JOURNAL OF IMAGE AND GRAPHICS

主办：中国科学院遥感与数字地球研究所
中国图象图形学学会
北京应用物理与计算数学研究所

中国图象图形学报

2013
12
VOL.18

ISSN1006-8961
CN11-3758/TB

图像分割 P1610

中国图象图形学报

刊名题字：宋健 | 月刊（1996年创刊）

第18卷第12期（总第212期）
2013年12月16日

中国精品科技期刊
中国国际影响力优秀学术期刊
中国科技核心期刊

主管单位 中国科学院
主办单位 中国科学院遥感与数字地球研究所
中国图象图形学学会
北京应用物理与计算数学研究所

主　　编 李小文
编辑出版 《中国图象图形学报》编辑出版委员会
邮政信箱 北京9718信箱
邮　　编 100101
电子信箱 jig@irsa.ac.cn
电　　话 010-64807995
网　　址 www.cjig.cn

广告经营许可证 京朝工商广字第0361号
总 发 行 北京报刊发行局
订　　购 全国各地邮局
海外发行 中国国际图书贸易集团有限公司
（邮政信箱：北京399信箱　邮编：100048）
印刷装订 北京科信印刷有限公司

Journal of Image and Graphics
Title inscription: Song Jian | Monthly, Started in 1996

Superintended by Chinese Academy of Sciences
Sponsored by Institute of Remote Sensing and Digital Earth, CAS
China Society of Image and Graphics
Institute of Applied Physics and Computational Mathematics

Editor-in-Chief LI Xiaowen
Editor, Publisher Editorial and Publishing Board of Journal of Image and Graphics
P.O.Box 9718, Beijing, P.R.China
Zip code 100101
E-mail jig@irsa.ac.cn
Telephone 010-64807995
Website www.cjig.cn

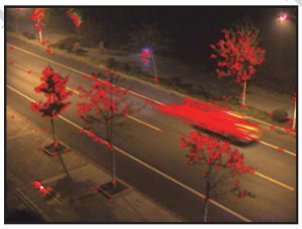
Distributed by Beijing Bureau for Distribution of Newspapers and Journals
Domestic All Local Post Offices in China
Overseas China International Book Trading Corporation
(P.O.Box 399, Beijing 100048,P.R.China))
Printed by Beijing Kexin Printing Co., Ltd.

CN 11-3758/TB
ISSN 1006-8961
CODEN ZTTXFZ

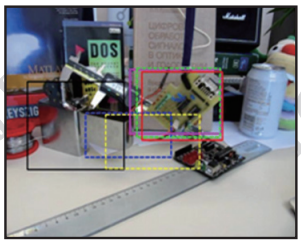
国外发行代号 M1406
国内邮发代号 82-831
国内定价 50.00元

2013年12月 第18卷 第12期（总第212期）
中国图象图形学报 Zhongguo Tuxiang Tuxing Xuebao

目次



稀疏光流快速计算的动态目标检测与跟踪(第1593页)

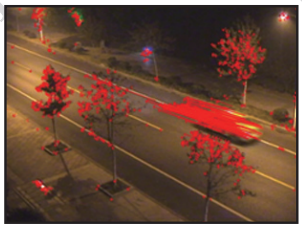


字典学习联合粒子滤波鲁棒跟踪(第1628页)

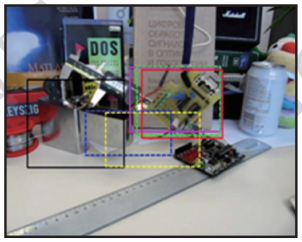
结合SURF特征的多功能彩色图像水印算法(第1694页)

Volume 18, Number 12
Published December 16, 2013

CONTENTS
JOURNAL OF IMAGE AND GRAPHICS



Dynamic target detection and tracking based on fast computation using sparse optical flow (P1593)



Object tracking based on learning a dictionary joint practical filter(P1628)

Multi-purpose watermark algorithm of color images based on SURF(P1694)

E-mail: jig@irsa.ac.cn
Website: www.cjig.cn
Tel: 010-64807995

中国图象图形学报
JOURNAL OF IMAGE AND GRAPHICS

中图法分类号：TP37　　**文献标识码**：A　　**文章编号**：1006-8961(2013)12-1567-07
论文引用格式：金建国，王乐，魏明军，苏晶晶．混沌密钥调制 DFRFT 旋转因子的视频加密[J]．中国图象图形学报，2013，18(12)：1567-1573.
[DOI：10.11834/jig.20131203]

混沌密钥调制 DFRFT 旋转因子的视频加密

金建国[1,2]，王乐[2]，魏明军[2]，苏晶晶[2]
1. 河北联合大学理学院，唐山　063009；2. 河北联合大学信息工程学院，唐山　063009

摘　要：现有分数阶傅里叶变换(FRFT)由于旋转因子的单一性很少应用于视频实时加密，而当前单纯混沌加密算法的安全性又存在着诸多缺陷。为此，提出一种新的视频实时加密算法——混沌密钥调制 DFRFT 旋转因子。该算法将混沌加密与分数阶傅里叶变换进行了有机结合。首先将离散分数阶傅里叶变换(DFRFT)的旋转因子用混沌密钥进行调制，然后用调制后的旋转因子对视频数据进行分数阶傅里叶变换，最终完成了对视频数据的加密系统。该加密系统在技术上实现了视频数据在客户端的实时采集、实时加密；密文在网络上的实时传输、密文在接收端的接收、实时解密和播放。实验结果表明，加、解密效果很好，满足了实时性与安全性的要求。对实验结果的理论、安全性分析表明，该算法简单易行、安全性高。该算法的安全性优于单纯的混沌加密算法或单纯傅里叶视频加密算法，且满足了实时性要求。为解决实时性与安全性冲突问题提供了一条新的途径。
关键词：视频数据；混沌密钥；分数阶傅里叶变换；旋转因子；实时传输

Video encryption based on chaotic key modulating DFRFT rotation factor

Jin Jianguo[1,2]，Wang Le[2]，Wei Mingjun[2]，Su Jingjing[2]
1. *College of Science*，*Hebei United University*，*Tangshan*　063009，*China*；
2. *College of Information Engineering*，*Hebei United University*，*Tangshan*　063009，*China*

Abstract：Because of the singleness of the rotation factor，fractional Fourier transform (FRFT) is rarely used in real-time video encryption. While at present，the simple chaotic encryption algorithms have many security problems. Consequently，a new real-time video encryption algorithm-chaotic key modulating discrete fractional Fourier transform (DFRFT) rotation factor is proposed. This algorithm combines chaotic encryption with DFRFT. First，we modulate the DFRFT rotation factor by a chaotic key. Second，we use the modulated rotation factor to carry on fractional Fourier transform，so as to complete the encryption operation for video data. The encryption system realizes real-time acquisition，real-time encryption and transmission，as well as real-time reception，real-time decryption and playing at the receiving terminal. The experimental results show that the system has a good effect in the encryption and decryption and can meet our real-time and security requirements. The theoretical analysis on the experiment results indicate that this algorithm is simple and practicable，with a high-level of security. The security of the algorithm is better than simple chaotic encryption algorithm or the simple FRFT encryption algorithm. We can draw a conclusion from results that this algorithm provides a novel mechanism for resolving the dispute between real-time and security.
Key words：video data；chaotic key；fractional Fourier transform；rotation factor；real-time transmission

收稿日期：2012-11-08；**修回日期**：2013-05-27
第一作者简介：金建国(1956—　)，男，教授，硕士研究生导师，主要研究方向为信息安全与混沌加密技术。E-mail：jjg1956@126.com

中国图象图形学报
JOURNAL OF IMAGE AND GRAPHICS
Vol. 18, No. 12, Dec. 2013

0 引 言

随着 Internet 的快速发展,视频数据传输的保密性问题日益严重。目前单纯的混沌序列加密已可用空间重构法和穷举法进行破译,甚至混沌伪随机序列加密算法也是不安全的,且目前一些类型的混沌加密算法存在着对微小的变化不够敏感和不能抵御明文攻击等安全性缺陷[1-5]。分数阶傅里叶变换(FRFT)作为一种崭新的时频分析工具和旋转算子为信号处理领域的研究人员所广泛接受,但多数应用在图像加密和语音加密等领域[6-9],很少应用于视频实时加密传输领域。且单纯的分数阶傅里叶加密存在密钥空间小、密钥的敏感性差和单一旋转因子容易破解等缺点。

针对加密领域出现的上述问题,将混沌理论和分数阶傅里叶变换二者相结合应用到视频实时加密领域中。通过混沌序列产生加密密钥,应用该密钥来调制分数阶傅里叶变换的旋转因子实现对视频数据的实时加密处理。

1 理论分析

1.1 离散分数阶傅里叶变换

为方便加解密变换,采用 Pei 等人提出的基于正交投影的特征分解型离散分数阶傅里叶变换(DFRFT)[10]方法。特征分解型 DFRFT 是目前为止唯一严格意义上的 DFRFT 定义,它和连续分数阶傅里叶变换非常接近,同时还满足旋转相加性。用同一子程序即可完成旋转相加性的正、逆变换,这就使得用计算机编程完成加解密变换极为方便和简单。

DFRFT 的核矩阵为

$$\boldsymbol{F}^{2\alpha/p} = \boldsymbol{U}\boldsymbol{D}^{2\alpha/p}\boldsymbol{U}^{\mathrm{T}} = \begin{cases} \sum_{k=0}^{N-1} \mathrm{e}^{jk\alpha}\boldsymbol{u}_k\boldsymbol{u}_k^{\mathrm{T}} & N\text{ 为偶数} \\ \sum_{k=0}^{N-2} \mathrm{e}^{jk\alpha}\boldsymbol{u}_k\boldsymbol{u}_k^{\mathrm{T}} + \mathrm{e}^{jk\alpha}\boldsymbol{u}_N\boldsymbol{u}_N^{\mathrm{T}} & N\text{ 为奇数} \end{cases} \tag{1}$$

式中,$\boldsymbol{U}$ 为 Hermite 特征向量矩阵,当 N 为奇数时为 $\boldsymbol{U}=[\boldsymbol{u}_0\ \boldsymbol{u}_1\cdots\boldsymbol{u}_{N-1}]$,当 N 为偶数时为 $\boldsymbol{U}=[\boldsymbol{u}_0\ \boldsymbol{u}_1\cdots\boldsymbol{u}_{N-2}\ \boldsymbol{u}_N]$,$\boldsymbol{u}_k$ 是经正交化得到的归一化的 Hermite 特征向量[11]。$\boldsymbol{D}^{2\alpha/\pi}$是对角阵,定义为

当 N 为奇数

$$\boldsymbol{D}^{2\alpha/\pi} = \begin{bmatrix} \mathrm{e}^{-j0} & 0 & 0 & \cdots & 0 \\ 0 & \mathrm{e}^{-j\alpha} & 0 & \cdots & 0 \\ 0 & 0 & \mathrm{e}^{-j2\alpha} & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \mathrm{e}^{-j\alpha(N-1)} \end{bmatrix} \tag{2}$$

当 N 为偶数

$$\boldsymbol{D}^{2\alpha/\pi} = \begin{bmatrix} \mathrm{e}^{-j0} & 0 & 0 & \cdots & 0 \\ 0 & \mathrm{e}^{-j\alpha} & 0 & \cdots & 0 \\ 0 & 0 & \mathrm{e}^{-j2\alpha} & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \mathrm{e}^{-j\alpha N} \end{bmatrix} \tag{3}$$

当变换核 $\boldsymbol{F}^{2\alpha/\pi}$确定后,信号 $i(t)$ 的 DFRFT 的正变换为

$$\boldsymbol{I}_\alpha = \boldsymbol{F}^{2\alpha/\pi}\boldsymbol{I} = \boldsymbol{U}\boldsymbol{D}^{2\alpha/\pi}\boldsymbol{U}^{\mathrm{T}}\boldsymbol{I} \tag{4}$$

逆变换为

$$\boldsymbol{I} = \boldsymbol{F}^{-2\alpha/\pi}\boldsymbol{I}_\alpha = \boldsymbol{U}\boldsymbol{D}^{-2\alpha/\pi}\boldsymbol{U}^{\mathrm{T}}\boldsymbol{I}_\alpha \tag{5}$$

式中,$\boldsymbol{I}$ 表示信号 $i(t)$ 的离散样本向量,$\boldsymbol{I}=[i_1, i_2,\cdots,i_N]^{\mathrm{T}}$;$\boldsymbol{I}_\alpha$ 表示 $\boldsymbol{I}$ 经分数阶傅里叶变换后所得分数阶域的离散向量。

1.2 混沌序列的应用

采用的混沌模型为 Logistic 模型,其表达式为

$$x_{n+1} = f(\mu, x_n) = 1 - \mu x_n^2 \tag{6}$$

式中,$x_n \in [-1,1]$,$\mu \in [1.81,2]$。

此混沌模型在本文中有两个作用:1)调制分数阶傅里叶变换的旋转因子;2)对原始视频数据进行预加密。

2 加密算法描述

2.1 加密系统总体模型

如图 1 所示,加密系统发送端通过摄像头采集到原始视频流数据,通过 A/D 转换为发送端的视频流离散样本 y_n,混沌加密系统 M 产生调制 DFRFT 旋转因子所需的混沌序列 x_n,$C(k)$为经过混沌密钥调制 DFRFT 旋转因子加密后的密文数据包;$C'(k)$为通过 INTERNET 传输后的密文数据包,x'_n为混沌解密系统 M'产生的解密所需的混沌序列,y'_n为解密后的视频流数据包。当发送端混沌系统 M 与接收端混沌系统 M'同步时,通过分数阶傅里叶反变换则可实现 $y'_n = y_n$。即加密的视频信号可以恢复。其中,离散分数阶傅里叶变换模块需要

传入两个参数:一个是时域视频信号的离散样本 y_n,另一个是混沌序列 x_n。因此,离散分数阶傅里叶变换的数学表达式可表示成 DFRFT(x_n, y_n)形式。

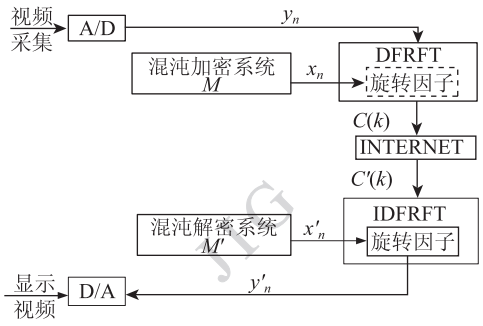


图 1　视频实时加密系统模型

Fig. 1　System model of video real-time encryption

2.2　加密算法实现过程

1)通过摄像头采集到原始视频流数据 y_n,确定 Logistic 混沌系统参数 u(u =2),以及系统初值 x,通过式(7)得到调制 DFRFT 旋转因子所需混沌密钥 x_n,即

$$x_n = 1 - \mu x_{n-1}^2 \tag{7}$$

2)利用混沌对傅里叶变换旋转因子进行调制,将式(7)产生的混沌密钥 x_n 乘以 π 替换式(1)中的旋转因子 α,即

$$\alpha = \pi x_n \tag{8}$$

然后,将 N 个离散视频样点的向量 $\boldsymbol{I}$,连同式(7)一起代入式(4),得发送端 DFRFT 加密方程,此时就完成了发送端混沌密钥调制 DFRFT 旋转因子 α,C_α 为密文序列的向量,即

$$\boldsymbol{C}_\alpha = \boldsymbol{F}^{2\alpha/\pi}\boldsymbol{I} = \boldsymbol{F}^{2x_n}\boldsymbol{I} = \boldsymbol{U}\boldsymbol{D}^{2x_n}\boldsymbol{U}^{\mathrm{T}}\boldsymbol{I} \tag{9}$$

3)将加密后的视频流数据也即密文数据 $\{c_n(k)\}$ 和驱动量 x_n(混沌序列产生的密钥)打包成 $\boldsymbol{M}(k) = \{x_n, \{c_n(k)\}\}$,通过网络进行发送。

4)接收端接收网络传输过来数据包 $\boldsymbol{M}'(k)$ 后,根据表达式(5),进行解密,即 IDFRFT,得

$$\boldsymbol{I} = \boldsymbol{F}^{-2\alpha/\pi}\boldsymbol{C}_\alpha = \boldsymbol{F}^{-2x_n}\boldsymbol{C}_\alpha = \boldsymbol{U}\boldsymbol{D}^{-2x_n}\boldsymbol{U}^{\mathrm{T}}\boldsymbol{C}_\alpha \tag{10}$$

5)重复上述操作,直到视频采集结束,从而完成了视频数据的实时加密传输,详细流程如图 2 所示。需要说明的是:为确保混沌子系统的安全性,式(8)中的 x_n 是式(7)经过若干次预迭代得到。即对收、发双方混沌系统均进行同样次数的预迭代。受篇幅限制,详情从略。

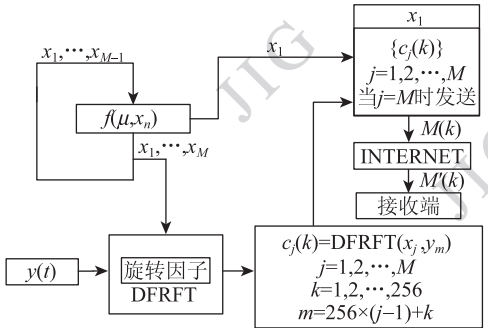


图 2　发送端加密模型

Fig. 2　Encryption model of sending terminal

3　加密系统的实现及加密效果

3.1　加密系统发送端和接收端实现

系统在 Microsoft Visual C + + 6.0 平台上使用 Windows 专门提供的 Video for Windows(VFW)软件包来对视频数据的采集与播放,采用 TCP 协议,使用 Winsocket 网络编程接口实现视频的实时传输,传输过程采用客户机/服务器模式。发送端如图 3 所示,在进行视频采集前,首先需要对视频设备及网络端口进行初始化。当缓冲区满时调用回调函数 CapSetCallbackOnVideoStream,采集视频数据,将视频数据存入视频缓冲区,从而调用函数 SendVideoData 对视频缓冲区中数据进行混沌密钥调制的分数阶傅里叶变换加密,将加密数据通过网络接口发送出去。数据发送结束后继续进行视频采集。从而在客户端完成了对视频数据的采集、加密和传输。

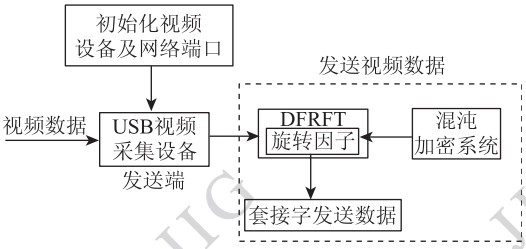


图 3　发送端程序运行过程

Fig. 3　Running process of the sender program

接收端如图 4 所示,当视频设备打开成功,接受发送端发来的视频通话请求,将接收到的加密视频数据存入视频缓冲区,调用函数 DisPlayVideoData 对视频数据进行混沌密钥调制的分数阶傅里叶逆变换,将解密数据放入播放缓冲区,进行播放,从而实现了在客户端接收、解密和播放视频数据。为了实

中国图象图形学报
JOURNAL OF IMAGE AND GRAPHICS
Vol. 18, No. 12, Dec. 2013

现双工,客户/服务器两端各设两个 Socket,分别用于接收和发送数据。

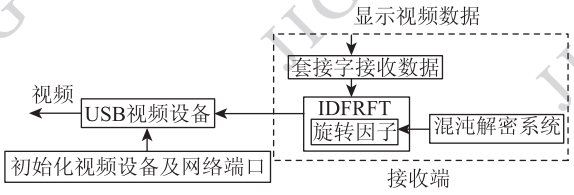
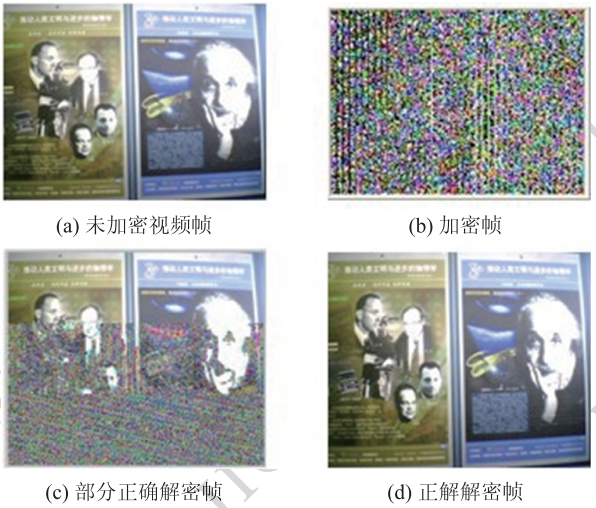


图 4　接收端程序运行过程

Fig. 4　Running process of the receiver program

3.2　加解密系统实现效果

通过摄像头采集到的视频流每帧大小 N = 38 400B,因为采集到的视频数据 30 帧/s,为防止视频加密数据过大而影响实时传输,系统采用一块一密的加密算法,每块数据 315 B,那么每帧需要的混沌密钥数为 38 400/320 = 120。通过单帧的提取,得到了图 5 所示的实验结果。其中图 5(b)为混沌密钥初值 x = 1.256 的密文帧,可以看到加密效果非常好,完全看不出原始帧的内容;图 5(c)为将 x = 1.256 调整到 x = 1.256 000 000 1 时的解密视频帧,可以看到部分解密成功;图 5(d)为解密混沌密钥初值也为 x = 1.256 时的正确解密帧,可见图 5(d)和原始明文帧图 5(a)吻合度很好,解密非常成功。



(a) 未加密视频帧　(b) 加密帧

(c) 部分正确解密帧　(d) 正解解密帧

图 5　实验结果图

Fig. 5　The results of encryption system

由图 5(c)可以看出,当接收端和发送端的系统初值密钥有微小差异时($\Delta x \geqslant 1.256\ 000\ 000\ 1 - 1.256\ 000\ 000\ 0 = 10^{-10}$),且当由此微小差异引起的混沌密钥迭代积累误差 $\Delta x' > 10^{-3}$,会导致在 N > 25 600部分以后的解码完全失败;而在 12 800 < N < 25 600部分只解密出一部分,可以看到图像大致轮廓;最后在 N < 12 800 部分,由于混沌迭代累计误差 $\Delta x \leqslant 10^{-3}$,因此解密成功。

如果对视频细心观察时,平均 250 ～300 s 内,偶见花屏闪烁一次。若不太注意时几乎察觉不到。其原因是由于部分个别数据丢失或错误而引起的解密错误。但由于采集到 30 帧/s 的数据,上述解密错误的视频帧并不影响整体视觉效果,因此对这些帧并没有做特殊处理。另外,由于本文算法采用每个数据包携带一个初始密钥,因此,在传输数据部分丢失的情况下系统密钥也无需重新同步,即每数据包一个初始密钥,系统具有自同步功能。

4　加密系统安全性和加密预处理分析

4.1　密钥空间容量和系统参量容量分析

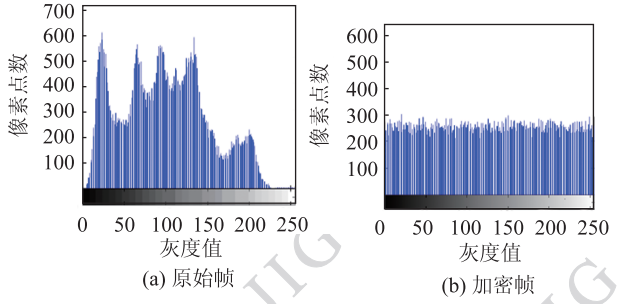
本文算法是基于 double 型变量进行运算的,密钥 $x_n \in [-1,1]$,而密钥容量的量级为 10^{16},即找到密钥 x_n 的概率为 $P_1 = 10^{-16}$,从而确保了一块(315 个数据)一密的原则,所以密钥是安全的。

为了确保 Logistic 方程处于混沌态和避开周期 3 窗口等缺陷,μ 值有效取值范围为[1.81,2],即 $\Delta\mu \approx 0.2$。由此得系统参量容量(量级)$N_\mu = 10^{15}$,即找到系统参量 μ 的概率 $P_2 = 1/N_\mu = 10^{-15}$,其概率很小,系统参量也是安全的。

4.2　抵抗统计攻击分析

4.2.1　直方图分析

图 6(a)(b)分别为视频流原始帧图 5(a)的灰度直方图和图 5(b)加密帧的灰度直方图。通过对比可发现,加密后的灰度直方图像素点分布非常均匀,完全改变原图像的统计特性,可以有效地抵抗统计攻击。



(a) 原始帧　(b) 加密帧

图 6　直方图分析

Fig. 6　The analysis of histogram

4.2.2　相邻像素的相关性分析

相邻像素相关性可以反映图像扩散程度，通常每帧视频图像的相邻像素间都具有较强的相关性，相关性越大，图像的扩散程度越不好；反之相关性越小，扩散程度越好，说明算法加密效果越好。本文对原始帧图 5(a) 和加密帧图 5(b) 相邻像素的水平、垂直和对角线分别进行相关性测试。相关系数 r_{xy}[12] 的计算公式为

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{11}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{12}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i \tag{13}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{14}$$

式中，x 和 y 代表图像中两个相邻像素点的灰度值。图 7 表示原始帧图 5(a) 和加密帧图 5(b) 垂直方向的相邻像素的相关分布情况。

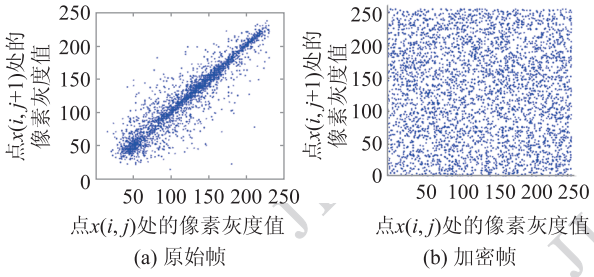


图 7　视频帧加密前后相邻像素垂直方向相关性

Fig. 7　The vertical pixel correlation of the video frame brfore and after encryption

表 1 列出了视频帧图 5(a) 和图 5(b) 水平、垂直和对角线方向的相关系数。从表 1 可看出，未加密帧相邻像素间相关系数非常接近 1，相关系数较大，是高度相关的；加密后视频帧相邻像素间的相关系数非常接近 0，相关系数比较小，相关性在极大程度上被破坏，相邻像素已基本不相关。这表明本文算法有效掩盖了明文的统计特性，具有较好的抵抗统计分析的能力。

4.3　旋转因子 α 敏感性分析

为了证明加密系统对 DFRFT 旋转因子 α 的敏感性，去掉系统中的混沌模块，只采用单一旋转因子作为加密密钥对图 5(a) 的明文进行加解密变换。

表 1　视频帧明文和密文相邻像素间的相关系数

Table 1　The adjacent pixels correlation of the video frame before and after encryption

	加密前	加密后
水平方向	0.995 4	0.042 6
垂直方向	0.984 4	0.040 1
对角线方向	0.984 7	0.008 1

经过实际测试，当采用单一旋转因子 $\alpha = 1.325$ 作为加密密钥，对图 5(a) 所示 1 帧视频图像进行分数阶傅里叶正变换(加密处理)，可以得到图 8(a) 所示分数阶傅里叶域加密后的图像。然后对图 8(a) 所示密文进行分数阶傅里叶逆变换(解密处理)，但是解密密钥不采用 $\alpha = 1.325$，而采用 $\alpha = 1.326$，得到解密后视频图像如图 8(b) 所示，不难看出解密失败了。如果用 $\Delta\alpha$ 来表示加密密钥和解密密钥的差，那么分数阶傅里叶变换当 $\Delta\alpha \geqslant 10^{-3}$ 时，解密将彻底失败。

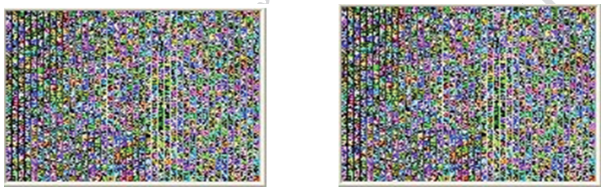


图 8　$\Delta\alpha = 10^{-3}$ 时敏感性测试

Fig. 8　Rotation factor sensitivity test of 10^{-3}

当采用单一旋转因子 $\alpha = 1.325\ 1$ 作为加密密钥，对图 5(a) 所示 1 帧视频图像进行分数阶傅里叶正变换(加密处理)，得到图 9(a) 所示分数阶傅里叶域密文图像。然后采用 $\alpha = 1.325\ 2$ 作为旋转因子(解密密钥)，对图 9(a) 所示密文进行分数阶傅里叶逆变换(解密处理)，得到图 9(b) 所示解密后时域视频图像。通过图 5(a) 所示原始视频图像和图 9(b) 所示解密后单帧视频图像的对比可以发现，两者

图 9　$\Delta\alpha = 10^{-4}$ 时敏感性测试

Fig. 9　Rotation factor sensitivity test of 10^{-4}

中国图象图形学报
JOURNAL OF IMAGE AND GRAPHICS
Vol. 18, No. 12, Dec. 2013

图像已经基本一致。通过以上实际测试可以发现,分数阶傅里叶变换旋转因子的灵敏度 $\Delta\alpha \geqslant 10^{-3}$。

4.4 不同局域网下测试结果

提出的视频实时传输是建立在100 M的局域网上的,分别在100 M的局域网、54 M无线局域网和10 M局域网中对系统的实时性进行了测试。测试方法为:让测试者在发送端镜头前以不同速度进行移动,让观察者在接收端观察视频的显示。对观察到的数据汇总,得出统计结果。测试结果如表2所示。

表2 不同局域网下测试结果

Table 2 The results of different local area network

	剧烈运动	正常运动	缓慢运动
100 M 局域网	图像清晰,流畅	图像清晰,流畅	图像清晰,流畅
54 M 无线局域网	偶尔出现停顿,丢帧率1%左右	图像清晰,人眼感觉流畅	图像清晰,流畅
10 M 局域网	偶尔出现停顿,丢帧率2%左右	图像清晰,人眼感觉流畅	图像清晰,流畅

4.5 加密预处理

为了进一步加强系统的安全性,防止攻击者采用穷举法破译密文,在对原始视频流数据 $y(t)$ 进行混沌调制分数阶傅里叶变换旋转因子加密之前,先对 $y(t)$ 进行一次混沌加密。利用式(6)混沌系统产生混沌序列 x'_n,x'_n也即预加密密钥,用 x'_n与 y_n 相乘,即

$$j_n = x'_n \times y_n \tag{15}$$

从而得到预加密处理后的离散样本 j_n,令 $\boldsymbol{J}$ 为元素 j_n 的向量,以 $\boldsymbol{J}$ 代替式(9)中的 $\boldsymbol{I}$,得

$$\boldsymbol{C}'_{\alpha} = \boldsymbol{F}^{2\alpha/\pi}\boldsymbol{J} = \boldsymbol{F}^{2x_n}\boldsymbol{J} = \boldsymbol{U}\boldsymbol{D}^{2x_n}\boldsymbol{U}^{\mathrm{T}}\boldsymbol{J} \tag{16}$$

式中,$\boldsymbol{C}'_{\alpha}$为经过加密预处理后,再经过变换域加密得到的密文序列。由此可以完成变换域加密。图10是对图5(a)所示单帧视频图像经过加密预处理后得到的图像。

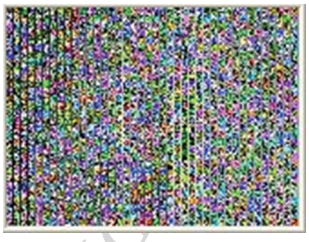


图10 加密预处理后图像

Fig. 10 The video frame of pretreatment encryption

视频流数据先经过加密预处理,然后再进行混沌调制分数阶傅里叶变换旋转因子的变换域加密,即对原始视频流数据进行了两次加密。在加入了加密预处理的情况下,即使攻击者利用穷举法正确解密经变换域加密的密文,但是由于视频数据先经过了加密预处理,这就使得攻击者无法在主观上判断对混沌调制DFRFT旋转因子部分的解密正确性。从而使系统安全,加密更有效。

5 结 论

针对视频实时保密通信提出了一种新的加密方案——混沌密钥调制傅里叶变换旋转因子,完成了对实时视频流的加密传输,实现了边采集,边加密,边传输,边播放。实验结果表明,该系统加密速度快,能满足实时传输的要求,对密钥非常敏感,具有很大的密钥空间,对各种攻击具有较强的抵抗性,优于单纯混沌加密或单纯傅里叶变换的视频加密算法。

参考文献(References)

[1] Zhang Y P, Zuo F, Zhai Z J. Survey on image encryption based on chaos[J]. Computer Engineering and Design, 2011, 32(2): 463-466. [张云鹏,左飞,翟正军. 基于混沌的数字图像加密综述[J]. 计算机工程与设计, 2011,32(2):463-466.]

[2] Wen C C, Wang Q, Miao X N, et al. Digital image encryption: a survey[J]. Computer Science, 2012, 39(12): 6-9. [文昌辞,王沁,苗晓宁,等. 数字图像加密综述[J]. 计算机科学, 2012, 39(12):6-9.]

[3] Li X J, Peng J H, Xu N, et al. Image encryption algorithm based on 2D hyperchaotic sequences[J]. Journal of Image and Graphics, 2003, 8(10): 1172-1777. [李雄军,彭建华,徐宁,等. 基于二维超混沌序列的图象加密算法[J]. 中国图象图形学报. 2003, 8(10): 1172-1777.]

[4] Wang Y, Wong K, Liao X F, et al. A new chaos-based fast image encryption algorithm[J]. Applied Soft Computing, 2011, 11(1): 514-522.

[5] Sun K H, He S B, He Y, et al. Complexity analysis of chaotic

pseudo-random sequences based on spectral entropy algorithm [J]. Acta Physica Sinica, 2012,11(62):1-8. [孙克辉,贺少波,何毅,等. 混沌伪随机序列的谱熵复杂性分析[J]. 物理学报,2012,11(62):1-8.]

[6] Ahmet S, Lutfiye D. The discrete fractional Fourier transform based on the DFT matrix[J]. Signal Processing,2011,33(91):571-578.

[7] Zhang H Y,Zhang W,Liu J M,et al. Fraction duffing system using in image encryption[J]. Computer Engineering & Sciennce, 2012,34(6):18-22. [张海英,张卫,刘金梅,等. 分数阶 Duffing 系统在图像加密中的应用[J]. 计算机工程与科学, 2012,34(6):18-22.]

[8] Jin J G,Lin R,Zhang Q L,et al. Real-time encryption system for audio frequency domain based on cascaded chaos[J]. Computer Engineering,2009,35(11):137-139. [金建国,林瑞,张庆凌,等. 基于混沌级联的语音频域实时加密系统[J]. 计算机工程,2009,35(11):137-139.]

[9] Nishchal N K,Joseph J,Singh K. Securing information using fractional Fourier transform in digital holography[J]. Optics Communications,2004,235(4-6):253-259.

[10] Pei S C, Yeh M H, Tseng C C. Discrete fractional fourier transform based on orthogonal projections [J]. IEEE Transactions on Signal Processing,1999,47(5):1335-1348.

[11] Jin J G,Chen C,Wei M J,et al. Audio encryption based on chaotic modulation DFRFT rotation factor[J]. Computer Engineering,2012,6(12):95-98. [金建国,陈晨,魏明军,等. 基于混沌调制 DFRFT 旋转因子的语音加密[J]. 计算机工程,2012,6(12):95-98.]

[12] Kwok H S,Tang W K S. A fast image encryption system based on chaotic maps with finite precision representation[J]. Chaos, Solitons and Fractals,2007,32(4):1518-1529.