

一种基于排列变换的数字图像置乱方法

刘建华,袁岁维,范九伦

(西安邮电学院 信息与控制系,陕西 西安 710061)

摘 要: 利用排列变换具有的强不规则性,提出一种数字图像置乱加密方法.借助混沌系统生成的混沌序列得到所需的排列数组,通过对排列数组的数值进行匹配操作,达到对图像行(列)互换的目的,实现对图像的置乱加密.方法对图像大小没有限制.仿真结果表明:该方法具有理想的加密效果和较高的安全性.

关键词: 排列变换;图像置乱;混沌系统;匹配操作

中图分类号: TP391

文献标识码: A

文章编号: 1000-7180(2010)06-0174-03

Digital Image Scrambling Method Based on Permutation Transformation

LIU Jian-hua, YUAN Sui-wei, FAN Jiu-lun

(Department of Information and Control, Xi'an University of Post and Telecommunications, Xi'an 710061, China)

Abstract: Used the strong irregularity of permutation transformation, a digital image scrambling encryption method is proposed. Using the chaos sequences obtained by chaos system to generate the required permutation arrays and through match operation of the array to achieve the purpose of exchange the rows (columns) of image, the purpose to encrypted images is arrived. The proposed method has no limitation for the size of image. Simulation results show that the proposed method has the ideal encryption effect and higher security.

Key words: permutation transformation; image scrambling; chaos system; match operation

1 引言

针对数字图像信息的保护有两种:数字水印技术与图像加密技术.图像置乱技术是一种重要的图像加密技术^[1],与图像分存技术相比,置乱技术不会引起数据量的膨胀,尤其适用于对较大图像的加密处理.传统的图像置乱变换主要有:Arnold变换、Hilbert曲线变换、Gray码变换、Conway游戏、IFS模型、幻方变换等^[2-3].排列变换是一种重要的图像置乱方法,文献[4]给出了一种基于采样理论以及几何运算的排列变换,方法简单且变换速度快,显示了排列理论在图像加密中的重要作用.

混沌系统是一种高度复杂的非线性动态系统^[5],对初始条件和系统参数非常敏感,所生成的混沌序列具有良好的伪随机性.在文献[4]的基础

上,文中提出一种基于排列变换的图像置乱加密方法.排列变换通过混沌系统生成的混沌序列实现.通过将混沌系统的生成序列转化为与图像的行(列)相同长度的排列数组,根据排列数组数值的匹配情形得到图像行(列)的匹配情形,完成行(列)互换的操作,最终达到图像置乱的目的.

2 图像置乱过程

2.1 图像预处理

对大小为 $M \times N$ 的原始图像 A ,为了使置乱结果图像看似平滑且杂乱无章,可以考虑在进行互换操作之前先进行简单的预处理后,再进行置乱处理.预处理过程如下:

假设数字图像灰度值的范围为 $0 \sim 255$,可以将像素点的灰度值用 8 位二进制数表示,鉴于 8 位二

进制数的最高位对该点的灰度值具有决定性作用,对原图像进行简单的预处理时,文中只考虑对所有像素点灰度值二进制表示的最高位进行处理。

利用混沌系统,随机生成系统所需的初值,得到长为 $M \times N$ 的随机序列,选取阈值对序列进行二值化处理后,转化为与图像大小相同的矩阵形式,称为二值矩阵,与原图像相结合,将每一个像素点灰度值二进制表示形式的最高位与二值矩阵中相应的二进制数进行异或运算,其余位保持不变,得到预处理后的结果图像。当然,也可以利用相同的方式对其它位进行异或运算。

2.2 图像置乱

首先考虑图像的行互换操作,随机生成混沌系统所需的初值,利用混沌系统迭代得到长为 M 的随机序列,将序列进行放大取整,得到 M 个随机整数,为了将其转化为1到 M 上的一个排列,应将 M 个随机整数变换为取值在 $1 \sim M$ 之间且互不相同的 M 个整数。

文中提出一种通过取模运算得到排列的方法,为了便于表述,引入主副指针的概念。首先主指针指向随机序列的第二个随机整数处,副指针指向第一个随机整数处,将主副指针指向的两个数进行比较,这里的比较是模 M 比较,以得到互不相同的整数。一旦两个数模 M 后相同,则将主指针指向的随机整数进行加1操作,副指针返回第一位,重新进行模 M 比较;当两个指针指向的数值互不相同,主指针位置不变,副指针指向下一位,直至副指针移动到主指针的前一位,表示主指针所指向的数值与前面所有的数值模 M 后均不相同,然后主指针指向下一位,副指针重新指向第一位,以进行下一位的比较。当主指针指向第 M 位且副指针指向第 $(M-1)$ 位时,表示转化已经完成,得到了 M 个互不相同的整数,最后将得到的 M 个互不相同的整数进行模 M 运算后重新排成一列,记为排列数组,并将数组中的0记为 M ,在比较过程中进行加1操作是为了遍历所有数值,以得到一个完整的排列。

利用已经得到的排列数组,将数组中的数值进行匹配操作,由于数组中的数值互不相同,并且值都在 $1 \sim M$ 之间,所以排列数组 b 的匹配条件为:如果 $b(i) + b(j) = (M+1)$,则表示第 i 位与第 j 位匹配,转换至图像中应为:将原图像中的第 i, j 行互换,由于数组包含了 1 到 M 的所有数值,那么对于 $(1+M) = M+1$,即表示数组中数值为1与 M 所处的两个位置是匹配的,相应的将图像中相应位置

表示的两行进行互换操作。

互换操作对图像大小没有限制,当图像为 M 行时,匹配的对数为 $[M/2]$,其中 $[]$ 表示取整操作。当 M 为偶数时,所有的行都会被改变位置;当 M 为奇数时,因为第 $(M+1)/2$ 与自身相匹配,所以不改变位置,其与行均会改变位置。

按照相同的处理方法,对图像的列也可进行互换操作,所不同的是生成序列的长度有所改变,且匹配条件变为 $b(i) + b(j) = (N+1)$,其余均不改变。

在图像置乱的具体实现过程中,用同一个混沌系统分别得到预处理图像与加密图像所需的混沌序列。通过随机生成不同的初值 x_1, x_2 ,对混沌系统方程进行迭代,从生成序列的第 c 位开始分别取所需长度的混沌序列进行图像处理操作。图像排列变换的过程如下:

Step1:输入待加密的原始图像 A ,大小为 $M \times N$ 。选定整数 $c > 0$,迭代次数 k 。随机生成初值 x_1 ,利用混沌系统生成随机序列,从 c 为开始取长为 $M \times N$ 的随机序列,将其进行二值化处理后转化为与图像大小相同的二值矩阵。

Step2:将原图像中所有像素值表示为二进制形式,将图像二进制表示最高位的二进制数与二值矩阵中相应位置处的二进制数进行异或运算,其余位保持不变,得到经预处理后的结果图像 B 。

Step3:随机生成初值 x_2 ,利用混沌系统生成随机序列,从 c 开始依次取长为 $(M+N)$ 的随机序列,其中前 M 个随机数用于行互换,后 N 个随机数用于列互换,分别进行放大取整,得到长度为 M 和 N 的随机整数。

Step4:首先进行行互换操作,将得到的 M 个随机整数进行取模运算,得到 1 到 M 的一个排列,称为行排列数组,将行排列数组中的数值进行匹配操作,将达到匹配条件的数值在数组中的位置记录下来,据此对预处理后结果图像 B 中相应的两行进行互换操作,达到行互换的目的。

Step5:其次进行列互换操作,利用后 N 个随机整数进行相同的取模操作,得到列排列数组,经过匹配操作后,得到匹配的数值在数值中的位置,将列互换操作后的结果图像相应的两列进行互换操作,达到列互换的目的,最终完成一次置乱操作。

Step6:将迭代次数 k 加1,若达到所需的迭代次数,则结束。否则,返回 Step3。

鉴于上述算法具有的对称性,对置乱加密图像

的解密过程是置乱操作的逆过程. 根据接收到的密钥, 按照相同的处理过程和相反的顺序便可以达到对加密图像的解密. 在进行解密时, 需要知道混沌系统方程的初值 x_1, x_2 , 整数 c , 迭代次数 k , 所以算法的密钥空间足够大, 具有高的安全性.

3 实验结果

实验部分采用常用的一维 logistic 混沌系统^[6], 其定义式为:

$$a_{n+1} = \mu \cdot a_n \cdot (1 - a_n) \quad (1)$$

其中, 初值 $a_0 \in (0, 1)$, 参数 $\mu \in (0, 4]$, 当 $3.569946 \dots \leq \mu \leq 4$ 时, Logistic 系统处于混沌状态.

对大小为 256×256 的 lena 图像进行置乱加密, 其中混沌系统的参数取为 4, 整数 c 取为 100, 实验中分别给出了未经预处理及经过预处理后对图像进行置乱加密的结果图像.

图 1 给出了对未经预处理的 lena 进行加/解密的结果图像, 加密时系统的初值为 0.1389, (b) 为加密 2 次得到的结果图像, (c) 为正确解密的结果图像, 以及当初值有 0.0000001 的改变时, 得到的错误解密的结果图像(d), 反映了算法对初值具有高的敏感性. 由于没有进行预处理, 所以图像的直方图在加密前后并不改变, 所以图 1 没有显示图像加密前后直方图的变化.

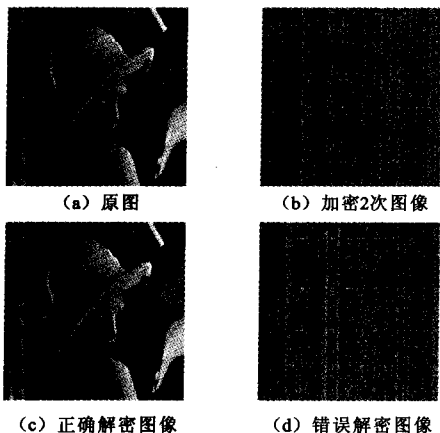


图 1 未经预处理的 lena 加/解密结果图像

图 2 给出了经简单预处理后对 lena 进行加/解密操作得到的结果图像. 预处理时系统的初值为 0.9355, 由于 Logistic 系统生成序列的范围为 $0 \sim 1$, 所以在进行预处理时, 对生成序列进行二值化时阈值取为 0.5, 当序列值大于 0.5 时, 二值化后数值取为 1, 否则二值化后数值取为 0. 加密时系统的初值取

为 0.9169.

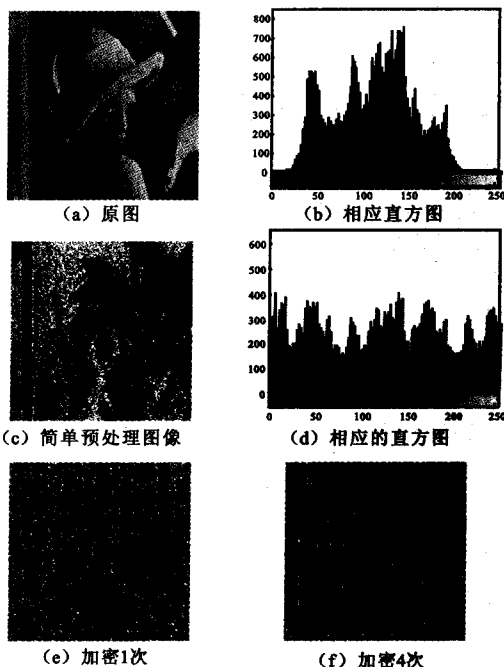


图 2 经预处理的 lena 图像加/解密结果图像

可以看出, 对图像加密之前进行简单的预处理, 可以使最终的加密结果图像具有更好的平滑视觉效果、更好的混乱效果以及更高的安全性.

通过加密效果评价可知, 对于相同的加密次数, 经过简单预处理得到的加密结果图像的相关性的统计平均值比未经预处理得到的加密结果图像的相关性的统计平均值小, 反映出在置换加密之前进行简单的预处理对图像有更好的置乱作用.

4 结束语

文中给出了一种利用混沌系统对图像进行排列变换加密的方法, 通过将图像的所有行(列)进行匹配后互换达到图像置乱的目的. 优点在于: 只要可以得到随机序列, 便可以利用序列得到的匹配结果对图像进行互换处理. 文中方法对图像的大小没有限制, 可以对任意大小的图像进行置乱加密, 适用范围较大, 保证了算法的安全性和实用性. 实验结果表明文中方法加密图像时可以达到理想的置乱加密效果.

参考文献:

- [1] 李昌刚, 韩正之, 张浩然. 图像加密技术综述[J]. 计算机研究与发展, 2002, 39(10): 1317-1324.
- [2] 孔涛, 张亘. Arnold 反变换的一种新算法[J]. 软件学报, 2004, 15(10): 1558-1564.

(下转第 180 页)

Liveness Properties

Dead Markings: None

Dead Transitions Instances:

New_Page'erro1 1

New_Page'error2 1

Live Transitions Instances:

New_Page't1 1

New_Page't2 1

Fairness Properties

New_Page'erro1 1 Fair

New_Page'error2 1 Fair

New_Page't1 1 Impartial

New_Page't2 1 Impartial

对以上状态空间的分析结果如下:

(1) 状态空间图共有个 16 个结点,16 条有向弧;

(2) 强连通图共有 1 个节点 0 条有向弧;

(3) 回归标识指从所有可达标识都能够到达的标识,该模型的标识都是回归标识.

(4) 死结点指没有变迁发生的结点,该模型没有死结点.

(5) 没有死变迁,这意味着每个变迁至少发生了一次.

(6) 公平性如下:变迁 erro1 和 erro2 是公平变

迁;变迁 t1 和 t2 是不公平变迁.

7 结束语

文中通过对基于固定路径的可靠数据传输机制进行建模研究,证明了该机制的正确性、可行性和完备性,能够保证网络数据正确、无误的传输.

参考文献:

- [1] Xu Z, Meng X, Wittbrodt C J, et al. IPv4 address allocation and the evolution of the BGP routing table[C]// Proceedings of IEEE Computer Communications Workshop (CCW). Arlington, 2003.
- [2] Robert Beverly, Karen Sollins, Arthur Berger. SVM learning of IP address structure for latency prediction[C]// Proceedings of the 2006 SIGCOMM workshop on Mining network data. Pisa, Italy, 2006:299-304.
- [3] 袁崇义. Petri 网原理[M]. 北京:北京电子工业出版社, 1998.
- [4] CPN Tools Help[EB/OL]. [2009-10-11]. <http://wiki.daimi.au.dk:8000/cpntools-help/cpntools-help.wiki>
- [5] 曹玉辉,王卫红,覃征,等. 基于有色 Petri 网的动态资源模型[J]. 微电子学与计算机, 2007, 24(8):106-109.
- [6] 喻莉,汪恒晶,戴声奎,等. 粒度区分和可调的无线流媒体可靠传输策略[J]. 微电子学与计算机, 2005, 22(8):121-123.

作者简介:

郑俊辉 男, (1977-), 硕士, 讲师. 研究方向为计算机网络与通信.

王焱 女, (1977-), 博士, 讲师. 研究方向为新型网络体系结构、网络服务质量.

(上接第 176 页)

- [3] 仲兴荣,刘家胜,黄贤武. 一种基于混沌猫映射的图像加密算法[J]. 微电子学与计算机, 2007, 24(12):131-134.
- [4] 吴旻升,王介生,刘慎权. 图像的排列变换[J]. 计算机学报, 1998, 21(6):514-519.
- [5] Marcel Ausloos, Michel Dirickx. The logistic map and the route to chaos[M]. Berlin:Springer, 2006.
- [6] 李鹏,田东平. 基于超混沌序列的数字图像加密算法

[J]. 微电子学与计算机, 2008, 25(3):4-7.

作者简介:

刘建华 男, (1963-). 研究方向为信息安全.

袁岁维 女, (1985-), 硕士研究生. 研究方向为图像处理.

范九伦 男, (1964-), 博士生导师. 研究方向为模式识别、图像处理.