142.
WANG Nian-ping. Security evaluation against linear cryptanalysis for a class of block cipher transform cluster [J]. Acta Electronica Sinica, 2020, 48(1): 137 – 142. (in Chinese)
[19] 范九伦,张雪锋,刘宏月. 密码学基础[M]. 西安:西安电子科技大学出版社,2008. 6 – 12.
FAN Jiu-lun, ZHANG Xue-feng, LIU Hong-yue. Fundamentals of Cryptography [M]. Xi'an: Xidian University Press, 2008. 6 – 12. (in Chinese)

作者简介

陈　帆　男,1971 年 8 月出生于河南平舆,博士,西南交通大学信息科学与技术学院副教授. 主要从事多媒体信息安全和数字水印等方面的研究.
E-mail:fchen@ swjtu. edu. cn

屈凌峰　男,1993 年 7 月出生于河南灵宝,西南交通大学信息科学与技术学院硕博连读生,主要从事图像加密域可逆信息隐藏等方面的研究.
E-mail:792443987@ qq. com

原长琦　男,1984 年 9 月生于陕西宝鸡,硕士,北京电子技术应用研究所助理研究员. 主要研究兴趣包括加密理论、信息安全等.

和红杰(通信作者)　女,1971 年 9 月出生于河南宝丰,博士,西南交通大学信息科学与技术学院教授. 主要从事多媒体信息安全和数字图像处理等方面的研究.
E-mail:hjhe@ swjtu. edu. cn