适合于网络传输的二次置乱图像加密算法

江 南 张 帆 刘文予
(华中科技大学电子与信息工程系, 武汉 430074)

摘 要 为了保证数据的安全性,在网络中传输的图像数据常需要进行加密处理。在这一过程中,不但要考虑加密算法的安全性,还需要考虑加密算法对码率的影响,以及图像传输的实时性要求。提出了一种基于二次置乱的图像加密算法,该算法将图像按一定的大小划分成若干宏块,对每一行的宏块进行置乱。然后在离散余弦变换的基础上,对量化以后每个 8×8 矩阵随机选取前任意数量的交流(AC)系数并进行置乱。理论分析和实验结果表明,该算法既保证了网络传输过程中图像内容的安全性,又在码率、运算复杂度上有很好的性能,平均码率增长 6.478%,满足网络传输的实时性要求。同时,该算法满足格式兼容性并具有一定的容错能力,适合作为基于网络传输的图像加密算法。

关键词 图像 加密 二次置乱 宏块
中图法分类号: TP309.7 **文献标识码**: A **文章编号**: 1006-8961(2009)05-897-08

An Encryption Algorithm for Image Transmission Based on Duple Permutation

JIANG Nan, ZHANG Fan, LIU Wen-yu
(*Deptartment of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan* 430074)

Abstract Encryption algorithm is used to ensure the transmission safety of multimedia data. Not only the security of algorithm, but also the compression efficiency and encryption complexity should be taken into consideration when design an encryption scheme. A new encryption scheme for image transmission is proposed in this paper, which is based on duple permutation. Firstly the original image is divided into several macro blocks in the light of certain size, and macro block within each row are permuted. Then, the first random S of AC coefficients in each 8×8 matrix are permuted after DCT (discrete cosine transform) and quantization. Theoretical analysis and experimental results indicate that the scheme proposed in this paper is secure and fast. It has little adverse impact on the compact ratio, 6.478% by average. Moreover, it is format compatible and robust to transmission errors. All the attributes mentioned above make this algorithm suitable to be the encryption approach for image transmission.

Keywords image, encryption, duple permutation, macro block

1 引 言

图像是人们获取信息的主要方式之一。随着网络技术的发展,图像在网络上的传输也越来越普遍。但是,网络中存在很多不安全因素,人们在享受互联网高效、快捷、经济的同时,还需要考虑图像信息在互联网传输过程中的安全性。尤其是移动视频技术、远程医疗技术等方面的发展,对网络中传输的图像数据的安全性提出了更高的要求。

基金项目:高等学校科技创新工程重大项目培育资金项目(705038);教育部博士点基金资助项目(20040487009)
收稿日期:2007-04-02;**改回日期**:2007-08-14
第一作者简介:江 南(1983~),女。华中科技大学通信工程专业博士研究生。主要研究方向为多媒体安全。
E-mail:qiningonline@126.com

图像加密算法是保证图像在网络中传输安全性的主要途径之一。用于网络传输的加密算法与普通图像加密算法的主要区别在于:后者着重考虑算法本身的安全性能;而前者除算法的安全性外,还需考虑图像加密算法对码率的影响、加密算法运算复杂度、网络传输过程中的格式兼容性和算法传输误码鲁棒性问题。近年来,研究人员提出了很多图像加密算法,大体分为完全加密算法和部分加密算法两大类。相较于完全加密算法,部分加密算法具有加密速度快,保持原有码流结构等突出优点。其中,部分加密算法主要包括分块加密算法、流加密算法以及置乱加密算法 3 种加密方式。由于置乱加密算法具有加密效率高、加密效果好、鲁棒性强等显著优势而受到人们的广泛关注。常见的置乱加密算法有:基于 Arnold 变换的数字图像置乱技术[1],基于仿射变换和亚仿射变换的数字图像置乱技术[2-3],基于非线性变换 A-F 变换算法[4-5],以及基于伪随机序列的宏块置乱视频加密方案[6]。但是,由于置乱矩阵的周期性,置乱加密算法存在安全隐患。非法拦截者在已知加密算法的情况下进行攻击,能在有限的时间内破译密文。Tang 提出的离散余弦变换(DCT)系数全置乱算法是一种典型的基于一次置乱的 DCT 系数加密算法[7],这种加密算法对码率的负面影响大,恶劣的情况下使用这种方法可以致使码率增加 46% 左右[8]。同时,由于直流(DC)系数明显大于各交流(AC)系数这一特性,该加密算法很难抵御唯密文攻击。DCT 系数全置乱加密的改进算法,如将 DC 系数拆分或者对 DC 系数进行异或运算的数据隐藏方式,也被证明不安全[8]。针对 Tang 所提出的加密算法中存在的问题,研究人员提出了一些改进算法。一种思想是将 64 个 DCT 系数分成 3 层并进行层内置乱[9],这种加密方式的置乱范围有限,不能很好地抵御唯密文攻击,同时,这种算法中图像的直流信息并没有得到保护。另一种改进算法是将同一位置的 DCT 系数组成一个子序列并进行置乱[10],这种算法运算复杂度高,要求较高的缓存容量,也不适宜作为基于网络传输的图像加密算法。综上所述,考虑用于网络传输的图像加密策略的性能要求,目前存在的置乱加密算法主要存在的问题有:(1)置乱矩阵的周期性小,安全性低;(2)DC 系数没有得到保护,难以抵御唯密文攻击;(3)加密算法对码率的负面影响大,不适合网络传输;(4)加密算法运算复杂度高,不能满足网络传输的实时性要求。

本文提出了一种基于二次置乱的图像加密算法,该加密算法的优势在于能克服目前存在的加密算法中所存在的主要问题,既能保证网络传输过程中媒体内容的安全性,又满足格式兼容,具有一定的容错能力,且加密算法的运算复杂度低,对图像码率影响小,能充分满足网络传输实时性要求。

2 背景知识

2.1 JPEG 图像编码标准

JPEG 标准是目前被广泛采用的静态图像传输标准。它不仅适用于静态图像压缩,也常用于视频图像序列帧内图像的压缩编码。JPEG 采用 8×8 大小子块的 2 维离散余弦变换。在编码器的输入端,把原始图像顺序地分割成一系列 8×8 的子块。DCT 变换后生成 64 个 DCT 系数,这 64 个 DCT 系数所组成的 8×8 的数据块就是 JPEG 编解码过程中的基本处理单元。其中零频率对应的系数称为 DC 系数,8×8 数据块中其余的 63 个系数被称为 AC 系数。除 DC 系数外,其余 63 个交流系数采用行程编码。从左上方 AC_{01} 开始,沿对角线方向,以“Z”字形行程扫描,直到 AC_{77} 扫描结束。量化后待编码的 AC 系数通常有许多零值,沿“Z”字形路径进行行程编码,可增加行程中连续零的个数,如图 1 所示。63 个 AC 系数行程编码的码字,可用两个字节表示,如图 2 所示。

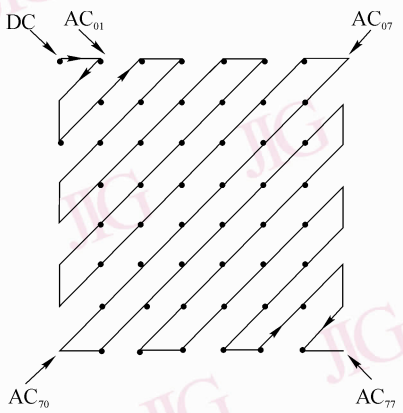


图 1 “Z”字形排列扫描

Fig. 1 The Zig-Zag procedure

为进一步压缩数据,需要对量化后的 DC 码和 AC 行程编码的码字再做基于统计特性的熵编码。JPEG 建议使用两种熵编码方法:哈夫曼编码和自适

图 2　AC 系数行程编码码字

Fig. 2　The run-length encoding of AC coefficient

应二进制算术编码。熵编码可分成两步进行,首先把 DC 码和行程码字转换成一个中间符号序列,然后给这些符号赋以变长码字。为了提高储存效率,JPEG 里并不直接保存数值,而是将数值按位数分成 16 组,对 AC 系数进行编码,而 DC 系数采用差分脉冲调制编码(DPCM)编码,或差分编码。

3　基于二次置乱的图像加密方案

本文提出了一种基于二次置乱的图像加密方案,算法的核心思想是:在对图像压缩效率影响不大的情况下,提高图像加密的安全性,满足图像在网络传输过程中的实时性要求。首先将待加密图像划分成若干宏块,对每一个宏块行中的宏块进行第一次置乱。接着,在 DCT 变换基本单元内随机选取前 S 个 AC 系数进行第二次置乱。两次置乱的结合增加了置乱矩阵的样本空间容量,克服了已知明文攻击,保证了加密算法的安全性。

3.1　加密阶段

何时加密媒体内容,通常有 3 种策略:一种是在媒体压缩编码之前加密(如图 3 中的第 1 个阶段或者第 2 个阶段),另一种是在媒体编码之后加密(如图 3 中第 5 个阶段),还有一种是将加密与熵编码相结合加密方式。在压缩编码之前加密,由于加密算法破坏了媒体数据间的相关性,媒体的压缩效率会受到影响。另外,如果媒体压缩是有损的,那么解码后的媒体会有质量损失,这导致在解密时会遇到困难。在压缩编码之后对图像进行加密则有可能出现两个问题。第一,图像熵编码后具有一定的码流结构和语法,此时加密会破坏图像数据的码流结构;第二,不考虑传输打包的规则而在压缩编码之后进行数据加密,可能会使得加密的媒体数据在传输出错时,出现错误蔓延。因此,在图像加密算法中这些都不是理想的加密阶段。考虑到运算复杂度和压缩效率,本方案选择在量化以后进行系数置乱(如图 3 第 3 个阶段)。

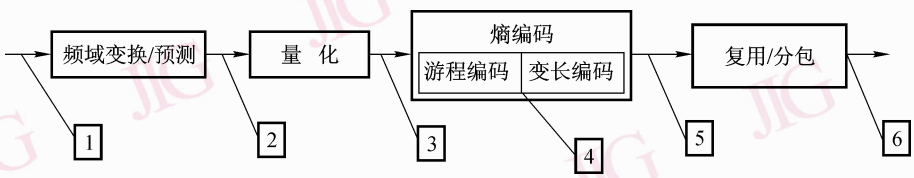


图 3　加密阶段分析图

Fig. 3　The analysis of encryption phase

3.2　加密算法

本方案对图像进行两次置乱以实现加密的目的。首先,以 16×16 的方阵为基本单元对图像进行分块,对每一个宏块行中的宏块进行第一次置乱。选取此种规格方阵作为基本单元进行宏块置乱是为了适应 JPEG 的编码格式。设 Q 是按“Z”字形扫描顺序排列的 AC 系数序列序号,满足 $1 \leqslant Q \leqslant 63$。定义随机数 S,$1 \leqslant S \leqslant Q$,对量化以后 8×8 的块中前 S 个 AC 系数进行第二次置乱。其中,一个随机数生成种子对应生成一个用于宏块行置乱的随机数序列,用于第一次置乱中生成置乱矩阵的种子各不相同,第二次置乱中随机数序列的生成方式与其类似。

以尺寸为 $m \times n$ 的图像为例,对图像进行分块,每行有 $n/16$ 个宏块,共 $m/16$ 个宏块行,令 $M = m/16$,$N = n/16$。选取任意参数 A,B 作为密钥。

加密步骤:

(1)以 $(A + k_1 B)$ 为种子,$k_1 = 0, 1, \cdots, M - 1$,使用陷门单向函数[11]生成伪随机序列 a,根据伪随机数序列 a 产生用于每一个宏块行的置乱矩阵 $\boldsymbol{P}$。

(2)根据置乱矩阵 $\boldsymbol{P}$,对图像的每一个宏块行中的宏块进行重新排列,实现第一次置乱加密。

(3)重复上述步骤,直至图像中 M 个宏块行中的宏块全部被置乱。

(4)以 $(B + k_2 A)$ 为种子,$k_2 = 0, 1, 2, \cdots, N - 1$,使用陷门单向函数生成伪随机数 S 和伪随机序列 b,根据伪随机数序列 b 产生用于 AC 系数置乱矩

阵 $\boldsymbol{T}$。

(5)根据置乱矩阵 $\boldsymbol{T}$,对量化后基本单元中前 S 个 AC 系数做第二次置乱。

(6)重复步骤(4)、(5),直至图像中所有 8×8 方阵 AC 系数均被置乱。

3.3 解密算法

解密算法与加密算法基本原理相同,是加密算法的逆运算。

解密步骤:

(1)解密端根据伪随机数种子($B+k_2A$),$k_2=0,1,2,\cdots,N-1$ 和生成函数重新生成伪随机数 S 和矩阵 $\boldsymbol{T}$。

(2)由置乱矩阵 $\boldsymbol{T}$ 计算得到还原矩阵 $\boldsymbol{C}$。

(3)根据还原矩阵 $\boldsymbol{C}$ 还原量化后基本单元中前 S 个 AC 系数。

(4)重复步骤(1)~(3),直至图像中所有 8×8 方阵被置乱的 AC 系数均被还原。

(5)以($A+k_2B$)为种子,$k_1=0,1,2,\cdots,M-1$,使用限门单项函数重新生成置乱矩阵 $\boldsymbol{P}$。

(6)由置乱矩阵 $\boldsymbol{P}$ 计算得到还原矩阵 $\boldsymbol{D}$。

(7)根据还原矩阵 $\boldsymbol{D}$,对图像中每一个宏块行中的宏块进行重新排列,实现置乱还原。

(8)重复步骤(5)~(7),直至图像中所有的宏块行均被置乱还原。

3.4 参数的选取

3.4.1 两次置乱所需伪随机序列的种子的选取

本方案中,需要生成的伪随机序列有两种。一种伪随机序列用于生成第一次置乱所需的置乱矩阵,另一种伪随机序列用于生成 AC 系数置乱所需的置乱位数和置乱矩阵。由于生成伪随机数序列的独立性越好,通信双方需要传输的密钥数目越少,加密算法安全性越高。因此,本方案使用两个密钥,将双密钥以不同的基本运算方式组合在一起生成具有多样性的伪随机序列种子,并根据这些种子生成不同的伪随机序列,以此提高算法的安全性。

选取任意参数 A、B 作为密钥,将密钥 A、B 用基本四则运算组合在一起,本算法中是以($A+k_1B$)为种子用于生成第一次置乱所需的伪随机序列,以($B+k_1A$)作为种子生成随机数 S 和 AC 系数置乱矩阵,其中 $k_1=0,1,2,\cdots,M-1$,$k_2=0,1,2,\cdots,N-1$。

3.4.2 第二次置乱中置乱范围的选取

本方案中 AC 系数序列序号 Q 的选取与码率和安全性都有密切的关系。Q 值越大,安全性越高,对码率的负面影响也越大。相反,若 Q 值过小,安全性将降低,对码率的负面影响也会减小。因此 Q 值的选取需在安全性和码率之间进行折中。图 4 表示在几幅典型的图像中前 Q 个 AC 系数位非零系数个数与整幅图像中非零系数个数的比值分布图。

图 4 中,曲线上升越快,说明 AC 系数分布越趋向于低频部分,图像简单,细节不丰富,这种情况下,第二次置乱中对行程编码的影响更大,对码率的负面影响也相应增加。图 4 中曲线上升相对缓慢,说明 AC 系数在低、中、高频部分分布相对均匀,图像细节丰富。这种情况下,第二次置乱中行程编码的码字与不加密情况比较,中间码字变化较少,对码率造成的负面影响也相应减小。

因此,应选取使得图 4 中纵坐标相对较大,横坐标相对较小的值作为 Q 的取值。即图 4 中,曲线趋近于平稳,曲线的切线与水平线的夹角小于 45°的点所对应的 Q 值。可见,选取中频部分的 18~22 的 AC 系数位置值作为 Q 值比较适合。

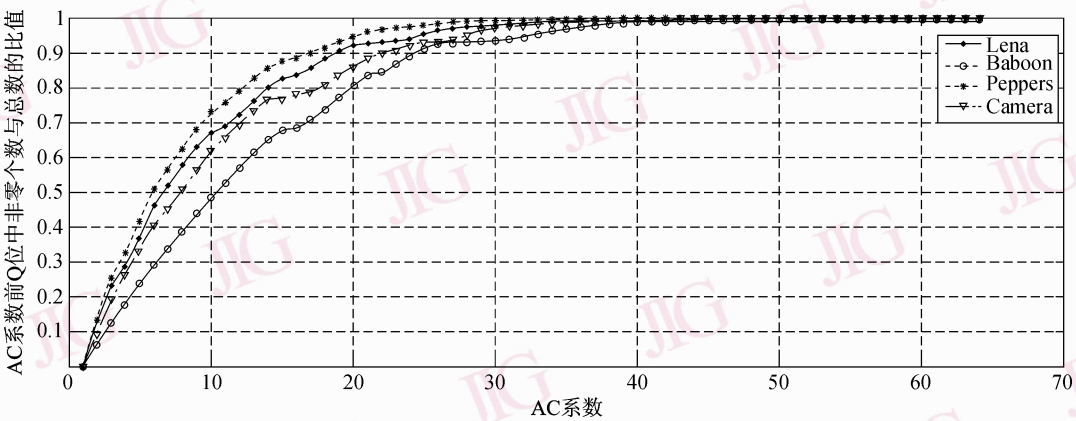


图 4 AC 系数分布图

Fig. 4 The distributing of AC coefficients

4　实验结果及分析

4.1　实验环境

本方案的实验是在 CPU-P4 2.66GHz,512M 内存的 PC 电脑上实现。图像加密算法在 Independent JPEG Group 的 JPEG C 语言源代码[12]基础上改写而成。密钥 A、B 的取值分别为 20、10,$\boldsymbol{Q}$ 的取值是 20。

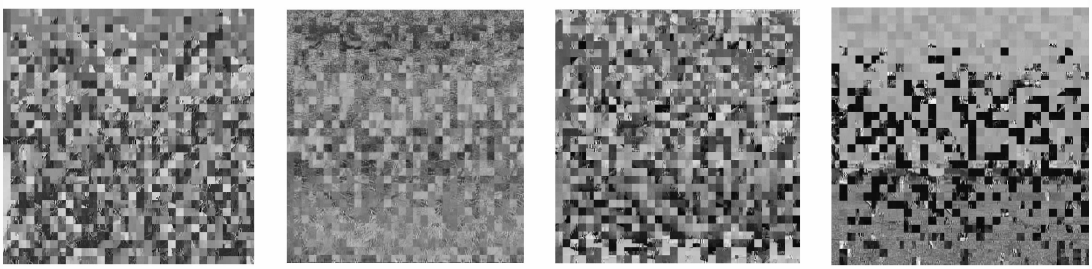
4.2　实验结果

实验中选取的 4 幅图像各有特点,Lena 属于频域系数正常分布的图像;Baboon 图像较为细腻,细节信息丰富,DCT 系数在低、中、高频部分分布较为均匀;Peppers 代表了色块集中的静物图像,DCT 系数主要趋向于低频部分;Camera 是近远景图像的典型代表。可以认为,这 4 种特性不同的图像具有普遍的代表性。

实验结果显示,经过加密后图像基本无法辨认,不会泄漏原始图像的结构和纹理信息,主观视觉上安全性高。实验数据显示,本文所提出的加密算法对码率所造成的增长影响最大为 8.455%,最小为 3.815%,平均值为 6.478%。相较于 Tang 所提出的算法[7],对码率的影响最高达到 46% 而言,本文所提出的图像加密算法对码率的负面影响非常有限。

由于二次置乱加密算法只改变图像宏块及系数的位置,而不改变系数的数值,所以,加解密过程是一个图像无损变换的过程,当图像经过无差错传输后,解密算法不会引起图像主观视觉的下降(如图 5(c)所示);当图像经过有噪信道发生误码且无丢包时,因为置乱加密算法扰乱了图像宏块的排列顺序,所以有利于接收端实施错误隐藏,这和交织编码以及灵活宏块排序的思想一致。当图像传输过程中发生丢包时,如果将丢包的数据做等长度的 0 比特填充,那么相对于一般的加密算法,采用本文的算法对误码图像进行解码不会对图像质量带来更差的恢复效果。

(a) 原始图像



(b) 二次置乱加密算法效果图

(c) 二次置乱解密算法效果图

图 5　实验结果

Fig. 5　Experiment results

表 1 基于二次置乱图像加密实验结果数据表

Tab. 1 The experiment data of duple permutation encryption

图像名称	原始图像大小(kB)	不加密、压缩图像大小(kB)	加密、压缩图像大小(kB)	加密后图像码率的增长(%)
Lena	257	34.9	37.1	6.304
Baboon	257	62.9	65.3	3.815
Peppers	257	34.3	37.2	8.455
Camera	257	32.7	35.1	7.339

5 算法分析

5.1 安全性分析

本加密方案是一种基于二次置乱的加密方案。一幅尺寸为 $m \times n$ 的图像,每行有 $n/16$ 个宏块,共有 $m/16$ 个宏块行。第 1 次加密针对宏块行进行置乱,每一行宏块置乱的样本空间大小是 $(n/16)!$。第 2 次加密针对 8×8 块的若干 AC 系数进行置乱,被置乱的 AC 系数个数由随机数 S 决定,S 有 Q 种可能的取值,则第二次置乱的样本空间大小为 $\prod_{K=1}^{Q} K!$。由此可知,每一个宏块行的样本空间大小为 $(m/16!) \times \left(\prod_{K=1}^{Q} K!\right)^4$,整幅图像的置乱空间的大小为 $\left((m/16!) \times \left(\prod_{K=1}^{9} K!\right)^4\right)^{n/16}$。

以一幅 512×512 的图像为例进行分析,则其每一行的宏块数为 32,共有 32 个宏块行。$Q=20$ 时,这样其置乱的样本空间大小为

$$\left((32!) \times \left(\prod_{K=1}^{20} K!\right)^4\right)^{32}$$

$$= ((2.631\,3 \times 10^{35}) \times (1.274 \times 10^{156})^4)^{32}$$

$$= ((2.631\,3 \times 10^{35}) \times (2.634\,4 \times 10^{624}))^{32}$$

足够大的样本空间保证了本文所提出的算法对于唯密文攻击的安全性。

根据量化后 DC 系数明显大于 AC 系数这一特性,提取 DC 系数并重建图像是一种常用的唯密文攻击方法[9],也是 Tang[7] 及其相关方案中不能抵御的一种攻击方式。本算法中,即使是将 DC 系数提取出来重建图像,由于第一次置乱加密,提取的图像仍然是密文,克服了单纯使用 DCT 系数置乱加密算法中存在的缺陷。

另外,在第二次置乱过程中低频 AC 系数的置乱破坏了图像的主观视觉信息,保证了本加密算法对于唯明文攻击的安全性。因此,本加密算法可以很好地满足图像在网络上传输的安全性。

同时,注意到在第一次置乱过程改变了 DC 系数的位置,但是并没有改变 DC 系数的数值,攻击者仍能够在较短时间内区分 DC 系数和 AC 系数,但是仅凭 DC 系数只能获得图像的部分轮廓,而不能获得图像细节,对于多媒体内容服务而言,其安全级别是可以接受的。另外,Q 的选取在一定范围内服从均匀分布,当 Q 的取值过小时,对单个置乱块的置乱效果有限,也会存在极小的范围内部分图像信息泄漏的可能。

5.2 加密算法对码率的影响

本加密算法对码率的影响主要表现在两个方面。其一,第一次置乱加密改变了宏块之间的先后次序,破坏了 DC 系数之间的相关性,使得差分编码中 DC 系数之间的差值,与不加密数据相比,可能存在差分编码值变大,增加编码长度的情况。其二,第二次置乱加密改变了低频 AC 系数的分布及次序,使得熵编码时编码长度存在差异。例如,假定原始图像数据“Z”字形行程扫描以后的 AC 系数为 $\underbrace{16,12,0,0,\cdots,0}_{63\text{个AC系数}}$置乱前 AC 序列中间码字为(0,5)10 000,(0,4)1 100,(end of block)

若第二次置乱加密以后,数据“Z”字形行程扫描得到的 AC 系数为

$\underbrace{0,0,12,0,16,\cdots,0}_{63\text{个AC系数}}$置乱后 AC 序列中间码字为(2,4)1 100,(1,5)10 000(end of block)

比较置乱前后标识 AC 系数实际值大小的中间码字…10 000…1 100 变成…1 100…10 000,编码长度并没有发生任何变化。这是因为本文所提出的图像加密方案对 AC 系数数值大小不产生影响,AC 系数对应数值进行编码时二进制码相同,使得这个部分的编码对码率不产生任何影响。而由于 AC 系数的位置的不同,造成了(行程数,所需比特位)的不同,即前例中(0,5)…(0,4)变成了(2,4)…(1,5),不同的(行程数,所需比特位)对应不同的二进制

数,而二进制数的不同造成了码流比特位长度的不同。这个部分对码率产生的影响是整个加密算法中造成码率变化的主要原因。但因 DCT 变换后即使图像细节丰富,AC 系数分布仍趋向于低频部分的特性,以及对 Q 值的适当的选取,本方案对中间码字带来的变化有限,因此,中间码字的不同给码率带来的负面影响被控制在一定的范围之内。实验结果表明,本加密算法给码率造成的负面影响较小,码率平均增加 6.478% 。

5.3　加密算法运算复杂度分析

在理论上,对于尺寸为 $m \times n$ 一幅图像,将加密算法引入图像压缩中,增加的运算量为:第 1 次置乱增加 $m/16$ 次 $(m/16) \times (n/16)$ 的矩阵乘法运算和 $((n/16)-1)$ 次 $(m/16) \times (n/16)$ 的矩阵加法运算。第 2 次关于 AC 系数置乱增加 $((m/8) \times (n/8))$ 次 8 ×8 的矩阵乘法运算。

算法实现过程中,置乱算法可以简化为程序对数据的处理顺序的不同。JPEG 编码标准中,数据按顺序存放于缓冲区中,置乱算法可以通过从缓冲区中改变数据的处理顺序从而达到置乱的效果。这时,运算量的增加仅在于顺序查找下一个需要处理的数据块的编号所需的时间和编号数值的比较过程,而这种操作在时间上和运算量上的开销很小。

5.4　格式兼容和容错性能分析

本加密算法的加密对象是图像信息,使用加密算法后图像数据的数据头和标识信息并没有变化。因此,在接收端或者中间节点处,都能识别出数据类型。本算法满足网络传输过程中格式兼容的要求。

对于有噪的信道传输环境,在网络中传输的压缩数据会因为噪声的影响而有部分数据段出现误码。本加密方案运算基本单元是宏块,信道噪声引起的误码只会使图像在解密端有若干宏块不能恢复原始图像,其他部分仍能正确解码。通常情况下,噪声引起的误码字段比较集中,由此造成解码时图像中某一区域信息完全丢失。在本方案中,解密端置乱恢复将原本集中的误码字段恢复到图像中各分散区域,弱化误码字段对图像视觉效果造成的负面影响,使本加密方案对码流误码的鲁棒性强。

6　总　结

本文提出了一种基于二次置乱的加密算法。相较于以往一些基于一次置乱的加密算法而言,本文所提出的加密算法在安全性和压缩效率上有了很大提高。理论分析及实验结果表明,本算法对码率、运算复杂度的负面影响很小,不会给编码过程引入新的误差,同时满足格式兼容,并具有较好的容错性能,是一种适合网络传输的图像加密算法。但是,本算法并没有改变量化后的 DC 系数数值,根据 Q 的取值不同会有部分 AC 系数位置不变,这些都会泄露一定的信息。

本加密算法仅考虑了图像的加密,如何将这种加密算法推广至视频等其他多媒体,扩大其使用范围,是下一步考虑的主要问题。

参考文献(References)

1　Ding Wei, Yan Wei-qi, Qi Dong-xu. Digital image scrambling technology based on arnold transformation[J]. Journal of Computer-aided Design & Computer Graphics, 2001, **13**(4):338-341. [丁伟,阎伟齐,齐东旭. 基于 Arnold 变换的数字图像置乱技术[J]. 计算机辅助设计与图形学报,2001,**13**(4):338-341.]

2　Zhu Gui-bin, Cao Chang-xiu, Hu Zhong-yu. An image scrambling and encryption algorithm based on affine transformation[J]. Journal of Computer-aided Design & Computer Graphics, 2003, **15**(6): 711-715. [朱桂斌,曹长修,胡中豫. 基于仿射变换的数字图像置乱加密算法[J]. 计算机辅助设计与图形学报,2003,**15**(6): 711-715.]

3　Bai Sen, Cao Chang-xiu. Property of sub-affine transformation and its application[J]. Journal of Computer-aided Design & Computer Graphics, 2003, **15**(2):205-208. [柏森,曹长修. 亚仿射变换的性质及其应用[J]. 计算机辅助设计与图形学报,2003,**15**(2): 205-208.]

4　Qi Dong-xu, Zou Jiang-cheng. A new permuted transformation and its application in data encryption[J]. Science in China (Series E). 2000, **30**(5):440-447. [齐东旭,邹建成. 一类新的置乱变换及其在图像信息隐藏中的应用,中国科学,2000,**30**(5):440-447.]

5　Wang dong-shun, Yang Di-lian, Qi Dong-xun. Two classes of nonlinear transformations for digital image and their periodicity[J]. Journal of Computer-aided Design & Computer Graphics, 2001, **13**(9):828-833. [王道顺,杨地莲,齐东旭. 数字图像的两类非线性变换及其周期性,计算机辅助设计与图形学报,2001, **13**(9):828-833.]

6　Yao Ye, Xu Zheng-quan, Yang Zhi-yun. MaroBlock permutation video encryption approach based on pseudo-random sequence[J]. Computer Engineering, 2005, **31**(20):162-164. [姚晔,徐正华,杨志云. 基于伪随机序列的宏块置乱视频加密方案[J]. 计算机工程,2005, **31**(20):162-164.]

7　Tang L. Methods for encryption and decryption MPEG video data efficiently[A]. In: Proceedings of the 4th ACM International Multimedia Conference[C], Boston, MA, USA, 1996:219-229.

8　Qiao Lin-tian, Nahrstedt Klara. Comparison of MPEG encryption Algorithms[J]. Comput & Graphics, 1998, **22**(4):437-448.

9 Tosun Ali Saman, Feng Wu-chi, Efficient multi-layer coding and encryption of MPEG video streams[A]. In: Proceedings of IEEE International Conference on Multimedia and Expo[C], New York, NY, USA, 2000:119-122.

10 Zeng Wen-jun, Lei Shaw-min. Efficient frequency domain video scrambling for content access control [J]. IEEE Transactions on Multimedia,2003,**5**(1):118-129

11 Schneier B. Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in C[M]. Brisbane, Queensland, Australia: John Wiley and Sons,1996. [Schneier B 著. 应用密码学: 协议、算法与 C 语言源程序[M]. (第 2 版)吴世忠等译. 北京: 机械工业出版社,2000.]

12 Independent JPEG Group's JPEG software, version 6b[EB/OL]. http://www.ijg.org, 2008-4-16/2009-1-19.