计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2021.20200011
58(4):849-861,2021

基于块调制-置乱的图像加密算法安全性分析

屈凌峰[1] 和红杰[1] 陈 帆[1] 张善俊[2]
[1](信号与信息处理四川省重点实验室(西南交通大学) 成都 610031)
[2](神奈川大学理学部计算机科学科 日本神奈川県平塚市 259-1293)
(792443987@qq.com)

Security Analysis of Image Encryption Algorithm Based on Block Modulation-Scrambling

Qu Lingfeng[1], He Hongjie[1], Chen Fan[1], and Zhang Shanjun[2]
[1](*Sichuan Key Laboratory of Signal and Information Processing* (*Southwest Jiaotong University*), *Chengdu* 610031)
[2](*Department of Information Science*, *the Faculty of Science*, *Kanagawa Univeristy*, *Hiratsuka City*, *Kanagawa*, *Japan* 259-1293)

Abstract Block modulation-scrambling image encryption is one of the common encryption methods for reversible data hiding in encrypted image (RDH-EI). It can effectively improve the embedding capacity of the algorithm and resist the existing ciphertext only and known plaintext attacks. For block modulation-scrambling image encryption, a key stream estimation method under known plaintext attack is proposed in this paper. First of all, the definition of image difference block is given, and it is pointed out that the ciphertext block generated by block modulation keeps the difference block unchanged with high probability. On this basis, a fast block scrambling key estimation method based on pseudo difference image construction and difference cube mean index search is proposed. The relationship between the cube mean distribution of the difference block and the block size and the accuracy of the scrambling key estimation is discussed. Finally, the possible solutions to improve the security of image encryption are given. The texture complexity and block size of the plaintext image are the main factors that affect the block scrambling key estimation accuracy and algorithm time complexity. When the block size is larger than 3×3, the accuracy of all test image block scrambling secret key estimation is more than 70%, at this time, the content information of ciphertext image is seriously leaked.

Key words reversible data hiding; image blocks scrambling encryption; known plaintext attack; image difference block; security analysis

摘 要 块调制-置乱图像加密是加密域可逆信息隐藏常用的加密方法之一,能有效提高算法的隐藏容量和抵抗现有唯密文、已知明文等攻击的能力.针对块调制-置乱图像加密,提出一种已知明文攻击条件下的密钥流估计方法.首先,定义图像差值块,分析指出块调制生成密文块以较高的概率保持差值块

收稿日期:2020-01-02;**修回日期**:2020-07-23
基金项目:国家自然科学基金项目(61872303,U1936113);四川省科技厅科技创新人才计划项目(2018RZ0143)
This work was supported by the National Natural Science Foundation of China (61872303, U1936113) and the Science and Technology Innovation Talents Program of Sichuan Science and Technology Department (2018RZ0143).
通信作者:陈帆(fchen@ swjtu.edu.cn)

不变的特性. 然后,提出一种伪差值图像构建、差值块立方均值索引查找等关键策略的块置乱密钥的快速估计方法. 分析讨论了图像的差值块立方均值分布、分块大小对置乱密钥估计正确率的关系. 最后,给出了提高图像加密安全性可能的解决方案. 实验结果表明,明文图像的纹理复杂度和分块大小是影响块置乱密钥估计正确率和算法时间复杂度的主要因素;分块大小大于 3×3 时,图像块置乱密钥的估计正确率达到 70%以上,密文图像的内容会被泄露.

关键词 可逆信息隐藏;图像块置乱加密;已知明文攻击;图像差值块;安全性分析

中图法分类号 TP391

图像加密域可逆信息隐藏(reversible data hiding in encrypted image, RDH-EI)是一种对原始图像加密后,在密文图像中可逆地隐藏附加信息,在接收端从含附加信息的密文图像提取信息后,能无损重建原始图像的技术.RDH-EI 结合密码学与信息隐藏技术,用来解决云存储场景中用户因图像所有权与管理权分离而产生的安全问题,已成为信息安全与云计算领域的研究热点[1-2].

近 10 多年发展,RDH-EI 在隐藏容量、解密图像质量等方面取得了较好的进展.以隐藏容量为例,从早期算法不足 0.01 bpp(bit per pixel)[3],逐步提高至 0.3 bpp[4-7]和 0.5 bpp[8],最新算法的隐藏容量已接近或超过 1 bpp.而对 RDH-EI 中加密算法的安全性研究才刚刚起步.加密算法的安全性事关图像内容安全保护的成败,对 RDH-EI 算法至关重要[2].传统图像加密(如像素异或与置乱[9-10]、像素置乱等)方法很难直接用于 RDH-EI 算法.这是因为加密图像不存在像素间冗余,难以腾出空间用于隐藏附加数据并得到高质量的解密图像.因此,RDH-EI 需要设计特殊的图像加密算法.

流密码加密[3-10]和块置乱加密[11-13]是 RDH-EI 常用的加密算法,流密码和块置乱加密算法具有简单、时间复杂度低的特点.然而,流密码加密方案已被证实无法抵抗唯密文攻击[2],且由于加密图像熵最大化,采用流密码加密的 RDH-EI 算法往往隐藏容量较低.相比于流密码加密,块置乱加密保留了图像块内像素值相关性,可有效提高 RDH-EI 算法的隐藏容量,然而,文献[14-16]的研究表明:置乱加密无法抵抗已知明文攻击.2008 年 Li 等人[14]分析并证明了对于已知明文攻击,利用不少于 $\log_L(2(MN-1))$ 对明文及其密文能获得较好的攻击效果,其中 MN 为图像大小,L 为最大灰度值;2011 年 Li 等人[15]分析文献[14]的算法时间复杂度,并基于二叉树查找原理降低了攻击算法的时间复杂度;2016 年文献[16]基于选择明文攻击,得到了完全正确的置乱序列,正确估计出置乱序列所需要的明文-密文对数为 $\log_L(MN)$;其他针对像素置乱加密的已知明文攻击如文献[17-18].

上述针对置乱加密所提出的已知明文攻击,均是基于置乱加密前后像素值不变的特点来进行攻击.当置乱加密后的图像像素值发生改变,上述已知明文攻击的基本条件将不再满足,生成的加密图像不仅可以抵抗文献[2]中提出的唯密文攻击,同时也可以抵抗上述提到的已知明文攻击.在尽可能多地保留加密图像冗余度的条件下,为了提高加密图像的安全性,2018 年 Liu 等人[19]提出了一种基于冗余信息转移的 RDH-EI 算法.该算法通过置乱图像的位平面改变原始图像的像素值,并有效提高了 RDH-EI 的嵌入容量.然而,我们研究发现[20],由于位平面置乱不改变像素位平面比特值,位平面置乱顺序在已知明文攻击下可以被精确估计.攻击者利用位平面置乱序列恢复原始图像的像素值,并估计块置乱序列导致密文图像内容泄露.

为提高安全性,RDH-EI 加密算法不仅要改变像素值大小还应进一步改变像素比特值.基于这一观点,研究者提出了块调制-置乱图像加密方案[21-24].块调制-置乱图像加密算法思想如下:首先将图像划分为不重叠的图像块;接着,在同一个图像块内,从[0,255]范围内产生一个随机数对块内像素进行模运算,改变明文图像像素的值,我们称这一过程为“块调制”;最后,将模运算后的图像块根据密钥进行置乱.块调制-置乱加密结合模运算和分块置乱加密,在密文图像块中保留了明文图像块内差值信息,有效提高隐藏容量.同时,由于块调制-置乱加密改变了明文图像的比特值,加密图像可以抵抗文献[20]提出的已知明文攻击.

不过,由于块调制-置乱加密算法在密文图像块中保留了明文图像块内像素间部分相关性,块调制-置乱加密算法在已知明文攻击的条件下仍存在安全隐患.为此,本文提出一种基于图像差值块分类查找

的已知明文攻击,可对块调制-置乱加密算法成功实施攻击.本文主要贡献有 3 个方面:

1) 定义差值直方图距离,通过明-密文差值图像迭代替换构建伪差值图像,明-密文伪差值直方图距离为 0,使得在明-密文图像间建立等量关系成为可能.

2) 定义差值块立方均值 ρ,将差值块分类并提出一种差值块分类查找的已知明文攻击方法,分析验证了块调制-置乱加密算法存在的安全隐患.

3) 分析已知明文攻击的时间复杂度,在保证加密图像空间冗余的前提下,给出抵抗已知明文攻击的解决方案.

1 块调制-置乱及特性分析

兼顾加密图像的安全性和隐藏容量,最新 RDH-EI 算法的研究采用块调制-置乱图像加密[21-24]策略生成加密图像.块调制-置乱加密不仅改变了像素值,同时打乱像素位置.用户通过密钥 $K=(key_1\ key_2)$ 生成的密文图像不仅能抵抗文献[2]提出的唯密文攻击,同时可以抵抗现有的已知明文攻击[17-18,20].另一方面,由于块调制-置乱加密算法保留了原始图像块像素间的部分相关性,有效提高了 RDH-EI 算法的隐藏容量,如文献[22]中 Lena 图像的隐藏容量达到 2.1 bpp,下面对块调制-置乱图像加密算法进行描述,并对其特性进行分析.

1.1 块调制-置乱图像加密

将大小为 $m\times n$ 的原始图像 X(以灰度图像为例)分为 N 个不重叠图像块 $X=\{X_i\mid i=1,2,\cdots,N\}$,每个图像块的像素个数为 $N_b=(m\times n)/N$.块调制-置乱图像加密可分为 2 步.

Step1. 块调制.由密钥 key_1 生成 N 个随机正整数集 R,$R=\{R_i\mid R_i\in[0,255],i=1,2,\cdots,N\}$,$R$ 即为图像块内像素值的调制密钥.图像块 X_i 中的像素值按式(1)加密,生成调制加密图像 E,$E=\{E_i\mid i=1,2,\cdots,N\}$.

$$E_i=(X_i+R_i)\bmod 256. \tag{1}$$

图像块 X_i 中所有像素的调制密钥 R 都相同.这样既改变了图像块中的像素值,又保留了原始图像块像素间的部分相关性.

Step2. 块置乱.由密钥 key_2 生成块置乱序列 Π,$\Pi=\{\pi(1),\cdots,\pi(i),\cdots,\pi(N)\}$,利用置乱序列 Π 置乱调制加密图像 E 中图像块,$E=\{E_i\mid i=1,2,\cdots,N\}$,得到密文图像 Y,$Y=\{Y_i\mid i=1,2,\cdots,N\}$,

$$Y_i=E_{\pi(i)}. \tag{2}$$

因此,块调制-置乱图像加密即改变了像素值,又改变了像素的位置.有效提高了算法抵抗现有唯密文攻击[2]和已知明文攻击[17-18,20]的能力.同时,密文图像块内还保留了原始图像块内部分像素间的相关性,为提高 RDH-EI 的隐藏容量提供了可能.文献[22]对密文图像块内像素值求差值,利用差值二叉树编码技术[22]使得 RDH-EI 算法的隐藏容量达到 2 bpp 以上.

不过,密文图像块内保留原始块的部分相关性,是否有可能带来新的安全隐患,是一个值得研究的问题.本文研究表明,当攻击者得到 1 对明-密文图像(X,Y)时,有可能估计出部分密钥,从而导致其他密文图像集的内容信息泄露.

1.2 块调制-置乱图像加密特性分析

设攻击者得到密文图像 $Y=\{Y_i\mid i=1,2,\cdots,N\}$及其对应的明文图像 $X=\{X_i\mid i=1,2,\cdots,N\}$.对任一明文块 X_i,$X_i=\{x_{i,j}\mid j=1,2,\cdots,N_b\}$,若能找到与其对应的密文块 Y_i,$Y_i=\{y_{i,j}\mid j=1,2,\cdots,N_b\}$,则该图像块对应的调制密钥 R_i 为

$$R_i=\begin{cases}y_{i,1}-x_{i,1}, & \text{若 } y_{i,1}\geqslant x_{i,1};\\ y_{i,1}-x_{i,1}+256, & \text{若 } y_{i,1}<x_{i,1}.\end{cases} \tag{3}$$

因此,如何在密文图像中找到明文块 X_i 对应的密文块 Y_i,$Y_i=E_{\pi(i)}$,即估计块置乱序列 Π 是已知明文攻击的主要工作.本文利用明-密文图像差值块对块调制-置乱图像加密实施已知明文攻击,估计块置乱序列.本节,给出图像差值块定义,分析并证明了明-密文图像差值块在加密前后有较高概率保持不变的特性,给出具体定义及分析.

定义 1. 图像差值块.对任一图像块 X_i(以明文图像块为例),$X_i=\{x_{i,j}\mid j=1,2,\cdots,N_b\}$.块内所有像素值与第 1 个像素值的差值,为图像块 X_i 对应的图像差值块 D_i,$D_i=\{d_{i,j}\mid j=1,2,\cdots,N_b\}$,称差值块.

$$d_{i,j}=x_{i,j}-x_{i,1},\ j=1,2,\cdots,N_b. \tag{4}$$

相应的密文差值块表示为 $D_{\pi(i)}$.明文图像 X 和密文图像 Y 中共有 N 对相互对应的图像块,表示为 $[X_i\ Y_i]_{i=1,2,\cdots,N}$.对明-密文所有图像块分别求差值,得到明文差值图像 $D^X=\{D_i\mid i=1,2,\cdots,N\}$和密文差值图像 $D^Y=\{D_{\pi(i)}\mid i=1,2,\cdots,N\}$,明-密文差值图像中 N 对相互对应的差值块表示为$[D_i\ D_{\pi(i)}]_{i=1,2,\cdots,N}$.

对于任意明文块 X_i,$x_{i,\max}$和 $x_{i,\min}$分别为明文块 X_i 中的最大值和最小值,块内调制密钥为 R_i.

根据调制加密前后差值块$[D_i\ D_{\pi(i)}]$是否发生改变，明文块被分为 Case1 和 Case2 这 2 种类型：

$$\text{Case1}:\begin{cases}(x_{i,\min}+R_i)-256>0,\\(x_{i,\max}+R_i)-256<0,\end{cases}\qquad(5)$$

Case2：其他.

当明文块 X_i 满足 Case1 时，与图像块$[X_i\ Y_i]$对应的差值块$[D_i\ D_{\pi(i)}]$满足 $D_i\equiv D_{\pi(i)}$，即差值块 D_i 与 $D_{\pi(i)}$ 中的差值大小相同.当明文块 X_i 满足 Case2 时，$D_i\neq D_{\pi(i)}$，即差值块 D_i 与 $D_{\pi(i)}$ 中的差值大小不同.

为直观描述 Case1 与 Case2，图 1 给出一个例子(以 2×2 图像块为例).对明文块 X_i，设调制密钥分别为 $R_i=96$，$R_i=91$，$R_i=94$ 时，生成 3 组对应的密文块 Y_i，如图 1 上方所示.由式(4)分别计算差值块如图 1 下方所示.

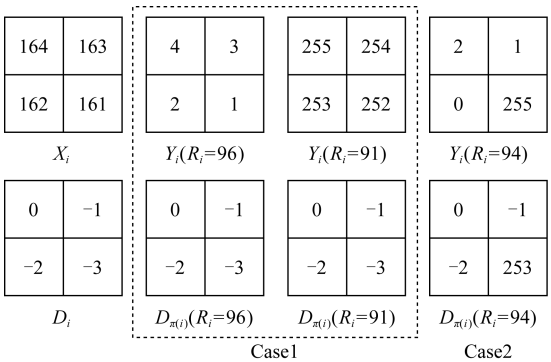

Fig. 1 Plaintext-ciphertext image block and difference block

图 1 明-密文图像块及差值块

由图 1 可看出，Case2 图像块在调制加密后块内差值发生变化，而 Case1 图像块在调制加密后块内差值不会发生变化，即满足 $D_i\equiv D_{\pi(i)}$.明文块是否属于 Case1 与调制密钥 R 和明文块 X_i 中的最大值与最小值有关.

性质 1. 块调制-置乱图像加密生成的明-密文差值块$[D_i\ D_{\pi(i)}]_{i=1,2,\cdots,N}$，满足 $D_i\equiv D_{\pi(i)}$ 的差值块有较高的出现概率.

证明. 块调制-置乱图像加密同一个图像块中，调制密钥 R_i 相同，已知调制密钥 R_i 出现的概率为 1/256，对明文图像 X 中任一明文块 X_i，该明文块为 Case1 图像块，即差值块满足 $D_i\equiv D_{\pi(i)}$ 的概率为

$$P_i=1-\frac{x_{i,\max}-x_{i,\min}}{256},\qquad(6)$$

其中，$x_{i,\max}$和 $x_{i,\min}$分别为明文块 X_i 中的最大值和最小值.自然图像中，由于块内像素间具有较高相关性，明文块 X_i 中的最大值与最小值差值远小于 256，导致差值块满足 $D_i\equiv D_{\pi(i)}$ 的概率 P_i 值较高.进一步计算明文图像 X 中 Case1 图像块所占比例为

$$Q=\frac{1}{N}\sum_{i=1}^{N}P_i.\qquad(7)$$

为验证性质 1，以 2×2 图像块为例，测试不同纹理复杂度的灰度图像 Lena 和 Baboon，在 50 种不同密钥 key_1 下 Q 的理论值与实际值，测试结果如图 2 所示：

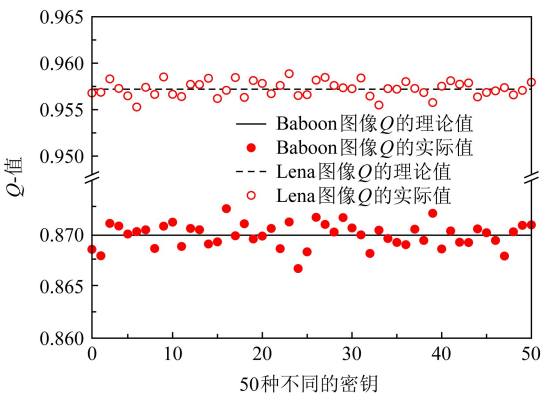

Fig. 2 Theoretical and actual values of Q value for Lena and Baboon under different secret keys

图 2 Lena 和 Baboon 在不同密钥下 Q 的理论值与实际值

由图 2 可看出 Q 的理论值与实际值的误差范围是[−0.2%，+0.2%]，对于纹理复杂度较高的 Baboon 图像，Q 值达到 87%，对于 Lena 图像 Q 值达到 95.8%.可见，差值图像中，满足 $D_i\equiv D_{\pi(i)}$ 的差值块有较高的出现概率. 证毕.

攻击者可利用加密前后保持不变的差值块，在明-密文建立等量关系实施已知明文攻击.然而，由于 Case2 图像块的存在，明-密文差值图像并不完全一致，因此，已知明文攻击的主要工作包括：1)构建完全一致的明-密文伪差值图像，利用构建的明-密文伪差值图像，在明文和密文建立等量关系进而估计块置乱序列 Π；2)块置乱序列 Π 的快速估计.

2 基于差值块分类的已知明文攻击

由 1.2 节分析可知，块调制-置乱图像加密在密文图像中保留了原始图像块内差值信息，不过，加密图像的差值直方图和原始图像的差值直方图并不完全相同.而构建完全一致的明密文伪差值图像，是估计块置乱序列 Π 的前提条件.

2.1 构建伪差值图像

在详细描述伪差值图像构建算法之前,为便于描述,先给出相关基本符号与概念的解释和定义.

定义 2. 差值直方图距离.明文差值图像为 D^X,密文差值图像为 D^Y,相应差值直方图分别表示为

$$H^1=\{h_i^1\mid i=-255,-254,\cdots,0,\cdots,+254,+255\},\tag{8}$$

$$H^2=\{h_i^2\mid i=-255,-254,\cdots,0,\cdots,+254,+255\},\tag{9}$$

其中,h_i 表示差值元素 i 出现的频数,差值图像 D^X 和 D^Y 的直方图距离 $d_{\mathrm{H}}(H^1,H^2)$ 定义为

$$d_{\mathrm{H}}(H^1,H^2)=\sum_{h=-255}^{+255}(|h_i^1-h_i^2|).\tag{10}$$

为降低构建伪差值图像算法时间复杂度,以明文差值块 $D_i=\{d_{i,j}\mid j=1,2,\cdots,N_{\mathrm{b}}\}$ 为例,将明文差值块中的差值求 β 次方平均值,将差值块 D_i 用 α 值表示:

$$\alpha_i=\frac{d_{i,1}^{\beta}+d_{i,2}^{\beta}+\cdots+d_{i,N_{\mathrm{b}}}^{\beta}}{N_{\mathrm{b}}},\tag{11}$$

其中,$\beta=2k+1$,$k\in\mathbb{N}_+$,k 为迭带次数.$d_{i,j}^{\beta}$ 表示对第 i 个差值块中的第 j 个差值求 β 次方.对所有明文差值块求 α 值得到明文 α 值序列 A,$A=\{\alpha_i\mid i=1,2,\cdots,N\}$.对密文差值块执行同样的操作,得到密文 α 值序列 B.α 值序列 B 中 A 的相对补集也称为 B 和 A 的集合差,表示为 $B\backslash A$,其元素 α_i 属于 B,但不属于 A,即:

$$B\backslash A=B-A=\{\alpha_i\mid\alpha_i\in B,\alpha_i\notin A\}.\tag{12}$$

显然,明-密文伪差值图像应满足的条件为:

1) $B\backslash A=\varnothing$,且 $A\backslash B=\varnothing$;

2) $B\bigcap A=A=B$.

当明文 α 值序列 A 与密文 α 值序列 B 满足以上 2 个条件时,明密文伪差值图像的直方图距离为 0.构建伪差值图像的算法如算法 1 所示:

算法 1. 伪差值图像构建算法.

/* 由差值图像(D^X,D^Y),构建伪差值图像(D,D') */

输入:明文差值图像 D^X、密文差值图像 D^Y;

输出:明文伪差值图像 D、密文伪差值图像 D'.

将明文、密文差值图像 D^X,D^Y 分解为 N 个不重叠的图像块;

for $k=1,2,\cdots n$ do

由式(11)分别计算 D^X,D^Y 所有图像块的 α 值,得到序列 A 和 B;

求 $\Lambda(A\backslash B)$ 和 $\Lambda(B\backslash A)$;

将差值块 $D_{\Lambda(A\backslash B)}$ 与 $D_{\pi(\Lambda(A\backslash B))}$ 替换为同等大小的全 0 块;

根据式(10)计算差值直方图距离;

if $d_{\mathrm{H}}(H^1,H^2)=0$

$D=D^X$;

$D'=D^Y$;

break; /* 替换成功,退出循环 */

else 替换失败,继续 for 循环;

end if

end for

return 明密文伪差值图像 D,D'.

其中,$\Lambda(A\backslash B)$ 表示取 $A\backslash B$ 对应差值块的索引地址.

2.2 基于差值块分类的 Π 估计

基于 2.1 节构建的伪差值图像 D 和 D' 的基础上,利用分块置乱加密不改变差值的特点,定义差值块立方均值 ρ.差值块 D_i 的 ρ 值为

$$\rho_i=\frac{d_{i,1}^3+d_{i,2}^3+\cdots+d_{i,N_{\mathrm{b}}}^3}{N_{\mathrm{b}}}.\tag{13}$$

根据差值块的 ρ 值将差值块分类:ρ 值在 0 附近的图像块为平滑块,反之为纹理块.图 3 统计了 Lena 差值图像在 2×2 分块下的 ρ 值分布.

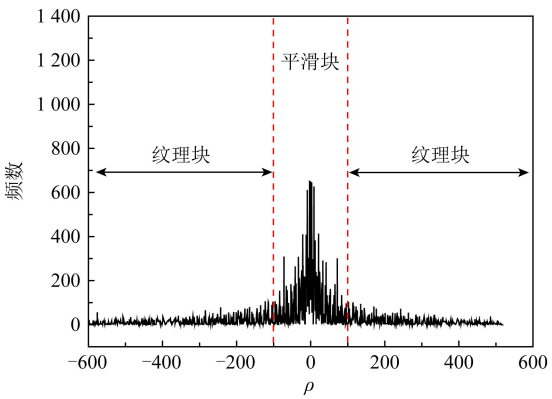

Fig. 3 Distribution of ρ values

图 3 ρ 值分布图

由图 3 可看出,大多数差值块的 ρ 值在 0 附近.为快速查找密文图像块的置乱坐标,本文提出一种基于差值块 ρ 值的分类查找算法,描述如 Step1~Step3.

Step1. ρ 值排序.将明-密文伪差值图像分为 N 个大小相等、不重叠的差值块.计算明文伪差值图像 D 与对应密文差值图像 D' 中所有差值块的 ρ 值,并按升序排序:

1) 明文伪差值图像 D 中所有差值块的 ρ 值排序构成集合 J, $J=\{\rho_1,\cdots,\rho_i,\cdots,\rho_N\}$;

2) 密文伪差值图像 D' 中所有差值块的 ρ 值排序构成集合 J', $J'=\{\rho'_1,\cdots,\rho'_i,\cdots,\rho'_N\}$.

Step2. 差值块分类.提取 D 与 D' 中 ρ 值相同的差值块,同时保留其原始索引构成的块集合 C.伪差值图像 D 中,所有块集合构成分类集合 Ω, $\Omega=\{C_1,\cdots,C_i,\cdots,C_M\}$.其中, C_i 为 ρ_i 对应的块集合, $C_i=\{D_1^i,D_2^i,\cdots,D_\varepsilon^i\}$.块集合满足 4 个条件:

1) M 为块集合的总个数, $M\leqslant N$;

2) ε 为块集合中差值块个数, $\varepsilon\leqslant N$;

3) $C_i\cap C_j=\varnothing$, $\forall i\neq j$;

4) $C_1\cup C_2\cup\cdots\cup C_M=D$.

Step3. 差值块分类查找.明文伪差值图像 D 中,第 i 个块集合为 $C_i=\{D_1^i,D_2^i,\cdots,D_\varepsilon^i\}$, $\varepsilon\leqslant N$, N 为图像块数.同理,密文伪差值图像 D' 中,第 i 个图像块集合为 $C'_i=\{D^i_{\pi(1)},D^i_{\pi(2)},\cdots,D^i_{\pi(\varepsilon)}\}$.令 $\Lambda(D_x^i)(1\leqslant x\leqslant\varepsilon)$ 表示块集合 C_i 中第 x 个图像块 D_x^i 的原始索引.则块置乱序列 $\Pi=\{\pi(1),\pi(2),\cdots,\pi(i),\pi(i+1),\cdots,\pi(N)\}$ 的估计为

$$\pi(\Lambda(D_x^i))=\Lambda(D^i_{\pi(x)}),\ \text{若}\ D_x^i\equiv D^i_{\pi(x)},\quad(14)$$

其中, $D_x^i\equiv D^i_{\pi(x)}$ 表示差值图像块 D_x^i 与 $D^i_{\pi(x)}$ 块内差值元素值相同. ρ_i 对应的图像块集合查找如算法 2 所示:

算法 2. 块分类查找过程.

/* 由明密文伪差值图像(D,D'),估计 Π */

输入:明文伪差值图像 D、密文伪差值图像 D'、差图像块总个数 N;

输出:块置乱序列 Π.

分别计算 D 和 D' 中 N 个图像块的 ρ 值,排序并得到集合 J 与 J';

由图像块 ρ 值提取明密文差值图像块,构成分类集合 Ω;

for Ω 中每一个块集合 C_i 中的图像块 do

  if $D_x^i\equiv D^i_{\pi(x)}$

    $\pi(\Lambda(D_x^i))=\Lambda(D^i_{\pi(x)})$;

  end if

  if 任意的 $D_x^i\equiv D_y^i$, $D^i_{\pi(x)}\equiv D^i_{\pi(y)}$

    $\pi(\Lambda(D_x^i))=Rand(\Lambda(D^i_{\pi(x)}),\Lambda(D^i_{\pi(y)}))$;

  end if

end for

return 块置乱序列 Π.

其中, $\Lambda(\cdot)$ 表示取差值块索引, $Rand(\cdot)$ 为随机选取函数.

在算法 2 中,对于仅出现一次的纹理差值块可以精确估计其置乱顺序,而在同一个块集合 C 中,对重复次数较多的平滑差值块随机且不重复地为其分配坐标.影响置乱序列 Π 估计正确率的主要因素为纹理块的数量.

差值块分类查找算法对任意差值图像块 $D_x^i\in C_i$,攻击者对它的搜索空间从原来的 N 下降为 ε, ε 为块集合 C_i 中差值块个数.从而将 N 个图像块置乱序列 Π 的密钥空间从 $N!$ 降低至 $M\times(\varepsilon)!$.显著降低了已知明文攻击算法时间复杂度.

3 实验结果及分析

选取 6 幅(512×512)未压缩灰度图像,6 幅测试图像按纹理复杂度由低到高顺序排列,它们分别为 Airplane, Lena, Woman, Man, Baboon, Camera.测试图像及在 2×2 分块下的加密图像如图 4 所示.

在本文提出的已知明文攻击中,攻击者利用块内像素差值在加密前后基本保持不变的特点来估计

(a) Airplane (b) Lena (c) Woman (d) Man (e) Baboon (f) Camera

Fig. 4 Six test images and the corresponding encrypted images

图 4 6 幅测试图像和对应的加密图像

块置乱序列,对差值图像块采取分类查找的策略实现序列 Π 的快速估计.本节首先测试了分块大小对加密前后 Case1 差值块出现比例(Q 值)的影响.验证了块调制-置乱加密明-密文差值图像具有较高相似性,这是实施已知明文攻击的前提.然后,对影响块置乱序列 Π 估计正确率的主要因素进行分析.

3.1 分块大小对明-密文差值块的影响

在 1.2 节分析中,块内像素调制加密后,密文块被分为 Case1 与 Case2 这 2 种情况.其中,Case1 密文差值块与明文差值块一致,而 Case2 的密文差值块发生改变.一幅图像的 Case1 图像块占比越高,其明-密文差值图像直方图距离越小,构建伪差值图像所替换的图像块越少,已知明文攻击的效果越好.反之,已知明文攻击效果越差.

由式(7)可看出,Case1 图像块的比例(Q 值)与块内最大值 $x_{i,\max}$ 和最小值 $x_{i,\min}$ 的差值有关.随着分块尺寸和图像纹理复杂度的增大,块内像素相关性减弱,$x_{i,\max}$ 与 $x_{i,\min}$ 的差值增大,从而会导致 Case1 图像块比例 Q 值降低.

为验证分块大小对 Q 值的影响,图 5 统计了图 4(a)~(e)在不同分块大小下的 Q 值.由图 5 可看出,在同等分块大小下,随着图像纹理复杂度的增加,Case1 图像块占总图像块的比例降低.对于同一幅图像,随着分块尺寸增大,Case1 图像块占比有所下降.即使是纹理复杂度较高的 Baboon 图像在 8×8 分块下,Q 仍在 60%以上.可见,分块大小最大、纹理复杂度最高的情况下,1.2 节性质 1 仍然满足.

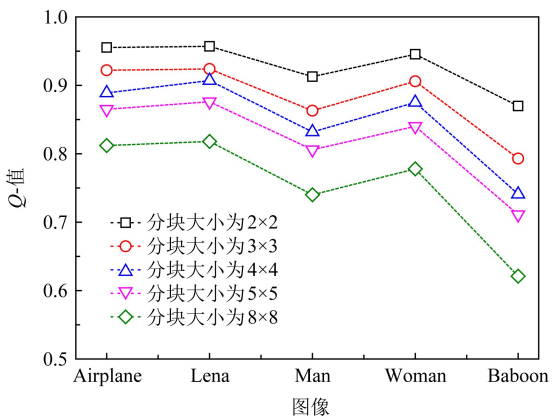

Fig. 5 Q-Value of the test images under different block sizes

图 5 测试图像在不同分块大小下的 Q 值

3.2 影响 Π 精确度因素分析

在 3.1 节中,明-密文差值图像直方图距离越大,构建伪差值图像所替换的图像块越多,对块置乱序列 Π 估计的精确度下降.在 2.2 节图像块分类查找,将差值块分为纹理块与平滑块,纹理块越多,Π 估计精确度越高.可见,影响 Π 估计精确度的主要因素为图像纹理复杂度与分块大小.本节,首先验证不同纹理复杂度下,现有已知明文攻击[14-18]和本文提出的已知明文攻击在块调制-置乱加密下的有效性,并分析不同纹理复杂度对块置乱序列 Π 估计精确度的影响.然后,分析不同分块对块置乱序列 Π 估计精确度的影响.

3.2.1 纹理复杂度对 Π 的影响

以图 4(a)Airplane、图 4(b)Lena、图 4(e)Baboon 为例,这 3 幅图像中,Airplane 图像纹理复杂度最低,Baboon 图像纹理复杂度最高.分块大小为 2×2 下,计算测试图像的 ρ 值,将 ρ 值范围在[-150,150]区域的像素置零,范围之外的像素值置为 255,生成的纹理分布图如图 6(a)所示.图 6(a)所示的纹理分布图中,白色为纹理块,黑色为平滑块.

像素置乱加密不改变明文图像的像素值大小,仅改变像素值位置.而块调制-置乱加密在加密过程中改变了像素值大小,因此现有的针对置乱加密的已知明文攻击[14-18]无法破解块调制-置乱加密.为验证现有已知明文攻击与本文提出的已知明文攻击对块调制-置乱加密的有效性,以 Li 等人[14]提出的针对置乱加密已知明文攻击算法为例,设攻击者分别获取 Airplane,Lena,Baboon 的明文及对应的密文图像,基于 2×2 分块,分别用文献[14]的已知明文攻击算法和本文提出的攻击算法估计块置乱序列 Π、调制密钥 R,进而解密图 4(f)的密文图像.解密结果如图 6(b)和图 6(c)所示.

由图 6(b)可知,现有针对仅置乱加密的已知明文攻击算法[14-18]无法破解块调制-置乱加密,这是因为该加密算法改变了明文图像的像素值.对比图 6(c)中的攻击结果可以看出,本文提出的已知明文攻击能破解块调制-置乱加密,且对纹理区的图像块攻击效果更好,而信息泄露的部分大多属于纹理区域.对于平滑块,由于差值图像块重复率较高,估计的 Π 精确度不高.在图 6(c)中,利用 Airplane 明-密文估计 Π 和 R 的正确率分别为 18.0%和 18.1%,利用 Lena 明-密文估计 Π 和 R 的正确率分别为 19.0%和 19.3%,利用 Baboon 明-密文估计 Π 和 R 的正确率分别为 57.0%和 57.1%.由图 6(c)可看出,虽然密钥估计正确率低于 20%,但密文图像仍有信息被泄露,由于 Baboon 纹理块较多,利用 Baboon 明-密文

图像估计的 Π 和 R 去解密图 4(f)的密文图像,解密图像视觉效果好于 Airplane,Lena.

Fig. 6 Texture distribution map and attack results under 2×2 block size

图 6 纹理分布图及分块大小为 2×2 的攻击结果

用本文提出的已知明文攻击算法测试 100 张不同纹理复杂度图像(UCID 标准图像数据库)在分块 2×2 下,块置乱序列 Π 的估计正确率,结果如图 7 所示.由图 7 可知,攻击者已知的明文图像内容不同,Π 的估计正确率不同.2×2 下块置乱序列 Π 估计正确率平均值为 30%.图 6(c)的攻击结果可知:当 30%块置乱序列被正确估计,密文图像的内容已被严重泄露.

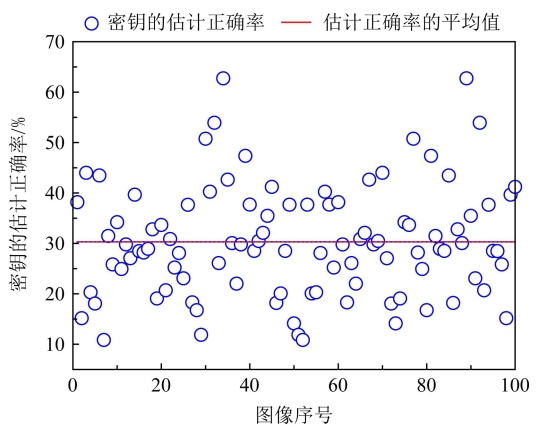

Fig. 7 The estimation accuracy of scrambling sequences Π estimated by using different images

图 7 不同图像内容下块置乱序列 Π 的估计正确率

3.2.2 分块大小对 Π 的影响

分块大小对 Π,R 的影响主要有 2 个方面:

1) 分块大小越大,块内像素间的相关性减弱,Case2 图像块占比增加,因此,在构建伪差值图像中,被替换的图像块数量增多,这导致 Π 与 R 的估计精度降低;

2) 分块大小越小,块内像素间的相关性越高,差值图像块的 ρ 值集中于 0 附近,即平滑块的数量提高,平滑块的增多会降低 Π 与 R 的估计精度.

由图 5 可知,对于纹理复杂度较高的图像按8×8 分块,明-密文差值图像仍然具有较高的相似度.可见,随着图像块尺寸的增大,Case2 图像块占比虽然提高,但是对 Π 与 R 的估计精度影响不大.因此,随着分块尺寸的增加,块置乱序列 Π 与调制密钥 R 的估计精度呈先升高后逐渐降低的趋势.为分析块大小对密钥估计精度的影响,利用图 4(a)~(e)在 2×2,3×3,4×4,5×5,8×8 不同分块大小下的明-密文图像分别估计密钥 Π 与 R,得到 5 组密钥,图 8 统计了 5 组密钥中块置乱密钥 Π 的正确率.

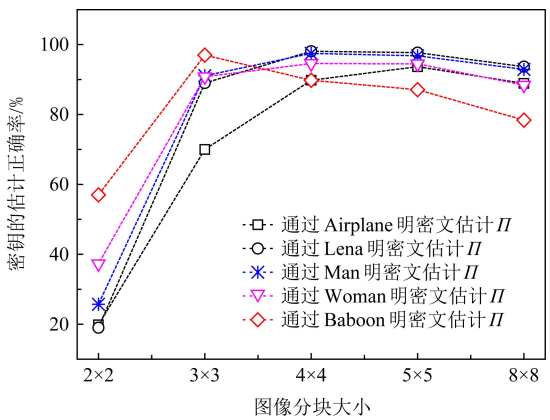

Fig. 8 Estimation accuracy of Π under different block sizes

图 8 置乱序列 Π 在不同分块大小下的估计正确率

由图 8 可看出,在分块大小为 2×2 时,Airplane 图像的块置乱序列 Π 的估计正确率虽然仅有 20%,但从图 6 可以看出,处于纹理块的图像内容仍然被泄露.在分块大小为 3×3 时,置乱序列 Π 的估计正确率达到 70%以上;当分块大小为 4×4 时,正确率可以达到 90%以上;当分块大小大于 5×5 时,密钥的估计正确率开始下降.实验结果表明:随着图像分块尺寸的增加,密钥估计正确率先升高后下降.利用 5 组估计密钥分别解密图 4(f)在对应分块大小下的密文图像.解密结果如图 9 和图 10 所示:

(a) 3×3分块大小下的攻击结果

(b) 4×4分块大小下的攻击结果

Fig. 9 The known plaintext attack results under 3×3 block size and 4×4 block size

图9 3×3分块及4×4分块下已知明文攻击结果

(a) 5×5分块大小下的攻击结果

(b) 8×8分块大小下的攻击结果

Fig. 10 The known plaintext attack results under 5×5 block size and 8×8 block size

图10 5×5及8×8分块大小下的攻击结果

由图9可看出,当分块大小大于2×2时,解密图像的视觉质量整体得到提高,加密图像的大部分原始内容已经泄露.在同样分块大小下,图像纹理复杂度越高,攻击效果可能有所下降,如4×4分块下Man的解密效果好于Baboon的解密效果;而对于纹理复杂度最高的Baboon图像,分块尺寸增加其攻击效果也可能有所降低,如3×3分块大小下Baboon的解密效果好于4×4分块大小下的解密效果.

继续增大分块尺寸,对比图9与图10的实验结果可知,随着分块尺寸的增大,明文图像纹理复杂度越低,攻击效果越好.当已知的明文图像纹理复杂度较高,如Baboon图像,随着分块大小的增加,已知明文攻击效果先提高后逐渐降低,3×3分块下攻击效果最好.解密图像视觉效果降低是因为图像分块大小以及纹理复杂度的增加会导致3.1节中Case1图像块占比的降低,构建伪差值图像所替换的图像块增加,导致块置乱序列 Π 与调制密钥 R 的估计正确率降低.

上述实验表明:当分块尺寸大于2×2时攻击者仅需1对明-密文就可以解密得到较好的图像.RDH-EI算法中,分块越小隐藏容量越低,但生成密文图像的安全性越高.为验证更小分块下(1×2和1×3分块)已知明文攻击效果,假设攻击者已知:1对明-密文(Baboon)、2对明-密文(Baboon & Woman)和3对明-密文(Baboon & Woman & Man),分别在1×2和1×3分块大小,用估计的块置乱序列 Π 解密Camera的密文图像,结果如图11所示:

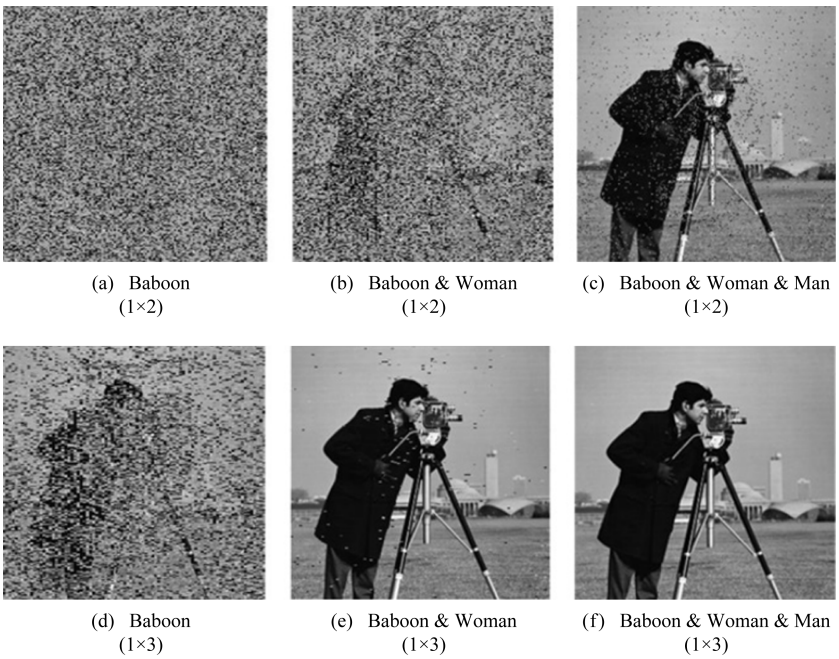

Fig. 11 Known plaintext attack results for 1 to 3 pairs of plain-ciphertext at block sizes 1×2 and 1×3

图 11 已知 1～3 对明-密文在分块大小为 1×2 和 1×3 下的攻击结果

图 11 中,在 1×2 分块下利用 1 对明-密文估计置乱序列 Π 的正确率仅为 1%,已知明-密文对数增加到 2 对,Π 的估计正确率达到 20.3%.当已知明-密文对数增加到 3 对,Π 的估计正确率达到 80.2%,如图 11(c)密文图像的大部分内容已被泄露(3 对明-密文).在 1×3 分块下利用 1 对明-密文估计置乱序列 Π 的正确率为 34.6%,密文图像的部分内容被泄露,当已知明-密文对数增加到 2 对时,Π 的估计正确率高达 98.8%,密文图像的内容被完全泄露.因此,即使在分块尺寸很小的情况下,块调制-置乱加密仍无法抵抗本文提出的已知明文攻击.

3.3 时间复杂度分析

算法时间复杂度是攻击效果的一个重要指标,攻击者的目标是在最短的时间内获得最好的攻击效果.下面对本文提出的已知明文攻击的算法时间复杂度进行分析,本文算法主要有 3 部分构成,算法每一步的时间复杂度及总的时间复杂度分析为:

Step1. 构建伪差值直方图.设迭代次数 k,计算所有图像块 α 值的时间复杂度为 N,N 为图像总分块数.利用明文密文差值图像替换 $B\backslash A$ 与 $A\backslash B$ 集合图像块的时间复杂度为 $k\times N^2$.因此,构建伪差值图像的时间复杂度为 $N+k\times N^2$.图 12 为测试图像在 2×2 和 3×3 下的 k 值.当分块大小大于等于 3×3 时 k 值都为 1,在 2×2 时,图像纹理复杂度越高,k 值越低.

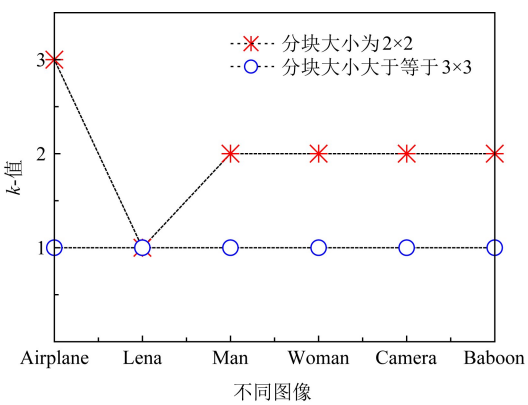

Fig. 12 k-value of different images under different block sizes

图 12 测试图像在不同分块下的 k 值

Step2. 计算每一图像块的立方均值 ρ 的算法时间复杂度是 N. 排序时间复杂度是 $N\times\mathrm{lb}\ N$.

Step3. 图像块分类查找.块集合最好的情况为集合内仅有一个图像块,此时查找的时间复杂度为 N.在 10 000 张图像测试集中发现,自然图像同一个块集合中,块元素个数不超过 $0.5N$,此时图像块分类查找的时间复杂度接近 $(0.5N)^2$.查找过程的平均

复杂度为$\frac{N+(0.5N)^2}{2}$.

因此,已知明文攻击算法总时间复杂度约为$\frac{5}{2}N+\left(k+\frac{1}{8}\right)N^2+N\times\mathrm{lb}\ N$.影响算法时间复杂度的主要因素为分块大小及迭代次数.表 1 给出已知明文攻击在不同分块大小下实际运行时间.

Table 1 Actual Running Time of the Known-plaintext Attack

表 1 已知明文攻击的实际运行时间 s

图像	分块大小				
	2×2	3×3	4×4	5×5	8×8
Airplane	64.37	2.28	1.42	0.73	0.31
Lena	12.64	1.58	0.80	0.44	0.19
Woman	12.77	2.51	1.44	0.95	0.47
Man	13.10	1.68	0.64	0.39	0.18
Baboon	6.50	7.09	6.16	2.00	0.90

从表 1 可以看出,已知明文攻击时间复杂度与分块大小和图像的纹理复杂度有关,对于平滑图像 Airplane 在分块大小为 2×2 下,估计块置乱密钥耗时最长,耗时约 64 s.在分块大小达到 8×8 时,对于所有测试图像,已知明文攻击估计块置乱序列仅需耗时 1 s 以内.

3.4 提高安全性的策略

为提高块调制-置乱图像加密的安全性能,主要目标是破坏置乱序列 Π 和调制密钥 R 的估计条件.在保留密文差值图像冗余度的条件下,给出 2 种提高加密图像安全性的方案.

策略 1. 自适应密钥.已知明文攻击的条件是用户使用相同的密钥加密多张明文图像,即密钥重用.当攻击者通过已知的明-密文对破解用户密钥 K,即可解密所有密文图像集.若不同图像内容所用的加密密钥不同时,已知明文攻击的条件无法满足.自适应密钥即用户基于密钥 K 和图像内容,生成不同的加密密钥 $\overline{K}$.自适应密钥加密过程中,密钥 K 是用户定义的,而图像加密密钥 $\overline{K}$ 是由散列函数生成的,从而实现了用户密钥和图像加密密钥的分离.如何生成加密密钥 $\overline{K}$ 是自适应密钥策略的关键,文献[25]中,Yi 等人提出一种基于 SHA 的自适应密钥生成方法.该自适应密钥加密算法中,分别输入用户定义的安全密钥 K 和原始图像 X,通过安全的 SHA 算法生成 2 个随机 SHA 序列.将 2 个 SHA 序列异或得到随机序列 $\overline{K}$,$\overline{K}$ 即为图像的加密密钥.自适应密钥的生成框架如图 13 所示:

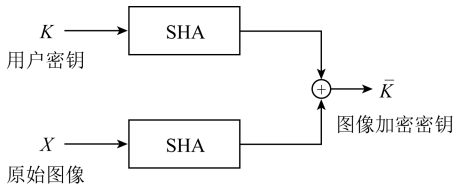

Fig. 13 The generation framework of the adaptive image encryption key

图 13 自适应密钥的生成框架

由于不同密文图像的置乱密钥均不相同,即使攻击者破解某对明-密文图像的置乱密钥,也无法解密其余密文图像.因此,自适应密钥可以抵抗本文提出的已知明文攻击.

策略 2. 分类加密.在本文提出的已知明文攻击中,信息泄露的区域主要集中在图像的纹理块区域,而处于纹理块区域的差值块可隐藏的信息量远低于平滑块.因此在加密前可先对图像的纹理块采用安全的图像加密算法加密,以改变纹理区的差值.对平滑块采用调制-置乱加密以保证隐藏容量.

4 结 论

为提高图像加密域可逆信息隐藏算法的隐藏容量,块调制-置乱图像加密算法在 RDH-EI 中被广泛应用.由于该加密算法结合模运算与分块置乱策略,在密文图像中保留了明文图像块内差值信息,有效地提高了加密图像的隐藏容量及安全性,可有效抵抗唯密文攻击和现有的已知明文攻击.本文分析了块调制-置乱加密算法的安全性,提出了一种基于差值块分类的已知明文攻击方法.首先利用明-密文差值图像迭代替换,构建出直方图距离为零的伪差值图像.在此基础上,利用图像块置乱不改变差值的特点定义差值块立方均值 ρ,将差值块分为平滑块与纹理块,并对差值块分类排序查找,实现块置乱序列的快速估计.分析讨论了块大小、图像纹理复杂度与块置乱序列估计正确率之间的关系,给出了在保证图像冗余空间的条件下提高加密图像安全性的策略.实验结果表明,图像分块越大,纹理差值块数量越多,块置乱序列估计正确率越高,块调制-置乱加密难以抵抗本文提出的已知明文攻击.为提高和设计更安全的 RDH-EI 算法,本文通过对 RDH-EI 常用的图像加密算法提出一种攻击方案,分析了块调制-置乱图像加密算法的安全性.

参 考 文 献

[1] Shi Yunqing, Li Xiaolong, Zhang Xinpeng, et al. Reversible data hiding: Advances in the past two decades [J]. IEEE Access, 2016, 4: 3210-3237

[2] 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

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

[4] Ma Kede, Zhang Weiming, Zhao Xianfeng, et al. Reversible data hiding in encrypted images by reserving room before encryption[J], IEEE Transactions on Information Forensics and Security, 2013, 8(3): 553-562

[5] Qian Zhenxing, Zhang Xinpeng. Reversible data hiding in encrypted images with distributed source encoding [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2016, 26(4): 636-646

[6] Hong Wien, Chen Tungshou, Wu Hanyan. An improved reversible data hiding in encrypted images using side match [J]. IEEE Signal Processing Letters, 2012, 19(4): 199-202

[7] Zhang Xinpeng, Qian Zhenxing, Feng Guorui, et al. Efficient reversible data hiding in encrypted images [J]. Journal of Visual Communication and Image Representation, 2014, 25(2): 322-328

[8] Xu Dawen, Wang Rangding. Separable and error-free reversible data hiding in encrypted images [J]. Signal Processing, 2016, 123: 9-21

[9] Yan Shu, Chen Fan, He Hongjie. Reversible data hiding in encrypted image based on neighborhood prediction using XOR-permutation encryption [J]. Journal of Computer Research and Development, 2018, 55(6): 97-107 (in Chinese)
(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): 97-107)

[10] Qu Lingfeng, He Hongjie, Chen fan. Reversible data hiding in encrypted image based on prediction error and classification scrambling [J]. Journal of Optoelectronics · Laser, 2019, 30(2): 168-174 (in Chinese)
(屈凌峰, 和红杰, 陈帆. 基于预测误差分类置乱的图像加密域可逆信息隐藏[J]. 光电子·激光, 2019, 30(2): 168-174)

[11] Yin Zhaoxia, Luo Bin, Hong Wien. Separable and error-free reversible data hiding in encrypted image with high payload [J]. The Scientific World Journal, 2014, 2014: 1-8

[12] Yin Zhaoxia, Abel A, Zhang Xinpeng, et al. Reversible data hiding in encrypted image based on block histogram shifting [C] //Proc of the 2016 IEEE Int Conf on Acoustics, Speech and Signal Processing (ICASSP). Piscataway, NJ: IEEE, 2016: 2129-2133

[13] Yin Zhaoxia, Abel A, Tang Jin, et al. Reversible data hiding in encrypted images based on multi-level encryption and block histogram modification [J]. Multimedia Tools and Applications, 2017, 76(3): 3389-3920

[14] Li Shujun, Li Chengqing, Chen Ghuanrong, et al. A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks [J]. Signal Processing: Image Communication, 2008, 23(3): 212-223

[15] Li Chengqing, Lo K. Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks [J]. Signal Processing, 2011, 91(4): 949-954

[16] Jolfaei A, Wu Xinwen, Muthukkumarasamy V. On the security of permutation-only image encryption schemes [J]. IEEE Transactions on Information Forensics and Security, 2016, 11(2): 235-246

[17] Li Shujun, Li Chengqing, 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

[18] Li Weihai, Yan Yupeng, Yu Nenghai. Breaking row-column shuffle based image cipher [C] //Proc of the 20th ACM Int Conf on Multimedia. New York: ACM, 2012: 1097-1100

[19] Liu Zilong, Pun C. Reversible data-hiding in encrypted images by redundant space transfer [J]. Information Sciences, 2018, 433: 188-203

[20] Qu Lingfeng, Chen Fan, He Hongjie, et al. Security analysis of image encryption algorithm based on bit plane-pixel block scrambling [J]. Journal of Applied Sciences, 2019, 37(5): 631-642 (in Chinese)
(屈凌峰, 陈帆, 和红杰, 等. 基于位平面-块置乱的图像加密算法安全性分析[J]. 应用科学学报, 2019, 37(5): 631-642)

[21] Chen Kai, Xu Dawen. An efficient reversible data hiding scheme for encrypted images [J]. International Journal of Digital Crime and Forensics, 2018, 10(2): 1-22

[22] Yi Shuang, Zhou Yicong. Separable and reversible data hiding in encrypted images using parametric binary tree labelings [J]. IEEE Transactions on Multimedia, 2019, 21(1): 51-64

[23] Xu Dawen, Su Shubing. Separable reversible data hiding in encrypted images based on difference histogram modification [J]. Security and Communication Networks, 2019, 2019: 1-14

[24] Yi Shuang, Zhou Yicong. Parametric reversible data hiding in encrypted images using adaptive bit-level data embedding and checkerboard based prediction [J]. Signal Processing, 2018, 150: 171-182

[25] Yi Shuang, Zhou Yicong. Binary-block embedding for reversible data hiding in encrypted images [J]. Signal Processing, 2017, 133: 40-51

Qu Lingfeng, born in 1993. PhD candidate. His main research interests include image processing and reversible data hiding in encrypted image.

屈凌峰,1993 年生.博士研究生.主要研究方向为图像处理和图像加密域可逆信息隐藏等.

He Hongjie, born in 1971. PhD, professor. Her main research interests include image processing, deep learning and reversible data hiding in encrypted image. (hjhe@swjtu.edu.cn)

和红杰,1971 年生.博士,教授.主要研究方向为图像处理、深度学习和图像加密域可逆信息隐藏等.

Chen Fan, born in 1971. PhD, associate professor. His main research interests include multimedia security, information hiding and computer applications.

陈　帆,1971 年生.博士,副教授.主要研究方向为多媒体信息安全、信息隐藏和计算机应用等.

Zhang Shanjun, born in 1964. PhD, professor. His main research interests include medical image processing, computer vision, image/video retrieval, information hiding, pattern recognition, and machine learning. (zhang@info,kanagawa-u.ac.jp)

张善俊,1964 年生.博士,教授.主要研究方向为医学图像处理、计算机视觉、图像/视频检索、信息隐藏、模式识别和机器学习.