计算机科学
COMPUTER SCIENCE

基于混沌YOLO v4的共享图像选择性加密方法

张国梅, 马琳娟, 张福泉, 李庆珍

引用本文

张国梅, 马琳娟, 张福泉, 李庆珍.基于混沌YOLO v4的共享图像选择性加密方法[J]. 计算机科学, 2022, 49(12): 368-373.

ZHANG Guo-mei MA Lin-juan, ZHANG Fu-quan, LI Qing-zhen. Selective Shared Image Encryption Method Based on Chaotic System and YOLO v4 [J]. Computer Science, 2022, 49(12): 368-373.

相似文章推荐（请使用火狐或 IE 浏览器查看文章）

Similar articles recommended (Please use Firefox or IE to view the article)

基于优化YOLO-V4的交通标志检测识别方法

Traffic Sign Detection and Recognition Method Based on Optimized YOLO-V4

计算机科学, 2022, 49(11): 179-184. https://doi.org/10.11896/jsjkx.220300251

基于双重二维混沌映射的压缩图像加密方案

Compressed Image Encryption Scheme Based on Dual Two Dimensional Chaotic Map

计算机科学, 2022, 49(8): 344-349. https://doi.org/10.11896/jsjkx.210700235

基于菌群优化的近邻传播聚类算法研究

Study on Affinity Propagation Clustering Algorithm Based on Bacterial Flora Optimization

计算机科学, 2022, 49(5): 165-169. https://doi.org/10.11896/jsjkx.210800218

一种基于Logistic-Sine-Cosine映射的彩色图像加密算法

Color Image Encryption Algorithm Based on Logistic-Sine-Cosine Mapping

计算机科学, 2022, 49(1): 353-358. https://doi.org/10.11896/jsjkx.201000041

基于改进YOLO v4的安全帽佩戴检测算法

Improved YOLO v4 Algorithm for Safety Helmet Wearing Detection

计算机科学, 2021, 48(11): 268-275. https://doi.org/10.11896/jsjkx.200900098

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220600139

基于混沌 YOLO v4 的共享图像选择性加密方法

张国梅[1]　马琳娟[2]　张福泉[2]　李庆珍[3]
1 广州理工学院计算机科学与工程学院　广州 510540
2 北京理工大学计算机学院　北京 100081
3 中国政法大学数据法治研究院　北京 102249

摘　要　针对社交平台共享图像的信息安全问题,提出了基于混沌 YOLO v4 和用户选择感兴趣区域(ROI)的图像加密方案。首先,利用 YOLO v4 自动检测图像中的目标,提供要加密的候选包围框;然后,利用 cosine 和 polynomial 映射的线性组合加密算法对用户选定的图像区域进行加密,使得只有合法授权用户才能访问共享图像的敏感信息。通过密钥发放和授权机制,实现对第三方转发图像中敏感信息的保护。实验统计和安全分析结果证明,所提方案能够抵御各种攻击,提供高度安全性,且处理速度能够满足在线用户的实时需求。

关键词:图像加密;共享图像;混沌映射;YOLO v4;感兴趣区域
中图法分类号　TP309;TP751

Selective Shared Image Encryption Method Based on Chaotic System and YOLO v4

ZHANG Guo-mei[1] MA Lin-juan[2],ZHANG Fu-quan[2] and LI Qing-zhen[3]
1 School of Computer Science and Engineering,Guangzhou Institute of Science and Technology,Guangzhou 510540,China
2 School of Computer Science & Technology,Beijing Institute of Technology,Beijing 100081,China
3 Institute of Data Rule of Law,China University of Political Science and Law,Beijing 102249,China

Abstract　Aiming at the information security problem of sharing images on social platforms,a selective region of interest(ROI) image encryption scheme based on YOLO v4 and hybrid chaotic map encryption is proposed. By utilizing YOLO v4,the uploaded image is automatically detected and the candidate bounding boxes to be encrypted are provided. Then the image areas selected by user are encrypted with the proposed hybrid encryption algorithm combining cosine and polynomial mapping,so that only legally authorized users can access the sensitive information of the shared image. Through the secret key issuing and authorization mechanism,the protection of sensitive information of the image forwarded by a third party is realized. Statistical and security analysis results prove that the proposed scheme can resist various attacks,and the processing speed can meet the real-time needs of online users.

Keywords　Image encryption,Shared image,Chaotic map,YOLO v4,Region of interest

1　引言

随着社交平台的兴起,互联网上产生了海量的媒体数据,增强了人与人之间的交互,但也带来了更多的安全性风险[1],特别是用户在社交平台上分享的图片中往往包含很多与个人生活相关的隐私信息,应该阻止未授权用户对此类信息的访问[2-3]。

密码系统和数据加密方法有助于保护共享数据的安全。混淆和扩散是安全密文的两个重要属性,例如 AES 等经典算法虽然满足该要求,但并不适用于图像加密领域[4-5]。混沌加密具有初值极端敏感性、非线性、长期不可预测性等优点,被广泛应用于图像加密中[6]。文献[7]提出的基于延迟耦合混沌模型的简单图像加密算法,利用一个映射的状态变量改变其他映射的控制参数,由此有效降低混沌映射的动态性衰减,并保留原始系统的相空间结构。文献[8]提出了基于云模型的混沌与矩阵卷积运算的图像加密算法,该算法利用混沌序列值实现像素值置换,并通过斐波纳契混沌序列与相邻像素值的异或操作生成加密图像。该方法加密安全性高,抗干扰性强,但处理速度较慢。文献[9]利用分岔分析和李雅普诺夫指数分析确定混沌特征,由此提出基于 1D 混沌映射的图像加密算法,其中置乱算法和代换算法均关联了混沌映射。文献[10]提出了基于 LDACLM 模型的快速图像加密算法,该算法结合了 Arnold 和 Logistic 混沌映射,取得了较好的加密性能和效率。但以上研究在大部分情况下仅需要对图像的重要部分而非整个图像进行保护,均没有考虑 ROI 加密。文献[11]提出一种单帧逐一加密和多帧组合加密相结合的算法,通过 Logistic 映射迭代得到 Logistic 混沌序列,利用生成的混沌序列对视频帧逐帧扩散,将组合矩阵重新分解为单帧图像,得到最终加密的图像。

到稿日期:2022-06-15　返修日期:2022-07-25
基金项目:国家自然科学基金(61601189);广东省普通高校科研项目(2019KTSCX243,2021ZDZX1070)
This work was supported by the National Natural Science Foundation of China(61601189) and Scientific Research Projects of Colleges in Guangdong Province(2019KTSCX243,2021ZDZX1070).
通信作者:张国梅(158060029@qq.com)

针对选择性图像加密，文献[12]提出了基于 2DDWT、Henon 混沌映射和 4DQi 超混沌的选择性图像加密方法，使用 2DDWT 对像素位置进行分解，利用 Henon 混沌映射置乱，然后利用 Qi 吸引子生成的密钥流，通过 XOR 进行扩散。文献[13]提出了用于彩色图像 ROI 的超混沌加密算法，该算法使用高斯混合模型识别人脸区域，使用包含 3 个正李雅普诺夫指数的超混沌系统对图像进行加密，并利用分级密钥确保加密序列的安全性，但该方法仅考虑脸部作为 ROI 区域。文献[14]提出了使用方波（SquareWave）和正交多项式变化的选择性图像加密方案，该方案处理速度非常快，适用于移动设备。但这些方案均未考虑到共享图片被其他用户转发的安全问题。当前一些社交平台并不限制用户分享其他用户发布的内容，用户可以简单地将内容转发至第三方，且没有应用任何数据保护，从而造成了隐私泄露。

针对上述问题，本文提出了基于 YOLO v4 和混合混沌映射技术的图像加密方案。通过 YOLO v4 实现自动图像检测，便于用户快速选择要隐藏的图像部分；利用 cosine-polynomial 混沌系统的加密算法对用户选定的图像区域进行加密，由此实现基于用户选择的 ROI 图像加密；此外，所提方案通过密钥发放和权限管理机制，使得第三方转发的图像中的敏感信息不会被未授权用户访问，极大地增强了社交平台上的图像的安全性。

2 目标检测与混沌映射

本文方案使用 YOLO v4 自动检测图像的 ROI 包围框，并利用所提混沌加密算法对相关区域进行加密。

2.1 YOLO v4

YOLO v4[15]是在 YOLO 基础上提出的端到端目标检测算法，其能够直接预测目标的类别和位置，因此检测速度非常快，比 YOLO v3 更加有效，且含有一个 SPP 模块。为执行特征提取，YOLO v4 依次使用 3×3 和 1×1 卷积层，并采用残差网络的理念。YOLO v4 中有 5 个残差块，利用残差单元，可以使用更深的网络深度，并避免梯度衰落。

YOLO v4 中对输入图像进行 5 次下采样，并预测最后 3 个下采样层中的目标。其中，以 3 个尺度进行目标检测。在尺度 3，使用 8 倍下采样的特征图来检测小目标；在尺度 2，使用 16 倍下采样的特征图来检测中等大小目标；在尺度 1，使用 32 倍下采样的特征图来检测大目标。使用特征融合进行目标检测，小特征图提供了深度语义信息，大特征图提供更细粒度的目标信息。为执行特征融合，YOLO v4 通过上采样重新调整较深网络层的特征图大小，由此将特征图转换为相同尺寸。通过串联，将浅层特征与深层特征合并，在检测较大和较小目标时均可达到优秀性能。

2.2 cosine-polynomial 混沌系统

选择性加密需要使用序列形式的加密方法，而非将整个过程视为一个模块，这意味着应该将整个图像作为一维数组形式进行处理。本文使用一维 cosine-polynomial 系统[16]进行图像加密。

$$\begin{cases} f:[-1;1]\to[-1;1] \\ x_{n+1}=f(x_n)=\cos(\mu(x_n^3+x_n)) \end{cases} \tag{1}$$

其中，μ 为实控制参数。对于大部分 μ 值，cosine-polynomial 系统表现出了极高的混沌性，其混沌区域涵盖了正实数的无限域。由此，cosine-polynomial 混沌映射满足密钥空间大、复杂度高、不可预测性的加密需求。

3 以用户为中心的选择性加密

本文针对社交平台上共享图片的隐私保护，设计了基于 YOLO v4 和混沌映射的选择性图片加密方案。所提方案的流程如图 1 所示。

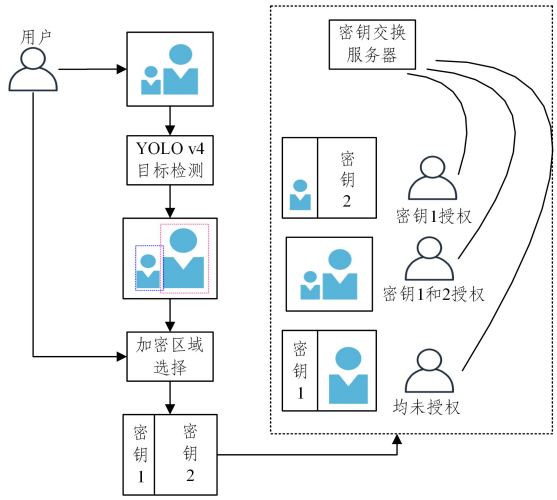


图 1 以用户为中心的选择性加密方案

Fig. 1 User-centered selective encryption scheme

3.1 图像加密算法

混沌图像加密系统是本文方案中的基础构建模块。对于大部分数值，cosine-polynomial 映射表现出了极高的混沌性，因此其混沌区域涵盖了正实数的无限域。cosine-polynomial 映射满足密钥空间大、复杂度高、不可预测性的加密需求。图 2 给出了所提方案的加密流程图，其采用了 cosine-polynomial 混沌。其中，所提方法结合了置乱和代换阶段，通过降低像素上的循环数，显著提高了加密速度。设 P 为明文图像，将加密过程分为行阶段和列阶段。为对图像行进行加密，从第一行到最后一行对图像行 P_i 进行迭代，并在每次迭代中对行 P_i 和行 $P_{EP(i)}$ 进行加密，EP 表示密钥流。也就是使用从 cosine-polynomial 混沌映射中生成的伪随机数序列和模运算，对这两行的数值进行掩模。然后，使用循环移位操作对行 P_i 的像素进行置乱。最后，通过对得出的图像进行转置，并在此应用行加密程序，对图像列进行加密。

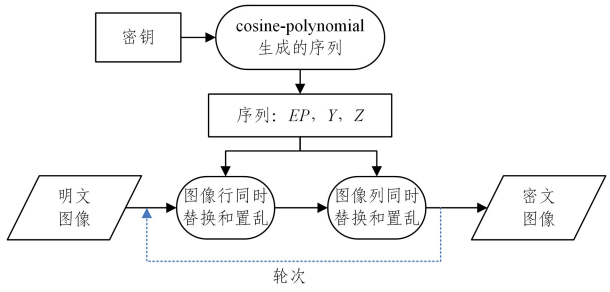


图 2 加密流程图

Fig. 2 Flowchart of encryption

3.2 加密过程

基于 cosine-polynomial 混沌映射的 ROI 图像加密算法

的详细步骤如下：

(1)取 ROI 明文图像 P，轮密钥 x_{ir}，μ_{ir}，$i\in\{1,2,3,4\}$，$r\in\{1,2,\cdots,T\}$，T 为总加密轮数；

(2)设轮数计数 $r=1$；

(3)设 M 为总行数，N 为总列数；

(4)使用 cosine-polynomial 映射生成长度为 M 的加密位置序列 EP，利用 x_{1r} 和 μ_{1r} 作为初始条件，并将 EP 值归一化：

$$EP=\{EP_i\mid EP_i=(EP_i\times 10^7)\bmod M\} \tag{2}$$

(5)计算 x_{5r}：

$$x_{5r}=x_{1r}+mean(P/\{P_1,P_{EP(1)}\}) \tag{3}$$

其中，$(P/\{P_1,P_{EP(1)}\})$为图像 P 中不包含第一行和第 $EP_{(1)}$ 行的平均像素值。

(6)分别使用 x_{3r}，x_{5r} 和 μ_{3r} 作为初始条件，通过 cosine-polynomial 映射生成长度为 N 的序列 Y 和 Z，然后再对生成序列进行归一化：

$$Y=\{Y_j\mid Y_j=(Y_j\times 10^7)\bmod 256\} \tag{4}$$

$$Z=\{Z_j\mid Z_j=(Z_j\times 10^7)\bmod 256\} \tag{5}$$

(7)从第一行到最后一行，每次迭代中对两个图像行 P_i 和 $P_{EP(i)}$ 进行加密：

$$\begin{cases}P_i=circshift((P_i+f(i)+pred(i))\bmod 256,EP(i))\\ P_{EP(i)}=(P_{EP(i)}+f(i)+pred(i))\bmod 256\end{cases}$$

其中，$circshift(P_i,n)$函数表示将行 P_i 向右进行 n 次循环位移操作，$f(i)$，$pred(i)$函数定义如下：

$$f(i)=\begin{cases}Y, & \text{if } i\neq 1\\ Z, & \text{if } i=1\end{cases}$$

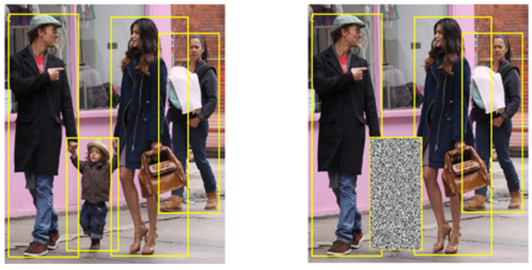
$$pred(i)=\begin{cases}P_M, & \text{if } i=1\\ P_{i-1}, & \text{if } i\neq 1\end{cases}$$

(8)对得到的图像矩阵进行 $P=P^t$ 转置，以对图像列进行加密，用 $x_{2r}+mean(\{X_{ir}\})$，x_{4r}，μ_{2r}，μ_{4r} 替代 x_{1r}，x_{3r}，μ_{1r}，μ_{3r}，重复执行步骤(3)－(7)，其中 $i\in\{1,2,3,4\}$，$mean(\{X_{ir}\})$为轮密钥均值。

(9)再次转置密文图像 $P=P^t$；

(10)依次增加轮计数器 $r=r+1$，并重复步骤(3)－(9)，直至 $r>T$。

在本文提出的基于用户选择的 ROI 图像加密方案中，首先，利用 YOLO v4 自动检测已知类别(如人、车辆等)的多个目标包围框；然后，用户与系统交互，选择需要隐藏的 ROI 区域，并输入密码作为图像解密的密钥；最后，应用所提的基于 cosine-polynomial 混沌映射的图像加密算法，对用户选择的 ROI 区域进行加密。图 3(a)给出了通过 YOLO v4 自动检测的包围框，图 3(b)给出了用户选择 ROI 区域后的选择性加密图像。



(a)原始图像 (b)加密图像

图 3 加密过程

Fig. 3 Encryption process

3.3 解密过程

通过反向执行所提图像加密算法，即可完成对 ROI 加密区域的解密，具体步骤如下：

(1)读取密文图像 P，轮密钥 x_{ir}，μ_{ir}，其中 $i\in\{1,2,3,4\}$，$r\in\{1,2,\cdots,T\}$，T 为总加密轮数。

(2)设轮计数器 $r=T$。

(3)转置密文图像矩阵 $P=P^t$ 以解密图像列。

(4)设 M 为总行数，N 为总列数。

(5)使用 cosine-polynomial 映射，通过设 $x_{2r}+mean(X_r)$ 和 μ_{2r} 为初始条件，生成长度为 M 的加密位置序列 EP，并应用式(2)将 EP 值归一化。

(6)利用 cosine-polynomial 映射，分别使用 x_{4r} 和 μ_{4r} 作为初始条件，生成长度为 N 的序列 Y。然后，应用式(3)将得出的序列归一化。

(7)从最后 1 行到第 2 行，在每次迭代中对 2 个图像行 P_i 和 $PEP(i)$解密：

$$\begin{cases}P_i=(circshift(P_i,EP(i))-Y-pred(i))\bmod 256\\ P_{EP(i)}=(PEP(i)-Y-pred(i))\bmod 256\end{cases}$$

(8)计算 x_{5r}：

$$x_{5r}=x_{1r}+mean(P/\{P_1,P_{EP(1)}\})$$

(9)利用 cosine-polynomial 映射，分别使用 x_{5r} 和 μ_{4r} 作为初始条件，生成长度为 N 的序列 Z。然后利用式(4)将序列归一化。

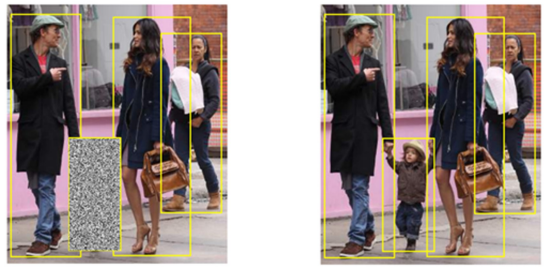
(10)解密第 1 行 P_1 和图像行 $P_{EP(1)}$：

$$\begin{cases}P_1=(circshift(C_1,EP(1))-Z-P_M)\bmod 256\\ P_{EP(1)}=(C_{EP(1)}-Z-P_M)\bmod 256\end{cases}$$

(11)对得出的图像矩阵 $\boldsymbol{P}=\boldsymbol{P}^t$ 进行转置，以解密图像行。然后利用 x_{1r}，x_{3r}，μ_{1r}，μ_{3r} 替换 $x_{2r}+mean(\{X_{ir}\})$，x_{4r}，μ_{2r}，μ_{4r}，并重复步骤(4)－(10)。

(12)依次减少加密轮计数 $r=r-1$，并重复步骤(3)－(11)，直至 $r<1$。

第三方用户访问使用本文方案加密后发布在社交平台的共享图像时，若该用户符合图像发布者定义的规则，则服务器自动向该用户发放密钥，其将看到解密后的图像，如图 4(b)所示；若该用户未得到授权，则仅能看到如图 4(a)所示的加密图像，其必须向服务器或图像发布方请求并得到密钥，才能完成图像解密。授权用户转发加密图像后，其他用户所访问的也是加密图像。由此保护了共享图像发布者的隐私信息。



(a)加密图像 (b)解密图像

图 4 解密过程

Fig. 4 Decryption process

4 实验结果与分析

本文通过执行一系列图像加密安全测试，以分析所提算

法的安全性和处理速度。这些图像包含 MHP 数据集以及一些标准测试图像。实验环境为 Intel i5 双核处理器，16 GB RAM，Windows10 操作系统，采用 MATLAB2011b 编程。

4.1 直方图分析

直方图可用于像素强度值的图形表征。灰度图像或单个彩色通道中存在 256 个不同的可能强度。因此，直方图的图形表示将展示 256 个强度和强度值之间的像素分布[17]。图 5 给出了灰度和彩色 Lena 图像的明文图像和密文图像的像素强度值直方图。从图中可发现，利用所提算法得到的密文图像的直方图是扁平且均匀分布的，证明其不会泄露任何有用信息。

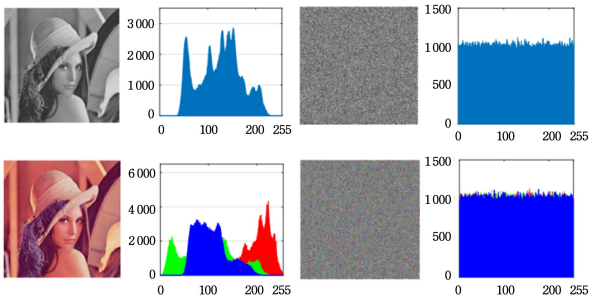


图 5 直方图结果

Fig. 5 Results of Histogram

使用卡方检验进一步证明密文图像直方图的均匀性[18]：

$$\chi^2=\sum_{i=0}^{255}\frac{(O_i-E_I)^2}{E_i} \tag{6}$$

其中，i 为灰度强度，O_i 为灰度 i 的观测发生频率，E_i 为灰度 i 的预期发生频率。假定显著性水平 $\alpha=0.05$，则 8 位灰度图像的临界值为 $\chi^2(255,0.05)=293.2478$。所提加密算法生成的密文图像的卡方检验值为 207.1030，低于临界值，证明密文图像有着均匀分布。

4.2 相关性分析

相关性分析用于寻找两个变量之间的关系。图像处理中，图像的每对邻近像素之间的相关性通常非常高，即像素与其邻近像素有着强关联。本文利用图像中水平、垂直和对角方向的像素计算相关性。图 6 给出了 ROI 区域的原始图像和加密图像所有通道在垂直方向上的相关性。像素值之间的相关性计算式为：

$$D(r)=\frac{1}{N}\sum_{i=1}^{N}[r_i-E(r)]^2$$

$$Cov(r,s)=\frac{1}{N}\sum_{i=1}^{N}[r_i-E(r)][S_i-E(s)]$$

$$r_{r,s}=\frac{Cov(r,s)}{\sqrt{D(r)}\sqrt{D(s)}} \tag{7}$$

其中，r_i 和 s_i 为两个连续像素的 8 位值。N 为像素对总数量。

图 6(a)－图 6(c)给出了明文图像 Lena 中，水平方向的相邻明文像素对的相关图，图 6(a)－图 6(c)分别表示绿色通道、红色通道和蓝色通道。图 6(d)－图 6(f)给出了使用所提算法加密后的相邻像素对的相关图，图 6(d)－图 6(f)分别表示绿色通道、红色通道和蓝色通道。从中可发现，明文图像的相邻像素之间存在强相关性，密文图像中相邻像素的灰度值则均匀分布。

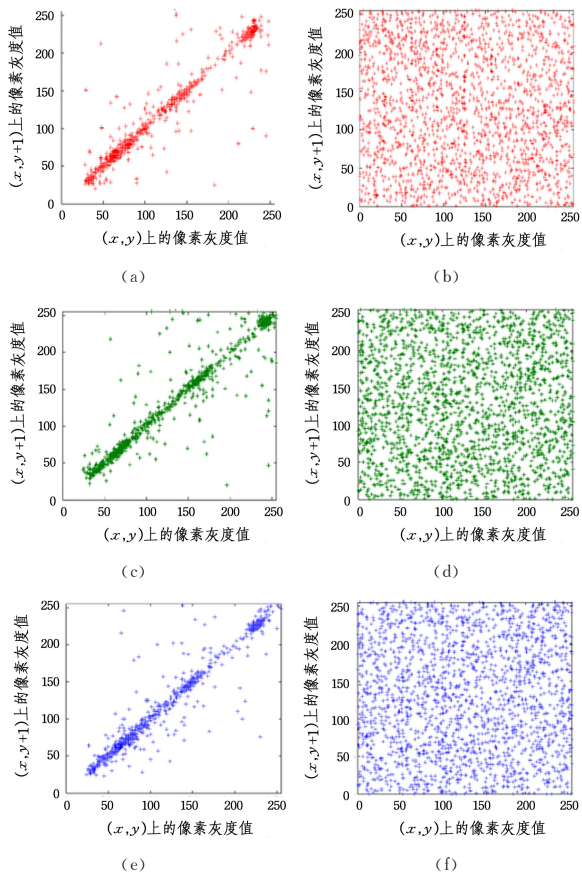


图 6 相关性分析结果

Fig. 6 Results of correlation analysis

4.3 信息熵分析

信息熵可量化给定消息 m 的信息不确定性。图像加密中，应用信息熵测量密文图像 C 的信息随机性。信息熵的理论最优值为 8，越接近最优值，证明加密方案安全性越高。信息熵的计算式为[19]：

$$H(C)=-\sum_{i=0}^{255}p(C_i)\log_2 p(C_i) \tag{8}$$

其中，$p(C_i)$ 为像素强度 i 在图像 C 中的出现频率。使用随机密钥，通过所提方法和其他先进方法对 Lena 图像进行加密，并应用 1 000 次熵检验，表 1 给出了测试结果。从中可以发现，所提方案生成的密文仅使用一轮加密，即取得了较高熵值。

表 1 信息熵测试结果

Table 1 Test results of information entropy

	最小值	最大值	均值	标准差
本文方案	7.9992	7.9997	7.9994	0.000055
文献[7]	7.9969	7.9985	7.9979	0.000238
文献[9]	7.9990	7.9994	7.9992	0.000060
文献[10]	7.9991	7.9994	7.9992	0.000059

4.4 明文图像敏感性

选择明文文本攻击(Chosen Plain-text Attack，CPA)是针对明文图像敏感度较低的加密方案的有效攻击手段。因此，安全的图像加密方案应对明文图像中的微小变化非常敏感。本文使用像素变化率(NPCR)和归一化平均变化强度(UACI)指标来检验明文图像敏感性，通过测试，对从两个有着细微差别的明文图像中生成的密文图像 C 和 C' 之间的差异进

行量化。NPCR 和 UACI 定义为：

$$NPCR(C,C')=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D_{ij}}{M\times N} \tag{9}$$

$$UACI(C,C')=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D|C_{ij}-C'_{ij}|}{M\times N\times F} \tag{10}$$

其中，若 $C_{ij}=C'_{ij}$，则 $D_{ij}=0$；若 N_α^*，则 $C_{ij}\neq C'_{ij}$。F 为最大可能像素值。相对于显著性水平 α，$NPCR$ 值必须大于 N_α^*，$UACI$ 值则必须在$[N_\alpha^{*-},N_\alpha^{*+}]$范围，以满足安全性要求。表 2 列出了当 $\alpha=0.05$ 时，不同图像尺寸下的 $NPCR$ 和 $UACI$ 阈值。

表 2 NPCR 和 UACI 理论阈值

Table 2 Oretical threshold of NPCR and UACI

（单位：%）

图像大小	NPCR N_α^*	UACI N_α^{*-}	UACI N_α^{*+}
256×256	99.5721	33.2820	33.6507
512×512	99.5902	33.3729	33.5551
1024×1024	99.5996	33.4207	33.5102

图 7 和图 8 分别给出了在不同 α 数值下，使用本文方案和其他加密方法时的 $NPCR$ 和 $UACI$ 结果。从中可以发现，本文方法的 $NPCR$ 值均高于 N_α^*，$UACI$ 值均在$[N_\alpha^{*-},N_\alpha^{*+}]$区间内，且与其他方法相比，本文方法的曲线更加稳定，证明所提算法对明文图像中的细微变化非常敏感，能够更好地抵御 CPA。

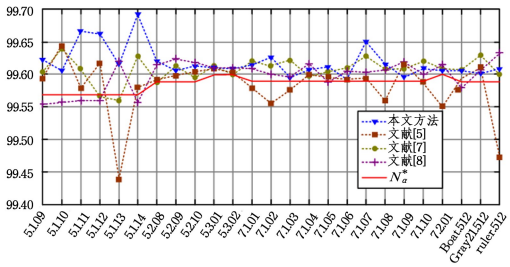


图 7 NPCR 结果

Fig. 7 Results of NPCR

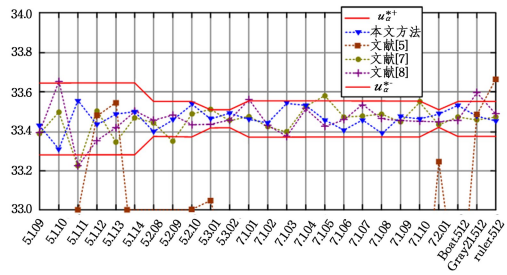
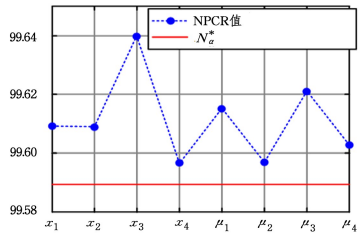


图 8 UACI 结果

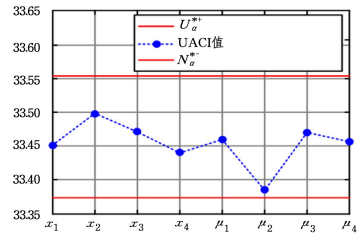
Fig. 8 Results of UACI

4.5 密钥分析

密码系统中，密码空间应足够大，以抵御蛮力攻击。所提加密算法的控制参数 μ 的双浮点精度为 10^{-16}，因此密码空间约为 $(10^{16\times4}\times10^{12\times4})^T\approx2^{392\times T}$，足以抵御蛮力攻击。此外，密钥必须对任何细微变化具有敏感性，对密钥的任何更改都会导致完全不同的密文图像。本文应用 UPCR/UACI 检验，对使用存在细微差异的密钥生成的密文图像之间的差异进行了测试。图 9 给出了测试结果，从中可发现，对密钥做任何更改所得到的结果都在 NPCR/UACI 的可接受范围内，证明所提算法具有很好的密钥敏感性。



(a) NPCR 值



(b) UACI 值

图 9 密钥敏感性测试结果

Fig. 9 Test results of key sensitivity

4.6 剪切攻击测试

在数据传输过程中，部分信息可能会丢失，这种情况被视为剪切攻击。图 10 给出了所提方法抵御剪切攻击的性能。图 10(a)中，密文图像损失了 30%的数据，这会造成一些图像块的丢失。但如图 10(b)所示，所提方法成功重建了其他区域的图像，这证明了所提方法能够很好地抵御剪切攻击，这得益于其在图像重建中分别利用了原始图像行和列的地址信息，因此部分信息的丢失并不会影响到其他图像区域，由此增强了压缩加密算法的鲁棒性。

(a)剪切攻击 (b)重建后

图 10 剪切攻击测试结果

Fig. 10 Test results of shear attack

4.7 处理速度

当前许多图像加密方案实现了极高的安全等级。但由于算法过于复杂，影响了处理速度，不适用于实时应用。表 3 列出了所提算法与其他先进方法在相同仿真环境中的理论和实际处理速度，从中可发现，对于不同分辨率的图像，所提算法的加密速度均大幅优于对比方法。这是因为所提算法通过大幅减少混沌映射的使用，将加密单元从像素级提升到行/列级，并合并代换和置乱阶段，由此显著加快了处理速度。

表 3 图像加密处理速度比较

Table 3 Comparison of image encryption processing speed

（单位：ms）

	本文方案	文献[7]	文献[9]	文献[10]
复杂度	$O(M+N)$	$O(MN)$	$O(MN)$	$O(MN)$
最小轮数	1	1	2	22
256×256	10.9	19.9	66.8	61.7
256×256	34.7	88.4	256.9	155.9
1024×1024	122.5	326.5	988.4	602.7

结束语 cosine-polynomial 映射在正实控制参数的较大区间内表现出非常高的混沌性，所提加密算法利用这一优点，并通过合并置乱和代换阶段，极大地提升了加密速度和安全性。仿真和实验结果表明，所提算法具有密钥空间大、不可预测性强、处理速度快的优点，能够稳定提供极高的安全性。基于所提加密算法的共享图像隐私保护方案通过 YOLO v4 快速检测 ROI，社交平台的用户在发布图像时，简单选择要加密的区域，即可保证隐私信息仅对特定授权人群开放，在分享图像的同时免受隐私泄露的风险。当处于计算资源受限的环境下，如嵌入式平台，所提算法的处理速度会大幅下降，如何将已有算法优化为一个轻量级的版本将是本文未来研究的方向之一。

参 考 文 献

[1] RATHORE S, SHARMA P K, LOIA V, et al. Social network security: Issues, challenges, threats, and solutions[J]. Information Sciences, 2017, 42(1): 43-69.

[2] LI L, XIE Y, LIU Y, et al. Exploiting opticalchaos for color image encryption and secure resource sharing in cloud[J]. IEEE Photonics Journal, 2019, 11(3): 1-12.

[3] REN H, NIU S Z, WANG M S, et al. Homomorphic and commutative fragile zero-watermarking based on SVD[J]. Computer Science, 2022, 49(3): 70-76.

[4] YU F, GONG X H, WANG S H. Cryptanalysis of medical image encryption algorithm using high-speed scrambling and pixel adaptive diffusion[J]. Computer Science, 2020, 47(2): 276-280.

[5] LI J Q, ZHOU J, DI X Q. Learning optical image encryption scheme based on CycleGAN[J]. Journal of Jilin University (Engineering and Technology Edition), 2021, 51(3): 1060-1066.

[6] LI F P, LIU J B, WANG G Y, et al. An image encryption algorithm based on chaos set[J]. Journal of Electronics & Information Technology, 2020, 42(4): 981-987.

[7] TANG J, YU Z, LIU L. A delay coupling method to reduce the dynamical degradation of digital chaotic maps and its application for image encryption[J]. Multimedia Tools and Applications, 2019, 78(17): 24765-24788.

[8] WEI L S, HU X C, CHEN Q Q, et al. A color image encryption algorithm based on new chaos and matrix convolution operation [J]. Computer Engineering and Science, 2020, 42(1): 80-88.

[9] LIU L, MIAO S. A new simple one-dimensional chaotic map and its application for image encryption[J]. Multimedia Tools and Applications, 2018, 77(16): 21445-21462.

[10] WANG X, FENG L, LI R, et al. A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model[J]. Nonlinear Dynamics, 2019, 95(4): 2797-2824.

[11] WEI C J, LI G D. Encryption algorithm of video images combining hyper-chaotic system and logistic mapping[J]. Computer Engineering, 2022, 48(5): 263-271.

[12] TRSOR L O, SUMBWANYAMBE M. A selective image encryption scheme based on 2d DWT, Henon map and 4d Qi hyper-chaos[J]. IEEE Access, 2019, 7(1): 103463-103472.

[13] XUE H, DU J, LI S, et al. Region of interest encryption for color images based on a hyperchaotic system with three positive Lyapunov exponets[J]. Optics & Laser Technology, 2018, 106(1): 506-516.

[14] KRISHNAMOORTHI R, MURALI P. A selective image encryption based on square-wave shuffling with orthogonal polynomials transformation suitable for mobile devices[J]. Multimedia Tools and Applications, 2017, 76(1): 1217-1246.

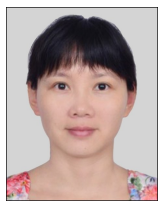
[15] ZHANG L D, DENG C. Multi-scale fusion of YOLOv3 crowd mask wearing detection method[J]. Computer Engineering and Applications, 2021, 57(16): 283-290.

[16] ZHU H, QI W, GE J, et al. Analyzing devaney chaos of a sine-cosine compound function system[J]. International Journal of Bifurcation and Chaos, 2018, 28(14): 176-188.

[17] GE J X, LAN L, QI W T, et al. Two-dimensional inverse-trigonometric hyperchaotic system and its application in image encryption[J]. Journal of Computer Applications, 2019, 39(1): 239-244.

[18] LIAO X, HAHSMI M A, HAIDER R. An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos[J]. Optik-International Journal for Light and Electron Optics, 2018, 153(2): 117-134.

[19] QAYYUM A, AHMAD J, BOULILA W, et al. Chaos-based confusion and diffusion of image pixels using dynamic substitution[J]. IEEE Access, 2020, 8(1): 140876-140895.



ZHANG Guo-mei, born in 1979, postgraduate, lecturer. Her main research interests include visual processing, graphics processing, virtual reality technology and application.

（责任编辑：何杨）