基于离散余弦变换的图像加密效果评估方法

李珊珊,周怡彤,张红丽,孙伟阳
(长安大学 信息工程学院,陕西 西安 710064)

摘 要:不动点比,图像相似度等是传统的图像加密效果评估方法,传统方法具有局限性和不准确性。文中提出一种基于离散余弦变换的图像加密效果评估方法,利用离散余弦变换(DCT)把图像从时域变换到频域,同时分析图像的能量分布状况,以此评估图像的加密效果;计算明文图像和密文图像的频谱系数差值,用该差值构造差值系数矩阵,最后计算图像信息熵,通过熵值大小判断图像加密效果,得到新的图像加密效果评估方法。通过不同图像加密方法对同一图像进行加密,用新方法进行加密评估;对同一图像分别采用新的加密评估方法与传统方法进行评估,比较评估结果准确性等实验,验证了新方法的有效性。提出的加密评估方法改善了传统加密评估方法的局限性,提高了评估准确性,评估结果也与人眼观察效果基本一致。

关键词:离散余弦变换;加密方法评估;图像加密;信息熵;置乱度
中图分类号:TP301 **文献标识码**:A **文章编号**:1673-629X(2020)05-0099-04
doi:10.3969/j.issn.1673-629X.2020.05.019

A Novel Image Encryption Performance Evaluation Based on Discrete Cosine Transform

LI Shan-shan,ZHOU Yi-tong,ZHANG Hong-li,SUN Wei-yang
(School of Information Engineering,Chang'an University,Xi'an 710064,China)

Abstract:Traditional image encryption performance evaluation methods,such as fixed point ratio and image similarity,have limitations and inaccuracy. A novel image encryption performance evaluation has been presented. The discrete cosine transform (DCT) is used to transform the image from time domain to frequency domain,and the energy distribution of the image is analyzed to evaluate the image encryption effect. The DCT coefficient difference between plain-text and cipher-text image is calculated to construct the difference coefficient matrix. Then the information entropy is employed to measure the encryption performance. The same image is encrypted by different image encryption methods,and the novel method is used for encryption evaluation. The effectiveness of the novel method is verified by comparing the accuracy of the new method with that of the traditional method. The proposed encryption evaluation method improves the limitation of the traditional encryption evaluation method and the accuracy of the evaluation,and the evaluation results are basically consistent with the observation effect of human eyes.

Key words:discrete cosine transform;encryption performance evaluation;image encryption;Shannon entropy;scrambling degree

0 引 言

随着计算机技术、信息存储技术以及互联网技术的快速发展,数字图像的存储和传输技术的安全性也越来越受到研究者们的广泛关注。图像加密技术提出有效而完善的加密方法来实现图像信息的安全接收与传输,是保障图像安全的重要手段[1]。

新的加密方案不断被提出,研究者们越来越关注图像加密性能评估。当前评估图像加密效果的算法主要分为主观和客观两种评估方法,其中主观方法主要是利用人类视觉主观感知来评估密文图像的加密效果,如果从中不能分辨出明文图像信息,就说明其加密效果较好[2]。主观评价直观易懂,但缺乏可靠性,速度慢,无法对参数调整提供建议。因此客观评估相比较主观评价更加实用。客观评估方法主要是定量计算密文图像的置乱度,用实际数据衡量加密效果[3-4]。

文中提出一种客观的图像加密效果评估方法。该

收稿日期:2019-05-09 **修回日期**:2019-09-11 **网络出版时间**:2019-12-18
基金项目:国家自然科学基金(211024140395);陕西省科学技术计划项目(213024160365);陕西省博士后科研项目(332200150024)
作者简介:李珊珊(1982-),女,副教授,硕导,博士,通信作者,研究方向为图像处理、图像识别和加密;周怡彤(1996-),女,硕士研究生,研究方向为图像处理、图像识别和加密。
网络出版地址:http://kns.cnki.net/kcms/detail/61.1450.TP.20190902.1645.002.html

方法将图像转换到频域,对其频域图像进行分析,之后计算明文图像和密文图像的频谱系数差值,用该差值构造差值系数矩阵,计算熵值得到密文图像的置乱度,用该置乱度评估加密效果。

1 传统图像加密评估方法

1.1 基于不动点比的图像加密效果评估方法

一般情况下,可以通过不动点比看出图像加密效果,不动点比越小,图像置乱度越好。

1.2 基于图像相似度的图像加密效果评估方法

评估图像加密效果,可以通过对比密文图像与原图像的相似度来评估其加密效果。相似度越高,说明其加密效果越差;反之其加密效果越好。

1.3 基于自相关性的图像加密效果评估方法

图像中相邻像素值是高度相关的[5],即其相关系数接近为 1。明文图像经过加密后相邻像素值的相关性降低,因此可以通过相关系数值来评估其加密效果。相关系数绝对值越接近于 1,其加密效果越差。通常为了检验明文图像和密文图像相邻像素的相关性,会从水平、垂直或对角方向计算其相关性。

2 基于 DCT 图像加密评估方法相关概念

2.1 离散余弦变换(DCT)

不同纹理细节特征的图像区域其变换后 DCT 系数的分布差别很大。对于图像加密算法,当密文图像中相邻像素的灰度差值越大,灰度分布越混乱,加密效果越好,图像频域集中程度越差,因此密文图像的频谱分布情况可以用来评估图像的加密效果[6-7]。

2.2 图像信息熵

1948 年,香农提出信息熵概念描述信息的不确定性,信息熵还可用来描述含有的信息量大小,或者说信息的不确定性、混乱程度。随机变量服从均匀分布时,其信息的不确定性越大,即熵值越大[8-9]。这说明随机变量的概率分布与均匀分布之间的差异性也可用熵值表示。若其概率分布越接近均匀分布,其信息熵越大,表明该图像加密算法的加密效果越好;反之,若概率分布越远离均匀分布,信息熵越小,表明该图像加密算法的加密效果越差[10-12]。

3 基于 DCT 的评估过程及步骤

图像加密算法破坏了相邻像素间的相关性,人无法通过观察密文图像获取明文图像的信息。文中利用离散余弦变换(DCT)以及信息熵,提出了基于离散余弦变换的图像加密效果评估方法。一方面将密文图像利用 DCT 得到其频域图像,通过观察比较密文图像的频域图像来评估加密方法加密效果;评估标准是频域中的频谱分布越均匀,则该加密算法的加密效果越好。另一方面可以通过明文图像与密文图像的频域图像做差值来构造一个二维差值矩阵,计算其信息熵值,通过熵值评估其加密效果。新的评估方法流程如图 1 所示。

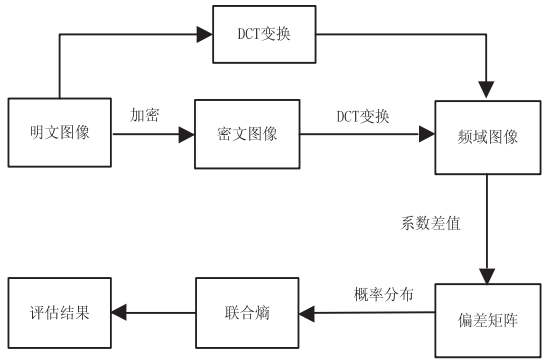

图 1 基于 DCT 的图像加密效果评估流程

假设加密前后的图像分别表示为 G 和 G',图像大小均为 $N \times N$。将其表示为:$G = \{g(x,y) \mid x,y = 1,2,\cdots,N\}$,$G' = \{g'(x,y) \mid x,y = 1,2,\cdots,N\}$,对图像 G 和 G' 进行 DCT 变换,其频域系数矩阵分别为 $\boldsymbol{H}_{ij}$,$\boldsymbol{H}'_{ij}$。即:$\boldsymbol{H}_{ij} = \{h_{ij}(x,y) \mid x,y = 1,2,\cdots,N\}$,$\boldsymbol{H}'_{ij} = \{h'_{ij}(x,y) \mid x,y = 1,2,\cdots,N\}$。

计算 G 和 G' 对应的频域系数偏差值,构造系数偏差矩阵:$\boldsymbol{\varphi}_{ij} = \{\varphi_{ij}(x,y) \mid x,y = 1,2,\cdots,N\}$,其中 φ_{ij} 的表达式为:$\varphi_{ij}(x,y) = \mid h'_{ij}(x,y) - h_{ij}(x,y) \mid^2$,这里 $\mid \cdot \mid$ 表示绝对值运算。

通过系数偏差矩阵构造二元离散概率分布函数,刻画加密前后图像 DCT 系数偏差的均匀性。使用概率分布的确定性程度来判断图像 DCT 系数偏差矩阵元素之间的均匀性。二元离散随机变量的联合熵定义为:

$$E_{ij}(x,y) = -\sum_{x=1}^{N}\sum_{y=1}^{N} P_{ij}(x,y)\log P_{ij}(x,y), \quad i,j = 1,2,\cdots,N \tag{1}$$

4 实验与分析

4.1 基于图像像素位置置乱的加密方法

Arnold 变换是目前较为经典的一种图像加密方法,俗称“猫脸变换”[13-14]。在本节中,对明文图像采用 Arnold 图像加密算法得到其密文图像,进而对新的加密评估方法进行验证。对明文图像进行不同迭代次数加密可以获得不同的密文图像,其加密效果也不同。图 2 是对 124×124 大小的明文图像进行不同次数迭代的加密结果,其迭代次数总共是 15 次。从图 2 中可以看到,1 次迭代和 2 次迭代后,图像开始出现混乱;5 次迭代人眼几乎无法得到原图像信息;随着迭代次数增加,明文图像逐渐恢复,当进行到第 15 次迭代时,恢复

为明文图像。

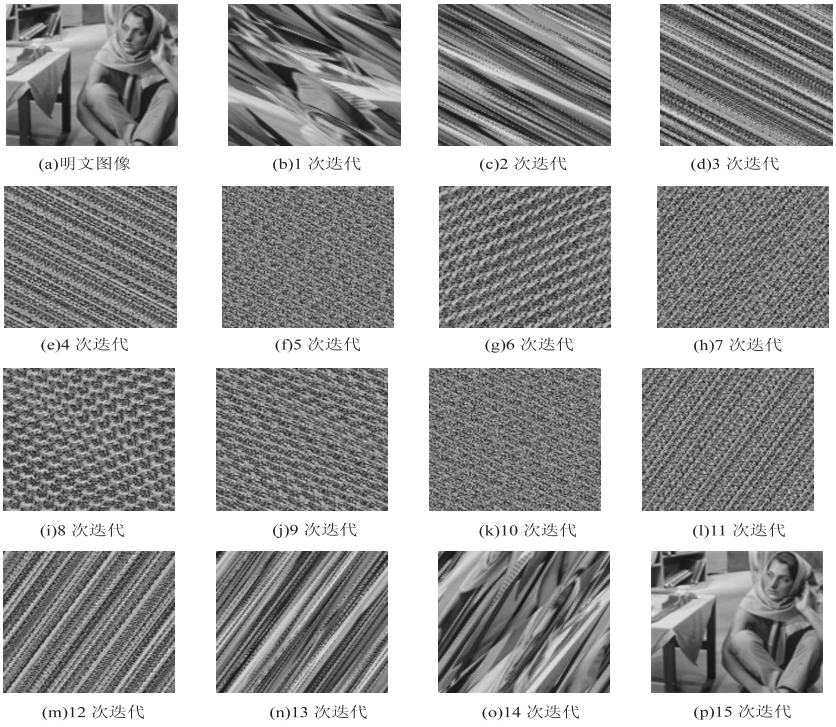

图 2　Arnold 图像加密结果

4.2　图像加密效果分析

4.2.1　新标准对不同加密方法效果评估

实验中采用 124×124 大小的灰度图像作为明文图像对式(1)提出的图像加密效果评估方法进行测试。采用 Arnold 变换和 Logistic 混沌映射[15-16]分别对图 2 中的明文图像进行加密,用提出的新标准求其置乱度。表 1 给出了对于两种加密方法,新标准得到的置乱度具体值。

表 1　Arnold 变换与 Logistic 混沌映射置乱度

迭代次数	置乱度	
	Arnold 变换	Logistic 混沌映射
1	4.532 2	4.307 4
2	4.564 6	4.277 8
3	4.582 8	4.285 9
4	4.579 5	4.316 7
5	4.573 8	4.317 7
6	4.592 4	4.315 5
7	4.582 9	4.294 0
8	4.595 1	4.312 7
9	4.573 9	4.306 2
10	4.601 2	4.311 7
11	4.587 3	4.308 1
12	4.598 3	4.289 1
13	4.597 2	4.271 8
14	4.547 8	4.284 3

从表 1 中可以看出,对同一图像采用不同加密方法进行加密,得到的密文图像用新方法求得的置乱度大小不同,但是不论是 Arnold 变换还是 Logistic 混沌映射,新标准都可以评估其不同迭代次数对应密文图像的加密效果。

4.2.2　不同加密效果评估方法的对比分析

采用上文中提到的传统方法不动点比对图 2 中经过 Arnold 变换得到的密文图像的加密效果进行评估,与文中提出的新方法进行对比。图 2 中的原图像与对应经过不同迭代次数 Arnold 变换所得到密文图像相比较,其不动点比值在表 2 中列出,这明显与图 3 中看到的结果不一致。

表 2　图 2 中密文图像的不动点比值

迭代次数	不动点比值/%
1	0.54
2	0.47
3	0.65
4	0.56
5	0.58
6	0.72
7	0.59
8	0.58
9	0.72
10	0.58
11	0.56
12	0.65
13	0.47
14	0.54

采用上文中提到的传统方法图像相似度对图 2 中

经过 Arnold 变换得到的密文图像的加密效果进行评估,与文中提出的新方法进行对比。图 2 中的原图像与对应经过不同迭代次数 Arnold 变换所得到密文图像相比较,其相似度在表 3 中列出,该结果与图 2 的结果不完全一致。

表 3 图 2 中密文图像与明文图像相似度

迭代次数	相似度
1	0.645 7
2	0.680 3
3	0.664 8
4	0.674 8
5	0.669 5
6	0.670 9
7	0.669 4
8	0.670 2
9	0.670 9
10	0.669 5
11	0.674 8
12	0.664 8
13	0.680 3
14	0.645 7

5 结束语

提出了一种新的方便实用的图像加密效果评估方法,该方法易于实现,并能够解决主观评估图像加密效果的不确定性。实验结果证明,该方法能够较好地评估图像加密效果,并与人的主观评估基本相符。

参考文献:

[1] LIU Lingfeng,MIAO Suoxia. A new image encryption algorithm based on logistic chaotic map with varying parameter [J]. SpringerPlus,2016,5:289.

[2] 张雪锋,范九伦. 两个新的数字图像加密效果评价准则[J]. 计算机科学,2010,37(2):264-268.

[3] 宋莉莉. 图像置乱算法及其评估研究[D]. 天津:河北工业大学,2015.

[4] DALHOUM A L A,MADAIN A,HIARY H. Digital image scrambling based on elementary cellular automata[J]. Multimedia Tools and Applications,2016,75:17019-17034.

[5] YUGANYA C. 2D cross correlation multi-modal image recognition[J]. Journal of Global Research in Computer Science,2013,4(4):13-17.

[6] 王远志,张歌凌,张 健,等. 分布均匀性的图像置乱衡量方法[J]. 计算机工程与应用,2009,45(34):155-158.

[7] 吴增珍. 数字图像置乱均匀度研究及其在图像安全中的应用[D]. 广州:暨南大学,2007.

[8] 张华熊,吕 辉,翁向军. 基于信息熵的图像置乱程度评价方法[J]. 电路与系统学报,2007,12(6):95-98.

[9] LONG Min,PENG Fei,WANG Shuaiping. Print-scan resilient binary map watermarking based on DCT and scrambling [J]. International Journal of Digital Crime and Forensics,2018,10(4):80-89.

[10] 韩 栋,王春华. 基于 DC 系数隐藏的 JPEG 图像加密算法[J]. 微电子学与计算机,2018,35(9):47-51.

[11] ITTONEN K,TRONNES P C,WONG L. Substantial doubt and the entropy of auditors' going concern modifications [J]. Journal of Contemporary Accounting & Economics,2017,13(2):134-147.

[12] LIU Xiaoyong,LI Rongli,ZHAO Hongwei,et al. Quality assessment of speckle patterns for digital image correlation by Shannon entropy[J]. Optik - International Journal for Light and Electron Optics,2015,126(23):4206-4211.

[13] 方 毅. Arnold 置乱变换图像加密算法研究[D]. 赣州:江西理工大学,2018.

[14] 李晴晴,杭后俊,尹天乐. 基于 Bezier 曲线的数字图像加密研究[J]. 计算机技术与发展,2019, 29(4):91-94.

[15] 施 飞,张红梅,张向利. 基于混沌映射和 DNA 编码的图像加密算法[J]. 计算机工程与应用,2018,54(5):91-95.

[16] 安守楠. 混沌图像加密算法研究与实现[D]. 太原:中北大学,2018.