



1. 一种对JPEG加密图像的快速攻击方法,其特征在于,包括以下步骤:  
设计明文图像DP的量化DCT系数矩阵dctDP;  
按照JPEG图像编码标准对矩阵dctDP进行解码,获得对应的设计JPEG明文图像DP;  
对设计JPEG明文图像DP进行加密,获得对应的JPEG密文图像DC;  
将JPEG密文图像DC的量化DCT系数矩阵分块,求解出全部区块加密前后的映射关系;  
将要攻击的密文图像C的量化DCT系数矩阵dctC分块,按照区块加密前后的映射关系来移动区块的位置,得到攻击结果A;  
由攻击结果A生成攻击图像G。
2. 根据权利要求1所述对JPEG加密图像的快速攻击方法,其特征在于:密文图像C的量化DCT系数矩阵dctC的行与列分别为M和N, JPEG编码使M和N都能被8整除。
3. 根据权利要求2所述对JPEG加密图像的快速攻击方法,其特征在于,所述设计明文图像DP的量化DCT系数矩阵dctDP包括以下步骤:首先将0与矩阵dctC中的每个元素相乘,得到和dctC行列数相同的矩阵dctDP1;然后将矩阵dctDP1分为 $M*N/64$ 个 $8*8$ 区块,将数字 $r+(c-1)*N/2$ 转换为64位二进制数,将这个二进制数作为一维向量,从最低位向上,每8位作为一列,转换为 $8*8$ 二维矩阵,赋值给矩阵dctDP1的第r行c列个区块;按上述方法生成共 $M*N/64$ 个 $8*8$ 的量化DCT系数区块,由生成的量化DCT系数区块组成矩阵dctDP。
4. 根据权利要求1所述对JPEG加密图像的快速攻击方法,其特征在于,将JPEG密文图像DC的量化DCT系数矩阵分成 $M*N/64$ 个 $8*8$ 区块;  
所述求解出全部区块加密前后的映射关系包括以下步骤:对于第u行v列的区块,令所有非零系数等于1,将其64个元素按列拉伸为一维向量,成为一个64位的二进制数B,将此二进制数转换为十进制数D,由此解出该区块在明文图像量化DCT系数矩阵中的位置,其行数按照取模运算的计算表达式为 $r=\text{mod}(D, N/8)$ ,列数按照向上取整运算的计算表达式为 $c=\text{ceil}(D*8/N)$ ;由此求解得到区块加密前后的映射关系 $(r, c) \rightarrow (u, v)$ 。
5. 根据权利要求1所述对JPEG加密图像的快速攻击方法,其特征在于,将要攻击的密文图像C的量化DCT系数矩阵dctC分成 $M*N/64$ 个 $8*8$ 区块,所述按照区块加密前后的映射关系来移动区块的位置为将其这些区块的位置 $(u, v)$ 移动到 $(r, c)$ ,得到攻击结果A。
6. 根据权利要求5所述对JPEG加密图像的快速攻击方法,其特征在于,所述由攻击结果A生成攻击图像G包括以下步骤:依次数出攻击结果A第i行j列个 $8*8$ 区块中的非零个数 $NZ(i, j)$ ,生成攻击图像G,其尺寸为 $(M/8)*(N/8)$ ,其第i行j列位置像素的灰度值为 $NZ(i, j)*255/\max(NZ(i, j))$ ,其中, $\max(NZ(i, j))$ 运算指找出所有 $NZ(i, j)$ 中的最大值。
7. 根据权利要求1所述对JPEG加密图像的快速攻击方法,其特征在于:所述的攻击图像G为原始明文图像加密后的概图。
8. 根据权利要求1所述对JPEG加密图像的快速攻击方法,其特征在于:所述要攻击的密文图像C是原始明文图像P通过加密算法加密后获得的密文图像。
9. 一种JPEG加密图像的快速攻击系统,其特征在于,包括:  
设计模块,用于设计明文图像DP的量化DCT系数矩阵dctDP;  
解码模块,用于按照JPEG图像编码标准对矩阵dctDP进行解码,获得对应的设计JPEG明文图像DP;  
加密模块,用于对设计JPEG明文图像DP进行加密,获得对应的JPEG密文图像DC;

求解模块,用于将JPEG密文图像DC的量化DCT系数矩阵分块,求解出全部区块加密前后的映射关系;

移位模块,用于将要攻击的密文图像C的量化DCT系数矩阵dctC分块,按照区块加密前后的映射关系来移动区块的位置,得到攻击结果A;

攻击模块,用于由攻击结果A生成攻击图像G。

10.一种计算机可读存储介质,所述计算机可读存储介质存储有计算机程序,其特征在于:所述的计算机程序被处理器执行时实现如权利要求1至8中任意一项所述对JPEG加密图像的快速攻击方法的步骤。

## JPEG加密图像的快速攻击方法、系统及可读存储介质

### 技术领域

[0001] 本发明属于图像处理领域,具体涉及一种JPEG加密图像的快速攻击方法、系统及可读存储介质。

### 背景技术

[0002] 图像加密是保护数字图像安全性的关键技术,主要是通过加密算法来隐藏视觉信息,从而保护图像内容的安全。JPEG是联合图像专家组(Joint Photographic Experts Group)的简称,JPEG是最常见的图像压缩和编码标准。对于使用JPEG标准编码后的图像进行加密,要尽量维持压缩率,并且加密方案要能抵御常见的攻击方法。为了维持压缩率,大多数JPEG图像的加密算法对量化离散余弦变换(DCT)系数中的零系数通常不进行加密,也就是量化DCT系数矩阵中非零系数的数量不变。传统的加密操作主要有:1、量化DCT系数8\*8区块中非零系数的个数和位置保持不变,只改变非零系数的值;2、改变量化DCT系数8\*8区块中非零系数的位置。JPEG图像量化DCT系数8\*8区块中的非零系数的数量能反映图像对应区域的边缘信息与纹理信息。因此,这两类JPEG图像传统加密操作存在泄露明文图像信息的风险。

[0003] 为了回避这个风险,一种改进的JPEG图像加密算法块间混洗算法IBS(Inter-block-shuffle)被提出。IBS加密算法的混洗不改变量化DCT系数8\*8区块内非零系数的数量,混洗这些区块,改变了区块的位置。因此这种算法能够抵抗非零计数NZCA(Number of none-zero-coefficient attack)的攻击。这种改进的加密算法改变了量化DCT系数矩阵的8\*8区块位置,从而保护了原始明文图像的纹理和边缘信息。由于该方案没有改变分块内非零系数的个数,而选择明文攻击可以通过改变每个块中非零DCT系数的数量来找出原始块和加密块之间的位置映射关系,因此,这种加密算法被证明可以被选择明文攻击方法破解。

[0004] 例如,论文Shanshan Li,Ruolan Ma,Hongli Zhang,Enhancing Security for JPEG Image Against Mosaic Attack Using Inter-Block Shuffle Encryption,IEEE Access,VOLUME 7,2019,72696-72702提出的攻击方法。这种攻击方法通过设计明文,每次加密能够解出64个区块位置混洗前后的映射关系。而对于尺寸大于64\*8\*8的图像,这种攻击方法需要对多副设计明文图像进行加密和寻找位置混洗的映射关系,因此存在攻击速度较慢的缺点。

### 发明内容

[0005] 本发明的目的在于针对上述现有技术中大尺寸的JPEG加密图像攻击速度较慢的缺点,提供一种JPEG加密图像的快速攻击方法、系统及可读存储介质,有效提高大尺寸图像的攻击速度,缩短攻击时间。

[0006] 为了实现上述目的,本发明有如下的技术方案:

[0007] 一种对JPEG加密图像的快速攻击方法,包括以下步骤:

[0008] 设计明文图像DP的量化DCT系数矩阵dctDP;

- [0009] 按照JPEG图像编码标准对矩阵dctDP进行解码,获得对应的设计JPEG明文图像DP;
- [0010] 对设计JPEG明文图像DP进行加密,获得对应的JPEG密文图像DC;
- [0011] 将JPEG密文图像DC的量化DCT系数矩阵分块,求解出全部区块加密前后的映射关系;
- [0012] 将要攻击的密文图像C的量化DCT系数矩阵dctC分块,按照区块加密前后的映射关系来移动区块的位置,得到攻击结果A;
- [0013] 由攻击结果A生成攻击图像G。
- [0014] 作为本发明的一种优选方案,密文图像C的量化DCT系数矩阵dctC的行与列分别为M和N,JPEG编码使M和N都能被8整除。
- [0015] 作为本发明的一种优选方案,所述设计明文图像DP的量化DCT系数矩阵dctDP包括以下步骤:首先将0与矩阵dctC中的每个元素相乘,得到和dctC行列数相同的矩阵dctDP1;然后将矩阵dctDP1分为 $M*N/64$ 个 $8*8$ 区块,将数字 $r+(c-1)*N/2$ 转换为64位二进制数,将这个二进制数作为一维向量,从最低位向上,每8位作为一列,转换为 $8*8$ 二维矩阵,赋值给矩阵dctDP1的第r行c列个区块;按上述方法生成共 $M*N/64$ 个 $8*8$ 的量化DCT系数区块,由生成的量化DCT系数区块组成矩阵dctDP。
- [0016] 作为本发明的一种优选方案,将JPEG密文图像DC的量化DCT系数矩阵分成 $M*N/64$ 个 $8*8$ 区块;所述求解出全部区块加密前后的映射关系包括以下步骤:对于第u行v列的区块,令所有非零系数等于1,将其64个元素按列拉伸为一维向量,成为一个64位的二进制数B,将此二进制数转换为十进制数D,由此解出该区块在明文图像量化DCT系数矩阵中的位置,其行数按照取模运算的计算表达式为 $r=\text{mod}(D,N/8)$ ,列数按照向上取整运算的计算表达式为 $c=\text{ceil}(D*8/N)$ ;由此求解得到区块加密前后的映射关系 $(r,c) \rightarrow (u,v)$ 。
- [0017] 作为本发明的一种优选方案,将要攻击的密文图像C的量化DCT系数矩阵dctC分成 $M*N/64$ 个 $8*8$ 区块,所述按照区块加密前后的映射关系来移动区块的位置为将其这些区块的位置 $(u,v)$ 移动到 $(r,c)$ ,得到攻击结果A。
- [0018] 作为本发明的一种优选方案,所述由攻击结果A生成攻击图像G包括以下步骤:依次取出攻击结果A第i行j列个 $8*8$ 区块中的非零个数 $NZ(i,j)$ ,生成攻击图像G,其尺寸为 $(M/8)*(N/8)$ ,其第i行j列位置像素的灰度值为 $NZ(i,j)*255/\max(NZ(i,j))$ ,其中, $\max(NZ(i,j))$ 运算指找出所有 $NZ(i,j)$ 中的最大值。
- [0019] 作为本发明的一种优选方案,所述的攻击图像G为原始明文图像加密后的概图。
- [0020] 作为本发明的一种优选方案,所述要攻击的密文图像C是原始明文图像P通过加密算法加密后获得的密文图像。
- [0021] 本发明还提供一种JPEG加密图像的快速攻击系统,包括:
- [0022] 设计模块,用于设计明文图像DP的量化DCT系数矩阵dctDP;
- [0023] 解码模块,用于按照JPEG图像编码标准对矩阵dctDP进行解码,获得对应的设计JPEG明文图像DP;
- [0024] 加密模块,用于对设计JPEG明文图像DP进行加密,获得对应的JPEG密文图像DC;
- [0025] 求解模块,用于将JPEG密文图像DC的量化DCT系数矩阵分块,求解出全部区块加密前后的映射关系;
- [0026] 移位模块,用于将要攻击的密文图像C的量化DCT系数矩阵dctC分块,按照区块加

密前后的映射关系来移动区块的位置,得到攻击结果A;

[0027] 攻击模块,用于由攻击结果A生成攻击图像G。

[0028] 本发明还提供一种计算机可读存储介质,所述计算机可读存储介质存储有计算机程序,所述的计算机程序被处理器执行时实现所述对JPEG加密图像的快速攻击方法的步骤。

[0029] 相较于现有技术,本发明至少具有如下的有益效果:只需要一幅明文图像就能够解出加密前后所有区块的映射关系,不需要对多副设计明文图像进行加密和寻找位置混乱的映射关系,因此有效提高了攻击速度,缩短了攻击时间。当图像尺寸较大时,本发明攻击方法的攻击时间较短。随着图像尺寸的增大,本发明攻击方法的时间优势更明显。

## 附图说明

[0030] 为了更加清楚地说明本发明实施例的技术方案,下面将对实施例中所需要使用的附图作以简单地介绍,应当理解,以下附图仅示出了本发明部分实施例,对于本领域普通技术人员而言,在不付出创造性劳动的前提下,还可以根据这些附图获得其他相关的附图。

[0031] 图1本发明快速攻击方法的流程图;

[0032] 图2本发明实施例明文图像:(a) Barbara原图;(b) lena原图;

[0033] 图3本发明实施例经过加密算法加密后的图像:(a) Barbara经过加密后的图像;(b) lena经过加密后的图像;

[0034] 图4本发明实施例经过攻击之后的图像:(a) Barbara经过攻击后的图像;(b) lena经过攻击后的图像。

## 具体实施方式

[0035] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员还可以在没有做出创造性劳动的前提下获得其他实施例。

[0036] 参见图1,本发明的一种对JPEG加密图像的快速攻击方法,包括以下步骤:

[0037] 步骤1)、获取密文JPEG图像C,密文图像对应的量化DCT系数矩阵是 $dctC$ ,其行与列分别为 $M$ 和 $N$ ,JPEG编码使 $M$ 和 $N$ 都可以被8整除;

[0038] 步骤2)、设计明文图像DP的量化DCT系数矩阵 $dctDP$ ,设计原则如下:首先将0与 $dctC$ 中的每个元素相乘,得到和 $dctC$ 行列数相同的矩阵 $dctDP1$ ,将 $dctDP1$ 分为 $M*N/64$ 个 $8*8$ 区块,将数字 $r+(c-1)*N/2$ 转换为64位二进制数,将这个二进制数作为一维向量,从最低位向上,每8位作为一列,转换为 $8*8$ 二维矩阵,赋值给矩阵 $dctDP1$ 的第 $r$ 行 $c$ 列个区块;

[0039] 步骤3)、按照步骤2),生成一共 $M*N/64$ 个 $8*8$ 的量化DCT系数区块,由它们组成矩阵 $dctDP$ ;

[0040] 步骤4)、对步骤3)所获得的 $dctDP$ 按照JPEG图像编码标准进行解码,获得对应的设计JPEG明文图像DP;

[0041] 步骤5)、用加密方案(其参数、密钥全部未知)加密设计的JPEG明文图像DP,获得对应的JPEG密文图像DC。

[0042] 步骤6)、将密文图像DC的量化DCT系数矩阵分成 $M*N/64$ 个 $8*8$ 区块,对于第 $u$ 行 $v$ 列的区块,令所有非零系数等于1,将其64个元素按列拉伸为一维向量,成为一个64位的二进制数 $B$ ,将此二进制数转换为十进制数 $D$ ,由此可以解出该区块在明文图像量化DCT系数矩阵中的位置,其行数 $r=\text{mod}(D, N/8)$ ,列数 $c=\text{ceil}(D*8/N)$ ,其中 $\text{mod}(E, F)$ 运算指 $E$ 对 $F$ 取模运算, $\text{ceil}(E)$ 运算指对数字 $E$ 向上取整运算。

[0043] 由于常用图像的像素个数一般不可能超过设计明文能够取到的最大值 $64*264$ ,因此只需要一幅设计明文图像,可以解出所有加密前后区块的映射关系 $(r, c) \rightarrow (u, v)$ ;

[0044] 步骤7)、按照步骤6)所求解出的所有 $8*8$ 区块的映射关系,将要攻击的密文图像C的量化DCT系数矩阵 $\text{dctC}$ 分成 $M*N/64$ 个 $8*8$ 区块,将其这些区块的位置 $(u, v)$ 移动到 $(r, c)$ ,得到攻击结果A;

[0045] 步骤8)、对攻击结果A,依次数出第 $i$ 行 $j$ 列个 $8*8$ 区块中的非零个数 $NZ(i, j)$ ,生成攻击图像G,其尺寸为 $(M/8)*(N/8)$ ,其第 $i$ 行 $j$ 列位置像素的灰度值为 $NZ(i, j)*255/\max(NZ(i, j))$ ,其中 $\max(NZ(i, j))$ 运算指找出所有 $NZ(i, j)$ 中的最大值。

[0046] 攻击图像G是密文图像C经过这种新型的快速攻击方法得到的结果概图。

[0047] 步骤1)的密文JPEG图像C是将明文图像P通过待攻击的加密方案加密后获得的密文图像,该方案通过改变图像的非零DCT系数的数值和块间混洗的方法来加密JPEG图像;

[0048] 步骤2)中通过将64位的二进制数转换为 $8*8$ 二维矩阵,赋值给 $\text{dctDP1}$ 中的第 $r$ 行 $c$ 列个区块,从而改变了 $\text{dctDP1}$ 中非零系数的个数,得到新的矩阵 $\text{dctDP}$ 。

[0049] 步骤6)中因为一般图像的像素点数不会超过 $64*264$ ,所以只需要一幅明文图像就可以接触加密前后区块的所有映射关系,可得到最终的概图攻击结果。

[0050] 下面结合实施例对本发明做进一步详细说明:

[0051] 步骤一:以图2(a)所示的Barbara原图和图2(b)所示的lena原图为例,将明文图像P通过待攻击的加密方案加密后获得任意密文图像C,如图3(a)和图3(b)所示。

[0052] 步骤二:设计密文图像的每个 $8*8$ 区块,区块在图像中的的位置为第 $r$ 行 $c$ 列,将数字 $r+(c-1)*N/2$ 转换为64位二进制数,将这个二进制数作为一维向量,从最低位向上,每8位作为一列,转换为 $8*8$ 二维矩阵,赋值给矩阵 $\text{dctDP1}$ 的第 $r$ 行 $c$ 列个区块,全部赋值后得到设计明文的量化DCT系数矩阵 $\text{dctDP}$ 。

[0053] 步骤三:对攻击结果A,依次数出第 $i$ 行 $j$ 列个 $8*8$ 区块中的非零个数 $NZ(i, j)$ ,生成攻击图像G,其尺寸为 $(M/8)*(N/8)$ ,其第 $i$ 行 $j$ 列位置像素的灰度值为 $NZ(i, j)*255/\max(NZ(i, j))$ ,其中 $\max(NZ(i, j))$ 运算指找出所有 $NZ(i, j)$ 中的最大值。G即本发明的最终攻击结果,它是明文图像的概图,能反应明文图像的主要内容,如图4(a)和图4(b)所示。

[0054] 本发明通过将64位二进制数转换为 $8*8$ 二维矩阵,赋值给 $\text{dctDP1}$ 中的第 $r$ 行 $c$ 列个区块,从而改变了 $\text{dctDP1}$ 中非零系数的个数得到新的矩阵 $\text{dctDP}$ ,按照JPEG图像编码标准进行编解码,获得对应的设计JPEG明文图像DP;在加密参数和密钥全部未知的情况下,加密DP图像得到对应的密文图像DC。另一方面,因为一般图像的像素点数不会超过 $64*264$ ,所以只需要一幅明文图像就可以解出加密前后所有区块的映射关系,得到最终结果。与论文Shanshan Li, Ruolan Ma, Hongli Zhang, Enhancing Security for JPEG Image Against Mosaic Attack Using Inter-Block Shuffle Encryption, IEEE Access, VOLUME 7, 2019, 72696-72702提出的攻击方法相比,攻击速度明显加快。表1列举出了针对不同尺寸密文图

像攻击的时间对比,由试验结果可以看出,当图像尺寸较小时,本发明的攻击时间长于参考文献的方案。当图像尺寸较大时,本发明的攻击时间较短。随着图像尺寸的增大,本发明的时间优势更明显。

[0055] 表1

|        |           |               |            |
|--------|-----------|---------------|------------|
| [0056] | 图像尺寸      | 参考文献方案攻击时间(秒) | 本方案攻击时间(秒) |
|        | 128*128   | 0.0237        | 0.0466     |
|        | 256*256   | 0.1868        | 0.1627     |
|        | 512*512   | 2.5613        | 0.6583     |
|        | 1024*1024 | 42.0221       | 2.5522     |

[0057] 本发明还提供一种JPEG加密图像的快速攻击系统,包括:

[0058] 设计模块,用于设计明文图像DP的量化DCT系数矩阵dctDP;

[0059] 解码模块,用于按照JPEG图像编码标准对矩阵dctDP进行解码,获得对应的设计JPEG明文图像DP;

[0060] 加密模块,用于对设计JPEG明文图像DP进行加密,获得对应的JPEG密文图像DC;

[0061] 求解模块,用于将JPEG密文图像DC的量化DCT系数矩阵分块,求解出全部区块加密前后的映射关系;

[0062] 移位模块,用于将要攻击的密文图像C的量化DCT系数矩阵dctC分块,按照区块加密前后的映射关系来移动区块的位置,得到攻击结果A;

[0063] 攻击模块,用于由攻击结果A生成攻击图像G。

[0064] 本发明还提供一种计算机可读存储介质,计算机可读存储介质存储有计算机程序,所述的计算机程序被处理器执行时实现如所述对JPEG加密图像的快速攻击方法的步骤。

[0065] 所述的计算机程序可以被分割成一个或多个模块/单元,所述一个或者多个模块/单元被存储在所述存储器中,并由所述处理器执行,以完成本发明JPEG加密图像的快速攻击方法。

[0066] 以上所述的仅仅是本发明的较佳实施例,并不用以对本发明的技术方案进行任何限制,本领域技术人员应当理解的是,在不脱离本发明精神和原则的前提下,该技术方案还可以进行若干简单的修改和替换,这些修改和替换也均属于权利要求书所涵盖的保护范围之内。

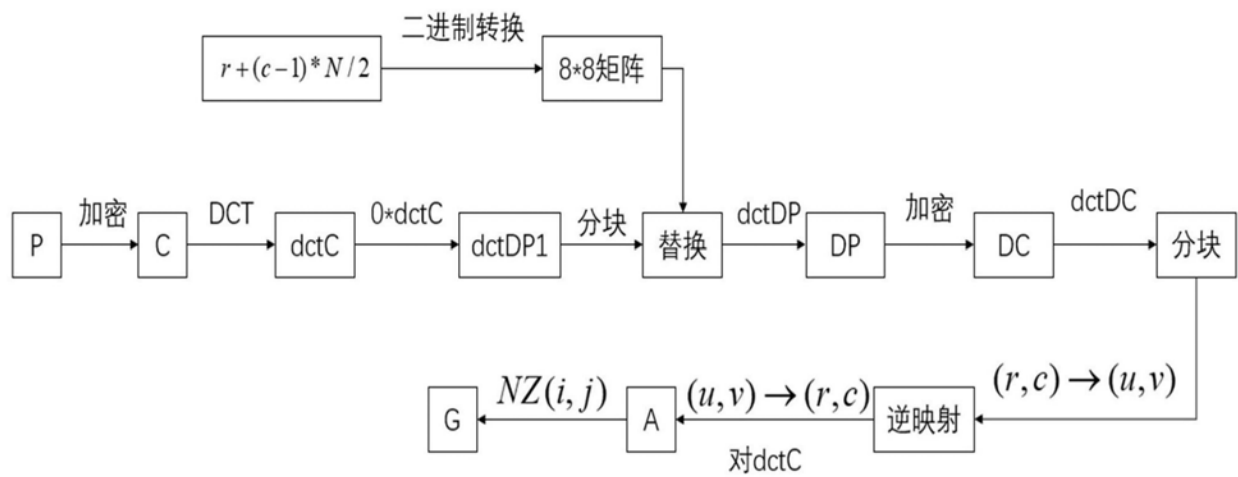


图1

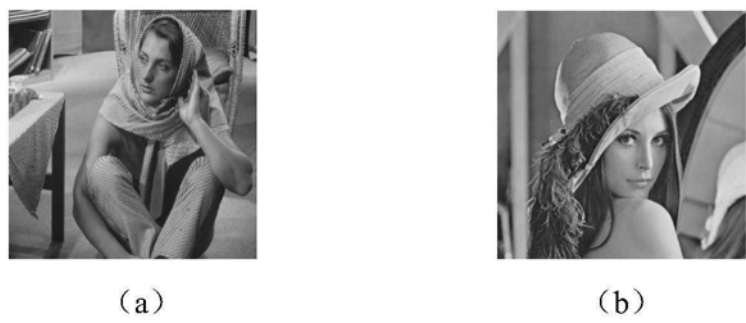


图2



图3



(a)



(b)

图4