一种基于混沌的JPEG2000图像加密算法

邓绍江 李艳涛 张岱固 杨吉云
(重庆大学计算机学院 重庆 400044)

摘 要 首先设计出一个性能优异的基于混沌系统的矩阵置乱算法。由于JPEG2000图像小波变换后的重要信息多集中在小波系数的低频系数部分,图像加密算法只选择了小波系数的低频分量进行置乱加密。算法巧妙地避免了以往基于JPEG2000图像加密的一些缺点,很好地将加密、解密与图像的编码、解码相结合。最后,实验验证并分析了算法的可行性和优越性,实验证明该算法复杂度高、保密性好、加密效率高,而又未明显降低图像的压缩率,具有很好的加密特性。

关键词 混沌,图像加密

JPEG2000 Digital Image Encryption Algorithm Based on Chaotic System

DENG Shao-jiang LI Yan-tao ZHANG Dai-gu YANG Ji-yun
(College of Computer Science of Chongqing University, Chongqing 400044, China)

Abstract This paper designed a matrix scrambling algorithm based on the chaotic system firstly which has excellent performance. As most important image information after DWT was concentrated upon the part of the lowest approximation coefficient, the image encryption algorithm was designed only to scramble the lowest approximation coefficient matrix for encryption. Therefore, the algorithm, which overcomes some shortcomings existing in preceding image encryption based on JPEG2000 skillfully, well comebined the encryption, decryption with image coding and decoding. Finally, experiments were implemented to testify and analyse the feasibility and superiority of the algorithm, and the results prove that the algorithm is characterized by high complexity, good performance of security and encoding efficiency.

Keywords Chaotic, Image encryption

JPEG[1]和JPEG2000[2-4]是目前被普遍运用的两个重要的图像压缩标准。由于小波变换在图像压缩领域有着众多优越特性,JPEG2000势必将成为新一代静止图像压缩的国际标准。小波变换因而也引起了人们的广泛关注。JPEG2000图像的加密算法也逐渐被人们所研究[7,8],出现了一些图像小波域内的加密算法。

1 已有JPEG2000图像加密算法存在的一些问题

在JPEG2000核心编码过程中,图像经过预处理,被分割成不重叠的矩形块,即瓦片。JPEG2000静止图像压缩标准中的离散小波变换是对每一个瓦片的每一个分量进行的。每一个瓦片分量(tile component)独立进行变换产生一系列的二维子带信息。经过一次小波变换后,每个瓦片分量被分为LL,HL,LH,HH。每一个子带代表了原图像在不同分辨率上、不同频带的表现。

在JPEG2000图像的小波系数加密中,为了避免传统加密对小波系数值的改变引起小波系数能量分布和相关性的破坏,对小波系数进行置乱加密的方法用得比较多。小波系数的置乱主要存在有两种不同的形式,分别为CWW和CWF[5],如图1所示。CWW(Confusion of wavelet coefficients on the whole image)即对小波系数在整幅图像范围内进行置乱。CWF(Confusion of wavelet coefficients on the subbands in frequency domain)即对小波系数在不同分辨率的不同子带范围内进行置乱。两种置乱方式都能达到一定的加密效果,但由于各自本身的特点,也分别存在一定的不足之处。

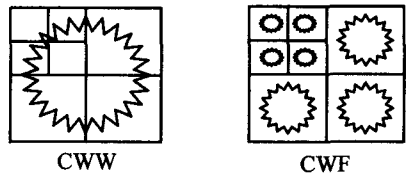

图1 CWW和CWF小波系数置乱方法

CWW的不足主要表现在整个图像范围内置乱小波系数,势必会造成高低频系数之间的迁移。而JPEG2000能达到较高压缩率的其中一个重要措施就是对高频系数用较少比特进行量化甚至对部分高频系数忽略。若高频系数迁移到低频子带,将严重影响编码效率。而低频系数迁移到高频子带,将会造成量化误差,造成图像信息的丢失或者锐减,严重影响解码图像的质量,甚至还会造成比特溢出而无法继续编码过程。

CWF的不足表现为:首先,它破坏了小波变换多分辨率

到稿日期:2008-12-30 本文受国家自然科学基金资助项目(60873201,60703035)资助。
邓绍江 副教授,博士后,主要研究方向为混沌密码;张岱固 博士研究生,主要研究方向为混沌密码学。

分解树型结构。由于小波变换后其系数构成一个树型结构，不同层数上、不同分辨率的小波系数都和相邻层上的小波系数有对应关系。JPEG2000 的编码也要充分利用这种树型结构对应关系。CWF 对每个子带进行的独立置乱，使这种树型结构对应关系遭到破坏，会影响编码效率和压缩率。另外，CWF 计算量太大。由于能量集中在低频，只有少数能量分布在高频小波系数中。高频小波系数的置乱对图像影响很小，但所需的计算量和密钥长度却非常大，导致编解码的效率将变得非常的低下。

本文最终设计的只针对小波系数矩阵水平低频-垂直低频分量进行置乱的方法，很大程度上避免了高低频系数的迁移，避免了树形结构的破坏，能适应小波变换之后的熵编码等过程，且计算量小。

2 本文算法设计思路

本文算法的基本思想（如图 2 所示）是在原始图像经预处理后，在正向小波变换过程中，针对图像主要信息集中在小波系数矩阵的水平低频-垂直低频分量（LL）中这一特点，为提高加密效果，只针对每次小波变换后的 LL 矩阵进行置乱，并且根据 JPEG2000 编码过程中不同的分层次数会存在相对稳定的最优编码效率的特点。为提高加密算法的效率，选择了比较合适的置乱次数（对前三层小波分解），使得算法得到优化。

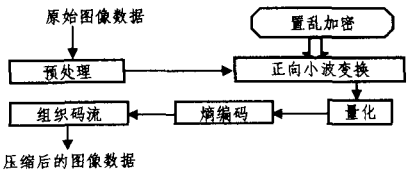

图 2 算法设计思想框图

3 基于混沌的矩阵置乱算法

置乱算法设计思想：按行从上至下、每行中从左至右的顺序遍历原始矩阵 I 中的每个元素，使其与矩阵中随机的任意一个元素进行对换。此过程中通过 Logistic 映射产生混沌序列值，将其离散化后生成与原矩阵等大的矩阵 D,H,L，其中 D 矩阵中的值用来控制矩阵 I 中元素的对换规则，H,L 矩阵中的值用来控制矩阵 I 中元素横向和纵向的移动距离。通过对矩阵 I 中每个元素的对换实现矩阵 I 的置乱。

算法的具体描述如下：

对任意一个矩阵 $I(m\times n)$，设矩阵 I 中元素的位置用 (i,j) 表示，其中 $i\in\{0,1,\cdots,m-1\}$，$j\in\{0,1,\cdots,n-1\}$。分别取矩阵 I 宽度的位长 l 和长度的位长 s，$l=\lceil\log_2 m\rceil$，$s=\lceil\log_2 n\rceil$。其中运算符$\lceil\ \rceil$是表示向上取整运算。

① 置乱加密过程

1）以 k_0 为初始值（同时也作为解密算法的密钥），通过 Logistic 映射迭代产生混沌序列值。取迭代 10000 次后的 $3mn$ 个迭代值 $X=\{x_0,x_1,\cdots,x_{3mn-1}\}$。

2）从 X 序列中取 x_{3t}（其中 $t=0,1,\cdots,mn-1$），构造与原始矩阵 I 等大的矩阵 $D(m\times n)$，使得

$D(i,j)=\lfloor 4x_{3t}\rfloor$（其中 $t=i\times n+j$）；

其中运算符$\lfloor\ \rfloor$是向下取整运算，这样 $D(i,j)\in\{0,1,2,3\}$。

3）从 X 序列中分别取 x_{3t+1},x_{3t+2}（其中 $t=0,1,\cdots,mn-1$），分别构造与原始矩阵 I 等大的矩阵 $L(m\times n)$，$H(m\times n)$，使得

$L(i,j)=\lfloor 2^s\times x_{3t+1}\rfloor$（其中 $t=i\times n+j$）；

$H(i,j)=\lfloor 2^l\times x_{3t+2}\rfloor$（其中 $t=i\times n+j$）；

这样 $L(i,j)\in\{0,1,\cdots,2^s-1\}$；$H(i,j)\in\{0,1,\cdots,2^l-1\}$。

4）从第一行起至第 m 行，对任意行 i，从 $I(i,1)$ 到 $I(i,n)$，遍历每个元素，使之分别与原始矩阵 I 中的一个元素 $I(p,q)$ 交换，$I(i,j)\Leftrightarrow I(p,q)$。其中

$$p=\begin{cases}(i-L(i,j))\bmod n, D(i,j)=0,1\\(i+L(i,j))\bmod n, D(i,j)=2,3\end{cases}$$

$$q=\begin{cases}(j-H(i,j))\bmod m, D(i,j)=0,3\\(j+H(i,j))\bmod m, D(i,j)=1,2\end{cases}$$

② 置乱解密过程

1）同加密过程的 3 个步骤

2）从第 m 行起至第一行，对任意行 i，从 $I(i,n)$ 到 $I(i,1)$，遍历每个元素，使之分别与原始矩阵 I 中的一个元素 $I(p,q)$ 交换，$I(i,j)\Leftrightarrow I(p,q)$。其中

$$p=\begin{cases}(i-L(i,j))\bmod n, D(i,j)=2,3\\(i+L(i,j))\bmod n, D(i,j)=0,1\end{cases}$$

$$q=\begin{cases}(j-H(i,j))\bmod m, D(i,j)=1,2\\(j+H(i,j))\bmod m, D(i,j)=0,3\end{cases}$$

4 加密算法的设计

JPEG2000 编码器必须确定小波变换分解层次。标准允许 0～32 层，但随着分解层次的增加，编码效率会逐渐增加到一个最优点，然后相对稳定（可能有比较微小的减少）。表 1 列出的是 512×512 像素的灰度图片 lena 进行小波变换分解，层次从 1 层到 9 层，在不同压缩比例下的重构图像的峰值信噪比[6]。从表中可以看出，分解 3 层至 5 层时就能很接近最优的编码效率，所以 JPEG2000 在编码过程中的分解层数以 5 层至 6 层作为比较合理的默认层数。为了提高加密效率，对进行 k 层（0 到 $k-1$，$k>3$）小波变换的图像，设计算法只对第 $k-1,k-2,k-3$ 这 3 层的水平低频-垂直低频（LL）子带分量矩阵进行置乱。

表 1 小波变换分层数对分层编码性能的影响（单位：dB）

码率	分层数								
/bpp	1	2	3	4	5	6	7	8	9
0.25	21.4	29.89	32.51	33.03	33.24	33.26	33.25	33.25	33.22
0.5	27.66	34.41	36.01	36.34	36.36	36.36	36.33	36.33	36.33
1.0	33.30	38.71	39.18	39.36	39.34	39.29	39.29	39.29	39.29

①加密算法：图像在 JPEG2000 的压缩编码过程中，若对图像进行 $k(k\geqslant 3)$ 次小波变换，则可利用上述基于混沌的矩阵置乱算法，对第 $k-1,k-2,k-3$ 这 3 层的水平低频-垂直低频（LL）子带分量矩阵进行置乱。在置乱过程之前，先利用 logistic 映射生成用于置乱的若干控制矩阵：

$\frac{n}{2}\times\frac{n}{2}$ 大小的矩阵：D_{k-1}，L_{k-1}，H_{k-1}。

$\frac{n}{4}\times\frac{n}{4}$ 大小的矩阵：D_{k-2}，L_{k-2}，H_{k-2}。

$\frac{n}{8}\times\frac{n}{8}$ 大小的矩阵：D_{k-3}，L_{k-3}，H_{k-3}。

对每个瓦片分量经离散小波变换所产生的小波系数矩阵中的水平低频-垂直低频（LL_{k-1}）子带分量矩阵进行置乱，置乱后的小波系数矩阵 LL'_{k-1} 再进行离散小波变换，生成新的

子带 LL'_{k-2}，HL'_{k-2}，LH'_{k-2}，HH'_{k-2}。再选取水平低频-垂直低频子带分量矩阵进行置乱，生成新的子带，进行离散小波变换，以此循环。置乱过程中，第 j 层（其中 $k-3\leqslant j\leqslant k-1$）小波系数的置乱使用对应下标相等的控制矩阵 D_j，L_j，H_j。最后图像经过离散小波变换，产生嵌入了加密过程的小波系数矩阵，再对小波系数量化和熵编码，最终形成 JPEG2000 码流，如图 3 所示。

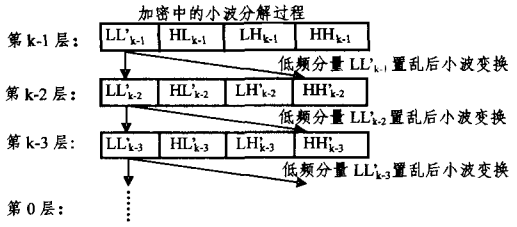

图 3　基于离散小波变换的加密过程示意图

②解密算法：解密过程是加密过程的逆过程。首先利用 logistic 映射生成用于置乱的若干控制矩阵，

$\frac{n}{2}\times\frac{n}{2}$ 大小的矩阵：D_{k-1}，L_{k-1}，H_{k-1}。

$\frac{n}{4}\times\frac{n}{4}$ 大小的矩阵：D_{k-2}，L_{k-2}，H_{k-2}。

$\frac{n}{8}\times\frac{n}{8}$ 大小的矩阵：D_{k-3}，L_{k-3}，H_{k-3}。

JPEG2000 码流在经过熵解码和反量化，在进行反向离散小波变换过程中，依然用与小波变换层数 j（其中 $k-3\leqslant j\leqslant k-1$）对应下标相等的控制矩阵 D_j，L_j，H_j 对每个子带的小波系数反向置乱之后，再进行反向离散小波变换。最终可得到解密解压后的图片。

5　加密算法的实验结果及其分析

以 256×256 像素大小的灰度图片 lena 为加密对象，对 lena 进行加密。实验利用了 Daniel Vollmer 提供的 JPEG2000 开源 C 语言程序代码（© 2001－2002）。在置乱算法中，依然选取 Logistic 映射作为混沌系统，取密钥初值 $k_0=0.8112$，Logistic 映射中取 $\lambda=3.8211$。

图 4 中（1）为 lena. bmp 原图像，（2）为无损压缩下加密后的图像，（3）为无损压缩下解密后的图像，（4）为有损压缩下加密后的图像，（5）为有损压缩下解密后的图像，（6）为有损压缩下错误密钥解密后的图像。从（2）、（4）可以看出，加密后的图像均能很好地隐藏原来图像信息，得到类似于噪声的图像，几乎不能从加密图像中识别原图像的几乎任何信息。而在错误密钥 $k_0=0.81120001$ 解密的情况下，图像解密后并未能获得原图像的任何信息，进一步验证了算法的安全性。

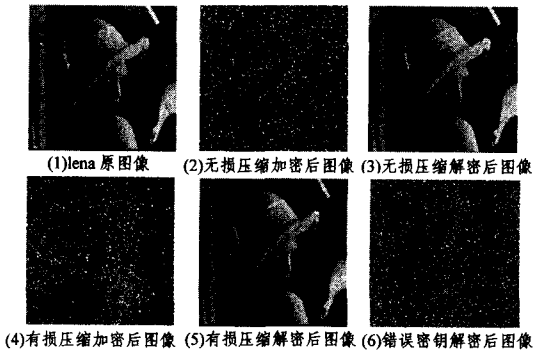

图 4　lena 图像压缩加密、解密实验结果

在相同压缩比、小波变换分层数为 5 的情况下，对有损压缩下解密后图像与原图像进行对比，其峰值信噪比的对比情况如表 2 所列。从数据可见相同压缩比的情况下解密过后图像质量并未见明显下降。反之若保持相同图像质量，不会大大降低图像压缩率。

表 2　解密后图像与原始图像峰值信噪比对比（单位：dB）

码率/bpp	原始图像	解密后图像
0.25	33.24	32.89
0.5	36.36	36.14
1.0	39.34	39.16

相比 CWW 和 CWF 两种针对 JPEG2000 编码过程小波系数的置乱方法，本文所描述的算法较好地避免了 CWW 和 CWF 的缺点。算法只选择前 3 次离散小波变换的水平低频-垂直低频（LL）子带进行置乱，忽略掉细节信息比较集中的高频系数的置乱，这样大大减少了计算量，同时也便于多为零值的高频系数在量化过程中消除，从而达到较好的压缩目的，增强了加密效率，但对加密效果并未产生较大的影响。算法中都是在确定子带进行置乱，没有小波系数的跨子带迁移，因而保证了置乱时不会发生高低频系数迁移，保证了小波变换后的量化和熵编码能顺利进行。另外，小波系数矩阵置乱的按层顺序进行，很好地避免了小波的多分辨率分解树形结构遭到破坏，保证了在小波变换之后的编码过程可以利用这种树形结构关系达到较高的编码效率和压缩率。

结束语　本文所述算法选取基于混沌的置乱方法，很好地利用了混沌系统良好的伪随机性、统计学和拓扑学特性，具有对初值敏感、算法复杂性高、保密性好的诸多优良特性。算法避开了以往 JPEG2000 图像加密中存在的一些问题，可以很好地适用于 JPEG2000 的无损与有损压缩方式，将图像压缩与加密工作结合在一起，是一个比较良好的 JPEG2000 图像加密算法。

参 考 文 献

[1] Wallace G K. The JPEG still picture compression standard. IEEE Trans. Consumer Electronics, 1992, 38(1): xviii-xxxiv

[2] Christopoulos C, Skodras A, Ebrahimi T. The JPEG2000 still image coding system: an overview[J]. IEEE Trans. on Consumer Electronics, 2000, 46(4): 1103-1127

[3] Rabbani M, Joshi R. An overview of the JPEG2000 still image compression standard[J]. Signal Processing: Image Commun., 2002, 17: 3-48

[4] Taubman D S, Marcellin M W. JPEG2000: standard for interactive imaging[C]// Proceedings of The IEEE. 1990(8): 1336-1357

[5] 平亮，孙军，周军. 一种基于 JPEG2000 标准的数字图像加密算法[J]. 视频技术应用与工程，2006，07(1)：87-90

[6] Taubman D S, Marcellin M W. JPEG2000 图像压缩基础、标准和实践[M]. 魏江力，柏正尧，等译. 北京：电子工业出版社，2004

[7] 王智娜，曹伯燕. 基于 JPEG2000 的图像加密算法[J]. 仪器仪表学报，2004，08(25)：243-247

[8] 顾国生，韩国强，王宁，等. 一种保持码流结构的 JPEG2000 加密算法[J]. 计算机科学，2007，34：222-223，263