基于ARM7的数字视频加解密系统研究

袁鹏飞

(南京晓庄学院电子工程学院,江苏 南京 211171)

[摘要] 为了在资源受限的ARM7嵌入式平台里实现数字视频加解密系统功能,在达到较好信息隐藏目的同时而不带来庞大的计算量是本文所关注的重点.加密算法方面,本文采用了基于Arnold变换和骑士巡游变换相结合的复合置乱算法.在算法软件实现时,本文对系统开销较大的骑士巡游算法进行了改进,找到一种基于映射表的方法,有效地避免了原算法不停查找巡游矩阵,从而大幅降低ARM7内核的系统开销,将处理一帧图像的速度提高了30倍左右.最后,给出了基于ARM7目标板进行加解密实验的结果分析.

[关键词] 数字视频,加解密,ARM7,骑士巡游变换,Arnold变换

[中图分类号]TP391 [文献标志码]A [文章编号]1672-1292(2015)03-0055-05

Reaserch of Digital Video Encryption and Decryption System Based on ARM7

Yuan Pengfei

(School of Electronic Engineering, Nanjing Xiaozhuang University, Nanjing 211171, China)

Abstract: As ARM7 processor has limited capability of processing digital videos, this article has proposed a new way to implement the video encryption and decryption system based on ARM7 processor. The way that can encrypt the important information of video very effectively costs little calculation of processor and prevents the attacks from hackers.This implementation is based on the composite algorithem of Knight-tour transform and Arnold transform which can benefit from each other.As Knight-tour transform costs lots of calculations of CPU, this article has found a good way based on LUT(Look-up table)to reduce costs of calculation. The experiment based on ARM7 target has approved that the speed of processing a frame of vedio has been improved up to 30 times with the way from this article for encryption.

Key words: digital video, encryption and decryption system, ARM7, Knight-tour transform, Arnold transform

数字视频和图像是信息的重要载体,对视频和图像进行加密保护是最常见的信息隐藏手段之一,而对像素进行空间位置置乱又是信息隐藏技术里发展历史最为悠久且最为成熟的一种方法,比较经典的有骑士巡游变换,Arnold变换,幻方变换等算法[1-3].本文所使用的是基于Arnold变换和骑士巡游变换相结合的复合置乱算法.

1 置乱算法介绍

1.1 Arnold 置乱算法

Arnold变换俗称猫脸变换[4],设有正方形上的点(x,y),将点(x,y)搬移到另一点(x',y')的Arnold变换为:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}N),\ x,y \in \{0,1,\cdots,N-1\}, \tag{1}$$

式中,N为图像的宽度和高度.

迭代使用式(1)可将一幅原始图像充分置乱以符合我们对图像"杂乱无章"的要求.由于Arnold变换具有周期性,利用此特性可以进行置乱恢复.对于给定的自然数$N>2$,Arnold变换(1)式的周期m_N是使得式(2)成立的最小自然数n[5]:

收稿日期:2014-12-11.

通讯联系人:袁鹏飞,工程师,研究方向:嵌入式. E-mail:ypfnuaa0401@126.com

$$\begin{bmatrix} \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{2n+2}-\left(\frac{1-\sqrt{5}}{2}\right)^{2n+2}\right] \\ \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{2n+3}-\left(\frac{1-\sqrt{5}}{2}\right)^{2n+3}\right] \end{bmatrix} (\mathrm{mod}\, N)=\begin{bmatrix}1\\1\end{bmatrix}, \tag{2}$$

由式(2)可计算出不同阶数 N 下 Arnold 变换的周期 m_N,如表1所示:

表1　不同阶数N下Arnold变换周期

Table 1　The period of Arnold transform according to para N

N	2	6	9	10	32	50	64	100	120	128	256	480	512
m_N	3	12	12	30	24	150	48	150	60	96	192	120	384

Arnold算法简单、具有良好的周期性,可充分置乱图像,但由于变换次数是加密的唯一参数,故其安全性是不够的.

1.2　骑士巡游置乱算法

在一块 $n\times n$ 棋盘上,让一位骑士(knight)从任一初始点开始,按国际象棋规则"日"字走动,要求寻找一种方案,使骑士走 n^2-1 步而遍历棋盘上的所有方格(使每个方格恰好经过一次),这就是骑士巡游问题[6].

例如8×8棋盘中的一条骑士巡游路径可用矩阵 $\boldsymbol{T}=[t(i,j)]_{n\times m}$ 来表示,称 $\boldsymbol{T}$ 为骑士巡游矩阵,其中 $t(i,j)$ 的值表示骑士第 $t(i,j)$ 步巡游到 i 行 j 列:

$$\boldsymbol{T}=\begin{bmatrix} 56 & 41 & 58 & 35 & 50 & 39 & 60 & 33 \\ 47 & 44 & 55 & 40 & 59 & 34 & 51 & 38 \\ 42 & 57 & 46 & 49 & 36 & 53 & 32 & 61 \\ 45 & 48 & 43 & 54 & 31 & 62 & 37 & 52 \\ 20 & 5 & 30 & 63 & 22 & 11 & 16 & 13 \\ 29 & 64 & 21 & 4 & 17 & 14 & 25 & 10 \\ 6 & 19 & 2 & 27 & 8 & 23 & 12 & 15 \\ 1 & 28 & 7 & 18 & 3 & 26 & 9 & 24 \end{bmatrix}, \tag{3}$$

上式矩阵中1表示骑士巡游的起点.

用骑士巡游矩阵对图像进行置乱变换称为骑士巡游置乱,这相当于对图像进行秘钥保护,巡游矩阵的数量相当于加密的密钥量且随着矩阵维数的增长成指数级的增长[7-8]. 因此,用其作为加密密钥对图像进行加密处理,其安全性较高. 对于图像 $A=[a(i,j)]_{n\times m}$ 和骑士巡游阵阵 $\boldsymbol{T}=[t(i,j)]_{n\times m}$,假设用 $\boldsymbol{T}$ 置乱 A 得到 $B=[b(i,j)]_{n\times m}$,其步骤可描述为:

```
for i=1 to n
for j=1 to m
  do
    if t(i,j)= =1 then
      (1)从 T 中找到第 u 行第 v 列元素,使
          t(u,v)=n×m
      (2)b(i,j)=a(u,v)
    else
      (1)从 T 中找到第 u 行第 v 列元素,使
          t(u,v)=t(i,j)-1
      (2)b(i,j)=a(u,v)
    end
```

1.3　基于Arnold变换和骑士巡游变换相结合的复合置乱算法

由Arnold变换和骑士巡游变换可知,这两种变换具有互补性,所以可以结合两种算法的特点,使图像置乱简单易行且具有更高的安全性和保密性.具体步骤如下:

(1)图像方块分割,因为Arnold变换只能用于高和宽相同的图像,所以置乱之前对非正方形图像 $n\times m$ $(n\neq m)$ 要做补零或裁边处理,使其变成高和宽相同的图像.根据式(2)计算出Arnold变换的周期 m_N;

(2)将分割后的图像进行Arnold置乱,选择合适的迭代的次数直至图像充分置乱(达到“杂乱无章”的效果),记下置乱次数 n ;

(3)将经过步骤(2)充分置乱后的图像根据其大小分块,如图像的大小为256×256,可分成8×256、8×128等大小相同的块,然后产生同样大小的骑士巡游矩阵,本文采用8×8的方阵;

(4)取(3)中的矩阵之一对Arnold密图骑士巡游置乱一次;

(5)用Arnold算法将(4)中的密图置乱 $(m_N - n)\bmod m_N$ 次,若可以看出原图像的任何痕迹,就重复(4),每一次重复可选择不同的巡游路径;

(6)直到(5)中的密图Arnold恢复后,仍是一幅无法分辨的图像.

2 算法软件实现的改进

分析骑士巡游算法和Arnold算法的复杂度不难发现:骑士巡游算法的复杂度要远大于Arnold变换,由于骑士巡游算法在置乱每个像素时都需要不停查找巡游矩阵的行与列从而带来庞大的系统开销.对于 $n\times n$ 的图像块,查找一次巡游矩阵所需的复杂度为 $n^2/2$,而基于此本文改进了传统骑士巡游的实现方法,大大降低算法运行的复杂度.若巡游矩阵 $\boldsymbol{T}=\left[t(i,j)\right]_{8\times 8}$ 中元素值 $t(i,j)$ 的坐标为 (i,j) ,则矩阵 $\boldsymbol{T}$ 可转换成如下映射关系:如规定巡游矩阵 $\boldsymbol{T}$ 中元素值为56的坐标为(0,0),元素值为24的坐标为(7,7),建立平面坐标系,则表2中(2,1)表示矩阵 $\boldsymbol{T}$ 中元素值为56的点将要移动到新位置(元素值为57的位置)上的坐标,(2,0)表示矩阵 $\boldsymbol{T}$ 中元素值为41的点待搬移到新位置的坐标,…,以此类推,棋盘上任意一点的新坐标均可以从表2中获取.

表2 骑士巡游矩阵映射表

Table 2 The mapping table of Knight transform matrix

(2,1)	(2,0)	(1,4)	(2,4)	(1,6)	(1,3)	(2,7)	(1,5)
(3,1)	(3,0)	(0,0)	(0,1)	(0,6)	(0,3)	(3,7)	(0,5)
(3,2)	(0,2)	(1,0)	(0,4)	(3,6)	(3,3)	(0,7)	(3,5)
(2,2)	(2,3)	(1,1)	(1,2)	(2,6)	(4,3)	(1,7)	(2,5)
(5,2)	(6,0)	(3,4)	(5,1)	(6,5)	(6,6)	(5,4)	(5,5)
(4,2)	(7,0)	(4,4)	(4,1)	(7,3)	(6,7)	(7,5)	(4,5)
(7,2)	(4,0)	(7,4)	(7,1)	(7,6)	(7,7)	(4,7)	(4,6)
(6,2)	(5,0)	(6,4)	(6,1)	(5,3)	(6,3)	(5,7)	(5,6)

以8位色位图为例,在编写C程序时设置了一个8×8的二维数组,该数组中的元素表示与上表中对应位置上的点与原点(0,0)在8×8图象中的字节地址偏移量,例如坐标(2,1)表示与原点在8×8图象中的地址偏移量为2×8+1=17字节,于是我们可将上表转换成像素偏移矩阵 $\boldsymbol{M}$,此矩阵即为算法改进实现密钥矩阵,

$$\boldsymbol{M}=\begin{bmatrix}17 & 16 & 12 & 20 & 14 & 11 & 23 & 13\\ 25 & 24 & 0 & 1 & 6 & 3 & 31 & 5\\ 26 & 2 & 8 & 4 & 30 & 27 & 7 & 29\\ 18 & 19 & 9 & 10 & 22 & 35 & 15 & 21\\ 42 & 48 & 28 & 41 & 53 & 54 & 44 & 45\\ 34 & 56 & 36 & 33 & 59 & 55 & 61 & 37\\ 58 & 32 & 60 & 57 & 62 & 63 & 39 & 38\\ 50 & 40 & 52 & 49 & 43 & 51 & 47 & 46\end{bmatrix}. \tag{4}$$

调试状态下ARM7对一幅256×256像素的8位色灰度图采用查找骑士巡游矩阵加密30次的时间开销约为140秒,而采用 $\boldsymbol{M}$ 矩阵加密30次的时间开销仅为4 s左右,处理速度提升了30多倍.

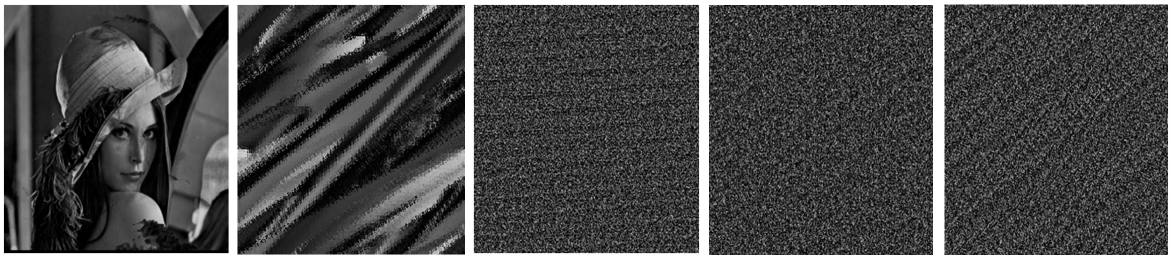
3 基于ARM7目标板的复合算法实验分析

本文所有实验均基于256×256像素8位色灰度图.

3.1 复合算法加密实验部分

对源图分别进行 m 次Arnold变换及 n 次骑士(Knight)巡游(简记为:m A+n K):1 A+1 K、8 A+2 K、30 A+2 K、50 A+10 K的结果依次如图1(a)~(d)所示.

实验结果表明:复合置乱算法具有很好置乱效果且计算量相对较少,是一种适合在嵌入式系统里实现的置乱方法.



源图　(a)　(b)　(c)　(d)

图1　复合置乱实验图

Fig.1　The results of composite encryption

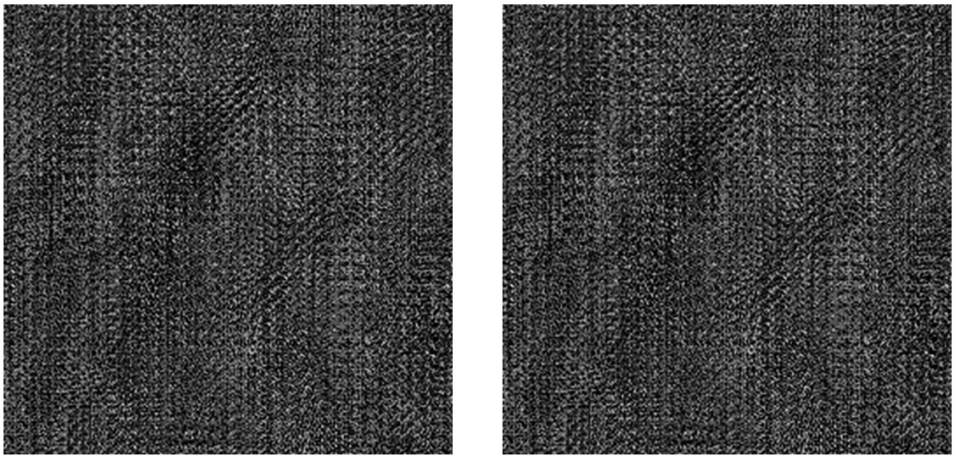
3.2　复合算法解密实验部分

对图1(b)进行2次骑士巡游及8次反Arnold变换(对于大小为256×256的图像相当于做192−8=184次Arnold变换).解密的结果与源图相同,表明经本设计置乱的图像具有可恢复性.

为检验设计的安全性和鲁棒性本文还做了下面4组实验,以下各实验均基于图1(b)的密图.

实验1:采用错误的骑士巡游矩阵对密图进行解密,结果如图2(a)所示;

实验2:采用错误的变换顺序进行恢复,结果如图2(b)所示;

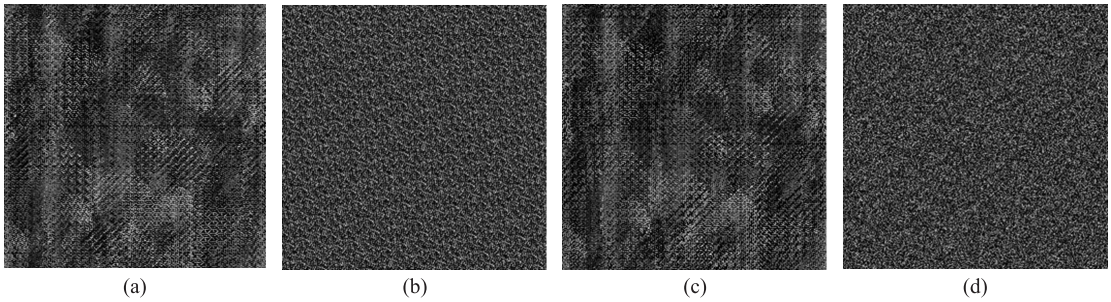


(a)　(b)

图2　实验1、实验2结果图

Fig.2　The result of experiment 1 and 2

实验3:采用错误的解密次数进行恶意猜测破解:对8 A+2 K密图分别进行1 K+184 A,2 K+100 A,3 K+184 A,5 K+50 A破解,结果依次如图3(a)~(d)所示.



(a)　(b)　(c)　(d)

图3　实验3结果图

Fig.3　The result of experiment 3

实验1~3表明,当且仅当解密的次序、解密的密钥、解密的迭带次数跟加密的过程完全吻合时才能破解成功.所以本设计具有很好的安全性.

实验4:抗剪切、抗噪声分析,对密图(图1(b))做右下角1/4剪切、随机破坏攻击、人为叠加噪声后反置乱的实验结果如图4(a)、(b)、(c)所示.

实验4表明,本设计具有抗噪声和抗攻击能力,具有一定的鲁棒性.

(a) 抗剪切攻击　(b)抗随机破坏攻击　(c)抗噪声污染

图4　实验4结果图

Fig.4　The result of experiment 4

4　结语

本文是基于ARM7平台通过软件的方式实现数字视频加解密功能,因ARM7的处理能力有限,在处理数字视频信号时显得有些力不从心,要做到每秒25帧以上的高分辨率视频信号的速度还要进一步努力,这个问题可以从进一步优化加解密算法的角度去考虑或寻求处理速度更快的内核.

[参考文献](References)

[1] 邹建成,铁小匀. 数字图像的二维Arnold变换及其周期性[J]. 北方工业大学学报,2000,12(1):10-14.
Zhou Jiancheng, Tie Xiaojun. Arnold transformation of digital image with two dimensions and its periodicity[J]. Journal of North China University of Technology,2000,12(1):10-14.(in Chinese)

[2] 柏森. 基于信息隐藏的隐蔽通信技术研究[D]. 重庆:重庆大学自动化学院,2002.
Bai Sen. A reaserch of encrypted communication based on information hidden technology[D]. Chongqing: School of Automation,Chongqing University,2002.(in Chinese)

[3] 王丽娜. 网络多媒体信息安全保密技术[M]. 武汉:武汉大学出版社,2003.
Wang Lina. Information Hidden Technology of Multimedia from Computer Network[M]. Wuhan: Wuhan University Press, 2003.(in Chinese)

[4] 丁玮,闫伟齐,齐东旭,等. 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学报,2001,13(4):338-341.
Ding Wei, Yan Weiqi, Qi Dongxu, et al. Digital image encryption technology based on Arnold transform[J]. Journal of Computer Aided Design and Photography,2001,13(4):338-341.(in Chinese)

[5] 齐东旭. 分形及其计算机生成[M]. 北京:科学出版社,1994.
Qi Dongxu. Division of Photograph and Computer Aided Generation[M]. Beijing:Science Press,1994.(in Chinese)

[6] 雷仲魁,孙秋燕,宁宣熙. 马步哈密顿圈(骑士巡游)在图像置乱加密方法上的应用[J]. 小型微型计算机系统,2010(5):984-989.
Lei Zhongkui, Sun Qiuyan, Ning Xuanxi. Image scrambling algorithms based on knight-tour transform and its applications [J]. Journal of Chinese Computer Systems,2010(5):984-989.(in Chinese)

[7] 柏森,曹长修,曹龙汉,等. 基于骑士巡游变换的数字图像细节隐藏技术[J]. 中国图象图形学报,2001,6(11,A):1 096-1 100.
Bai Sen, Cao Changxiu, Cao Longhan, et al. Digital image details hiding technology based on knight-tour transformation[J]. Journal of Image and Graphics,2001,6(11,A):1 096-1 100.(in Chinese)

[8] Parberry I. An efficient algorithm for the Knight's Tour Problem[J]. Discrete Applied Mathematecs,1997(73):251-260.

[责任编辑:陈　庆]