基于 QR 码和矩阵映射的强鲁棒性信息加密技术

孙业强，王晓红
（上海理工大学，上海 200093）

摘要：目的 为了避免传统加密算法直接将图像信息作为明文加密及加密图像含有明文图像信息而带来被破解的风险，提出一种将伪明文图像加密嵌入宿主图像传输的强鲁棒性信息加密技术。**方法** 首先对明文图像彩色 QR 码和伪明文图像进行初步加密，然后通过加性原则构造出两者之间的映射矩阵，最后基于小波变换和奇异值分解将加密后的伪图像嵌入到载体图像中。**结果** 仿真结果表明，该算法具有较高的安全性及强大的抗攻击能力。**结论** 算法通过将 QR 码作为明文图像建立与伪图像之间的关系，并将伪图像加密嵌入宿主图像传输，不仅有效地避免了明文被破解的风险，还具有较强的抗噪声、压缩、裁剪和旋转等恶意攻击能力，表明该加密算法具有良好的安全性和稳健性。

关键词： 彩色 QR 码；映射矩阵；小波变换；奇异值分解；信息加密
中图分类号： TP309.7 **文献标识码：** A **文章编号：** 1001-3563(2017)05-0194-06

Information Encryption Technology with Strong Robustness Based on QR Code and Matrix Mapping

SUN Ye-qiang, WANG Xiao-hong
(Shanghai University for Science and Technology, Shanghai 200093, China)

ABSTRACT: The work aims to put forward an information encryption technology with strong robustness by embedding pseudo plaintext image into host image transmission, in order to avoid the risk of being cracked brought by the traditional algorithm directly encrypting the image information as plaintext and the encrypted image with plaintext image information. First of all, preliminary encryption of plaintext image color QR code and pseudo plaintext image should be done, then the mapping matrix between two images by addition principle was constructed, and finally the encrypted pseudo image was embedded into the carrier image based on wavelet transform and singular value decomposition. Through establishing the relationship between the QR code (as plaintext image) and the pseudo image and embedding pseudo image into host image transmission, the algorithm not only effectively avoids the risk of cracked plaintext, but also has a strong ability to resist noise, compression, clipping, rotation and other malicious attacks, which shows that the encryption algorithm is of good security and robustness.

KEY WORDS: color QR code; mapping matrix; wavelet transform; singular value decomposition; information encryption

图像作为信息的主要载体，在信息传输中起到了重要作用，所以传统的信息加密技术大部分均是基于灰度图像直接对其加密传输[1—3]。随着计算机技术的发展，现有直接对图像进行加密的算法被破解的风险越来越大，同时现有加密算法还不具有强大的抗攻击能力，加密图像在被恶性攻击后不能较好地复原明文图像。2008年，郑凡等[4]提出了基于Henon映射的数字图像加密算法，算法直接对灰度图像进行加密传输具有较强的密钥敏感性，但抗噪声和裁切能力不强。2014年，刘效勇等[5]提出了基于压缩感知的光学图像加密技术研究，其基

收稿日期： 2016-03-08
作者简介： 孙业强（1992—），男，硕士，上海理工大学硕士生，主攻数字图像处理。
通讯作者： 王晓红（1971—），女，博士，上海理工大学教授，主要研究方向为颜色科学和数字图像处理。

于压缩感知理论对明文图像进行了多重加密，并嵌入到宿主图像进行传输。虽然该技术并没有对加密图像直接传输，但载体图像中仍含有明文图像加密后的信息，仍具有被破解的风险。同时，由于采用了压缩感知技术，所以加密解密时间较长，而且算法抗裁切能力一般，1/4的裁切攻击后PSNR值仅为14.5759。

针对这种状况，文中提出了一种基于彩色QR码和矩阵映射具有强大抗攻击能力的信息加密技术。针对传统图像传递信息有限的情况，通过使用彩色QR码作为明文图像进行加密，不仅极大地拓展了加密信息的内容和格式，而且对加密信息起到了一定程度的隐藏作用，即便在一定程度上被破解，如果不能成功识别，加密信息仍能得到保护，相对于传统方法及简单的二值QR码安全性得到了一定提高。通过建立彩色QR码和伪明文图像之间的映射矩阵并作为密钥，实现了明文图像不参与传输的过程，完全避免了针对传输图像被破解的风险。通过将伪图像嵌入载体图像传输也实现了被不法分子破解时的迷惑作用，有效地保护了加密信息的安全，同时基于DWT和SVD的嵌入手段，有效地提升了算法的抗攻击能力。

1　基本原理

1.1　Arnold 变换

Arnold变换又叫猫脸变换(Cat mapping)，Arnold变换的原理是先作x轴方向的错切变换，再作y轴方向的错切变换，最后的模运算相当于切割回填操作，Arnold变换直观、敏感性高、具有周期性，使用非常方便[6]。假如图像的阶数为N，原始图像像素点坐标为(x,y)，变换后的坐标为(x',y')，那么Arnold变换见式(1)。

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 11 \\ 12 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\, N) \tag{1}$$

Arnold变换具有周期性，周期与图像的大小相关，但并不成固定比例[7]。由于Arnold变换迭代到一定次数时就会恢复到原图像，所以须结合其它加密算法才能避免被轻易破解。

1.2　奇异值分解（SVD）

奇异值分解是数学中常用的将矩阵对角化的方法之一，它能够捕获矩阵数据重要的基本结构，在图像压缩、信号处理和模式识别等领域中具有广泛的应用[8]。设秩为r，大小为$N\times N$的矩阵$\boldsymbol{X}$，满足$r\le N$，则有奇异值分解见式(2)[9]：

$$\boldsymbol{X} = \boldsymbol{U}\boldsymbol{S}\boldsymbol{V}^{\mathrm{T}} \tag{2}$$

式中：矩阵 $\boldsymbol{U}$ 和 $\boldsymbol{V}$ 相互正交，矩阵 $\boldsymbol{S}$ 为奇异的对角矩阵，而且对角元素满足 $\lambda_1\ge\lambda_2\ge\ldots\ge\lambda_r\ge\lambda_r+1=\ldots=\lambda_N=0$。奇异值分解不仅对方阵有效，而且适用于非方阵，应用范围更广。当图像遭受攻击时，对奇异值的影响较小，具有较好的鲁棒性[10]。

2　信息加密与解密过程

2.1　信息加密算法

为进一步提高加密的安全性，选择具有结构层次和阶调变换的彩色QR码作为携带加密信息的明文图像。文中采用微信手机客户端生成的彩色二维码名片作为明文图像，在实践中可以使用专业的二维码制作软件生成具有不同效果彩色QR码，如HiVDP软件。文中加密算法的整体原理见图1。

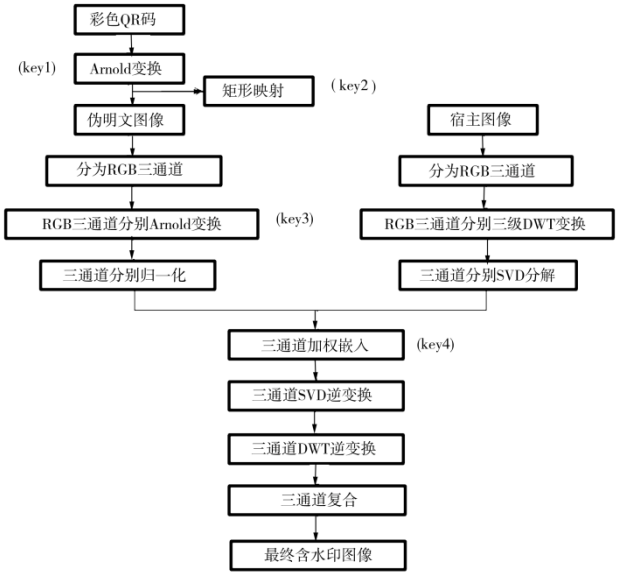


图 1　信息加密算法流程

Fig.1 The process of information encryption algorithm

1）对明文图像即彩色 QR 码进行初步加密。由原图像生成 R, G, B 三通道灰度图，对每一通道进行 Arnold 变换，每一通道迭代的次数作为密钥 1[11]。

2）将伪明文图像（即水印）分解为 R, G, B 三通道，由置乱后的 QR 码和伪图像生成两图像对应通道之间的映射关系 K，映射矩阵作为第 2 道密钥，也是作为解密过程中联系明文图像与宿主图像最重要的密钥 2，映射关系见式(3)。

$$K = X + Y \tag{3}$$

式中：X 为彩色 QR 码经 Arnold 变换加密后的分通道图像；Y 为伪明文图像对应的分通道图像；K 为映射矩阵即密钥 2。

3）对伪明文图像分通道进行 Arnold 变换加密，迭代的次数作为密钥 3。

4）对置乱加密后的伪图像进行归一化处理。由于彩色图像信息量太大将使不可见性较差，所以文中基于式(4)[12]对置乱后的各通道图像就行归一化处理。其中，r 为像素原始值；r'为归一化后的像素值，极大地减少了信息的嵌入量。

$$r = (r - 128)/128 \tag{4}$$

5）对宿主图像分通道进行三级小波变换后再对

其 SVD 奇异值分解。

6）嵌入伪明文图像。通过式（5）将伪明文图像各通道加密归一化后的信息 W 加权嵌入到载体图像 $\boldsymbol{S}$ 矩阵中，并保存 $\boldsymbol{U}_1$ 和 $\boldsymbol{V}_1$ 作为密钥 4。然后进行 SVD 逆变换、DWT 逆变换并合并得到含伪图像信息的宿主图像。

$$\boldsymbol{S}+\alpha W=\boldsymbol{U}_1\boldsymbol{S}_1\boldsymbol{V}_1^{\mathrm{T}} \tag{5}$$

式中：$\boldsymbol{S}$ 为步骤 5）奇异值分解后的对角矩阵，α 为水印嵌入强度，W 为步骤 4）处理后的伪图像信息，$\boldsymbol{U}_1$，$\boldsymbol{V}_1$ 为对嵌入伪图像信息后的对角矩阵再次进行奇异值分解生成的正交矩阵，$\boldsymbol{S}_1$ 为对应的对角矩阵，T 为转置。

7）将各通道宿主信息进行 SVD 逆变换和小波逆变换后复合为含伪图像信息的宿主图像进行传输。

2.2 信息解密流程

解密过程即为加密过程的逆运算，原理见图 2。

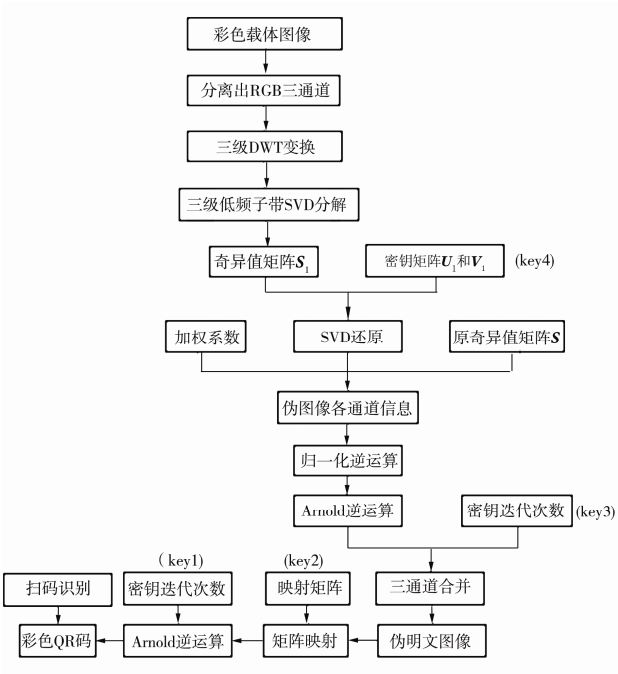


图 2 信息解密算法流程

Fig.2 The process of information decryption algorithm

1）对宿主图像进行三级小波变换，并对低频子带进行 SVD 分解得到奇异值 S_1。

2）基于 SVD 分解所得奇异值 S_1，借助密钥 4 经式(6)得到水印各通道信息 W。

$$W=(\boldsymbol{U}_1\boldsymbol{S}_1\boldsymbol{V}_1^{\mathrm{T}}-\boldsymbol{S})/\alpha \tag{6}$$

式中：$\boldsymbol{U}_1$，$\boldsymbol{V}_1$ 为对嵌入伪图像信息后的对角矩阵再次进行奇异值分解生成的正交矩阵即密钥 4；$\boldsymbol{S}$ 为原宿主图像奇异值矩阵；α 为加权系数；T 为转置。

3）对各通道水印信息通过反归一化公式进行反归一化处理。反归一化公式见式(7)。式中：r 为像素原始值；r'为归一化后的像素值。

$$r=r'\times 128+128 \tag{7}$$

4）将步骤 3）得到的各通道信息借助密钥 3 进行 Arnold 逆变换合并得伪明文图像。

5）通过式(8)借助密钥 2 对伪明文图像进行逆映射得彩色 QR 码加密信息 X。

$$X=K-Y \tag{8}$$

式中：X 为彩色 QR 码经 Arnold 变换加密后的分通道图像；Y 为伪明文图像对应的分通道图像；K 为映射矩阵即密钥 2。

6）再借助密钥 1 进行 Arnold 逆变换得到明文图像的 R，G，B 灰度图，进而复合得到明文图像即彩色 QR 码，并对其扫码识别提取加密信息。

3 实验仿真与分析

3.1 信息加密仿真实验准备

为了测试文中加密算法的性能，利用 Matlab2010a 进行仿真。选择像素大小为 64×64 的彩色 QR 码 a 和彩色 QR 码 b 作为携带加密信息的明文图像，像素大小为 64×64 的“音乐堂”作为伪明文图像，像素大小为 512×512 的“Lena”和“Peppers”作为宿主图像。

3.2 信息加密与解密效果分析

3.2.1 加密和解密图像质量分析

由于将伪明文图像嵌入到宿主图像中传输，必然会造成宿主图像质量有所损失，然而过多的质量损失会暴露宿主图像含有加密信息进而增加信息的风险性，所以在加密主图像含有加密信息进而增加信息的风险性，所以在加密过程中，应尽可能地减少对宿主图像质量的影响以提升信息加密的安全性。Wang 等[13]提出了结构相似性理论(SSIM)，对参考图像的亮度、对比度和

a 彩色 QR 码　b 彩色 QR 码　c 伪明文图像　d 宿主图像 Lena　e 宿主图像 Peppers

图 3 仿真实验所用图像

Fig.3 The images used in experiment

结构信息进行比较，能够有效地对图像进行质量评价，并得到了广泛地应用。SSIM的值在0和1之间，数值越接近1表明图像质量相对于原图损失的越少，宿主图像被发现隐藏信息的风险性也就越低，同理，明文图像即彩色QR码恢复的效果也就越好，进而更易被识别提取加密信息。

文中通过使用SSIM算法对原宿主图像和加密宿主图像、原彩色QR码和提取所得QR码进行图像质量评价，针对所提取的明文图像为QR码，采取更符合实际应用的手机微信中的QR码扫码器进行扫描识别，通过10次扫码的识别成功率对所提取的明文图像即彩色QR码进行评价。在初始密钥为K_{11}=90, K_{12}=120, K_{13}=70; K_{21}=75, K_{22}=110, K_{23}=80的条件下对两彩色QR码借助伪明文图像嵌入到两载体图像中，进行加密与正确解密的结果见表1。

通过分析可知，嵌入信号后的宿主图像SSIM值均高达0.9999，表明嵌入伪图像的不可见性很好；提取的明文图像SSIM值均达到0.97左右，表明提取的彩色QR码恢复良好，识别率均达到100%。由此可见，该信息加密算法的安全性和加密信息的恢复性较好。

表 1　图像加密与解密质量评价
Tab.1 Quality evaluation of image encryption and decryption

宿主图像	彩色QR码	宿主图像SSIM值	彩色QR码SSIM值	识别率/%
Lena	a	0.9999	0.9759	100
	b	0.9999	0.9706	100
Peppers	a	0.9999	0.9766	100
	b	0.9999	0.9694	100

3.2.2　抗恶性攻击能力分析

针对传输过程中可能遭受的各种恶性攻击，如裁剪、旋转、JPEG压缩、高斯噪声、椒盐噪声、泊松噪声、斑纹噪声等，通过matlab仿真检验知该算法对此类攻击的抵抗能力，并通过SSIM和识别率对算法进行评价，具体实验结果见表2。

表 2　抗攻击实验结果
Tab.2 The experimental result of anti-attack test

评价指标（SSIM/识别率）	Lena		Peppers	
	彩色 QR 码 a	彩色 QR 码 b	彩色 QR 码 a	彩色 QR 码 b
1/4 裁切	0.8456/100%	0.8164/100%	0.7632/100%	0.7148/100%
旋转 33°	0.7006/50%	0.7668/100%	0.7324/80%	0.7003/100%
旋转 121°	0.6988/70%	0.7603/100%	0.7358/90%	0.7024/100%
JPEG 压缩(50%)	0.9553/100%	0.9440/100%	0.9550/100%	0.9420/100%
JPEG 压缩(5%)	0.6988/70%	0.7397/100%	0.8148/100%	0.7730/100%
高斯噪声(0.05)	0.8195/100%	0.7710/100%	0.8586/100%	0.7997/100%
高斯噪声(0.1)	0.7743/70%	0.7004/100%	0.7789/100%	0.7283/100%
椒盐噪声(0.1)	0.8601/100%	0.8121/100%	0.8820/100%	0.8274/100%
椒盐噪声(0.2)	0.7743/90%	0.7216/100%	0.7965/100%	0.7481/100%
斑纹噪声(0.1)	0.8647/100%	0.8250/100%	0.8865/100%	0.8724/100%
泊松噪声	0.9662/100%	0.9510/100%	0.9656/100%	0.9649/100%

由表 2 分析可知，算法能够很好地抵抗多种攻击，稳健性较强。其中，对 JPEG 压缩、裁剪、旋转、椒盐噪声等攻击的抗攻击能力较强，对于结构复杂、层次丰富的彩色 QR 码，抵抗高斯噪声的能力相对较弱，所以，在应用中可根据需要选择复杂程度合适的彩色 QR 码作为隐藏加密信息的明文图像。

3.2.3　算法优势对比分析

文中通过与算法[5]进行优势对比，实验图像选择“Lena”为宿主图像和彩色 QR 码 b 为明文图像，实验对比结果见表 3。

由表 3 可知，相对于算法[5]，文中算法解密图像恢复效果更好，抵抗攻击能力更强，尤其对于裁切和旋转攻击，文中算法具有较大的进步；同时，在时效性上，文中算法速度具有较大的提升，能够更好地应用在实际生活中。

表 3　算法优势对比
Tab.3 Comparison of algorithms

算法	加密时间/s	解密时间/s	总时间/s	PSNR				
				解密图像	1/4裁切	旋转121°	椒盐噪声(0.1)	高斯噪声(0.1)
算法[5]	0.6875	12.6563	13.3438	30.8170	14.5759	不抗	30.7262	30.7432
文中算法	0.7725	1.6202	2.3957	41.0775	33.1079	29.5702	33.0155	30.5010

3.3　密钥安全性分析

3.3.1　密钥空间分析

高度的密钥敏感性和足够大的密钥空间可以抵抗穷举攻击[14]。相对于传统加密算法基于灰度图像加密，文中算法采用彩色图像作为明文图像和宿主图像，有效地增加了破解的难度。信息解密时需要四层密钥，其中多通道的迭代次数需要同时被破解才可解密图像，有效地扩大了密钥空间；同时，映射矩阵作为联系传输信息和加四层密钥同时正确时才能解密信息，仅截获密钥或获得解密算法并不能解密出加密信息，表明该算法具有强大的密钥空间。

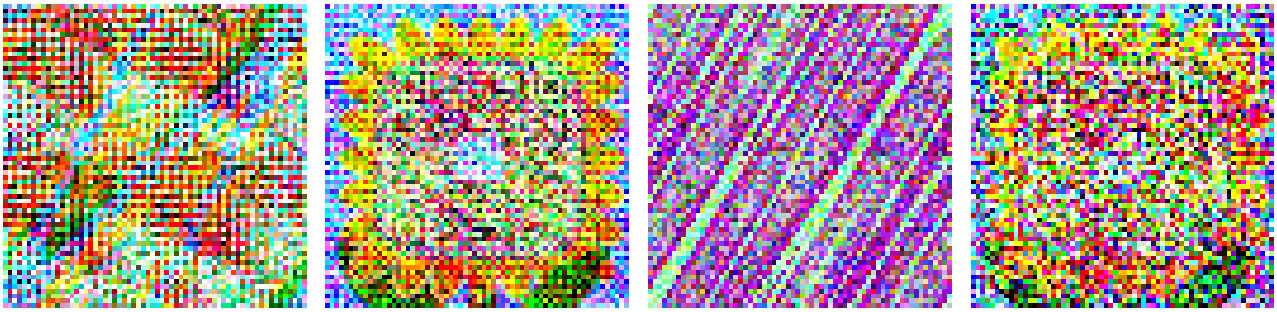
3.3.2　密钥敏感性分析

在密钥初始值 K_{11}=90, K_{12}=120, K_{13}=70; K_{31}=75, K_{32}=110, K_{33}=80 的条件下，采用明文图像即彩色 QR 码 a 和宿主图像 Lena 进行仿真实验。对图像进行解密并识别，解密效果图和识别结果见图 4，图 4 中的图像均无法识别。图 4a 中 K_{11}=91, K_{12}=119, K_{13}=71；K_{31}=74, K_{32}=111, K_{33}=8111=90；K_{12}=120。图 4b 中 K_{11}=90, K_{12}=120, K_{13}=70；K_{31}=74, K_{32}=108, K_{33}=80。图 4c 中映射矩阵密钥顺序错误。图 4d 奇异值正交矩阵错误。

由图 4 可知，当密钥均发生轻微误差或者其中部分密钥发生误差时，解密图像是一副乱码，彩色 QR 码无法辨析并不能识别解码，表明算法具有较高的密钥敏感性。即便能够模糊辨析明文图像的大致轮廓，但也不能获取任何加密信息，相对于传统直接将图像作为加密信息进行加密，在一定程度上增强了算法的安全性。

3.3.3　统计特性分析

通过对比原始图像和加密图像的直方图，可对原始图像和加密图像的相关性进行分析[15]。图 5a, b 分别为隐藏加密信息的明文图像即彩色 QR 码和加密宿主图像“Lena”的直方图。通过数据分析可知，加密前后图像的直方图具有明显的变化和差异，即明文图像的统计性被打破，降低了明文和密文的相关性，隐藏了图像的统计特性，在一定程度上降低了被破解的风险。



a SSIM=0.0360　　b SSIM=0.4585　　c SSIM=0.0384　　d SSIM=0.1959

图 4　错误密钥时的解密图像

Fig.4 The decrypted image with wrong key

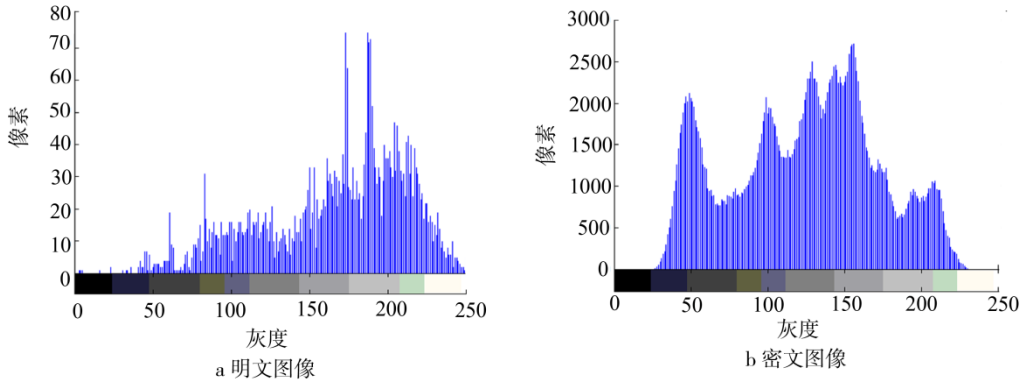


图 5　加密前后图像直方图对比

Fig.5 Image histogram comparison before and after encryption

4　结语

针对传统加密算法直接基于明文图像加密或嵌入载图像传输而带来易被破解的风险，提出了一种基于 QR 码和矩阵映射的信息加密算法。算法采用携带加密信息的彩色 QR 码作为明文图像，基于 Arnold 变换和奇异值分解等方法，通过建立其与伪明文图像的映射矩阵并将伪明文图像嵌入载体图像进行传输，实现了密钥和算法的密切结合，起到了单方面截获算法或密钥完全破解不出加密信息的作用，表明算法对不法分子具有较大的迷惑性的同时极大地增强了系统的安全性。通过 Matlab 仿真表明算法不仅能够有效地提

高加密的安全性，而且对裁剪、旋转、压缩、噪声等攻击具有强大的抵抗能力，在实际生活中具有较高的应用价值。

参考文献：

[1] 蔡宁, 沈学举. 基于傅里叶变换和 Gyrator 变换的图像加密[J]. 光学仪器, 2015, 37(1): 76—78.
CAI Ning, SHEN Xue-jun. Image Encryption Based on Fourier Transform and Gyrator Transform[J]. Optical Instruments, 2015, 37(1): 76—78.

[2] 芮坤坤. 基于离散傅里叶变换融合双混沌映射的图像加密算法研究[J]. 计算机应用与软件, 2014, 31(10): 322—328.
RUI Kun-kun. On Image Encryption Algorithm Based on Discrete Fourier Transformation Integrating with Doubling Chaotic Map[J]. Computer Applications and Software, 2014, 31(10): 322—328.

[3] 刘乐鹏, 张雪峰. 基于混沌和位运算的图像加密算法[J]. 计算机应用, 2013, 33(4): 1070—1073.
LIU Le-peng, ZHANG Xue-feng. Image Encryption Algorithm Based on Chaos and Bit Operations[J]. Journal of Computer Applications, 2013, 33(4): 1070—1073.

[4] 郑凡, 田小建, 范文华, 等. 基于 Henon 映射的数字图像加密[J]. 北京邮电大学学报, 2008, 31(1): 66—70.
ZHENG Fan, TIAN Xiao-jian, FAN Wen-hua, et al. Image Encryption Based on Henon Map, Journal of Beijing University of Posts and Telecommunications, 2008, 31(1): 66—70.

[5] 刘效勇, 曹益平, 卢佩. 基于压缩感知的光学图像加密技术研究[J]. 光学学报, 2014, 34(3): 91—99.
LIU Xiao-yong, CHAO Yi-ping, LU Pei. Research on Optical Image Encryption Technique with Compressing Sensing[J]. Acta Optic Sinica, 2014, 34(3): 91—99.

[6] 杨洋. 基于 Arnold 变换的数字图像加密算法[D]. 广州: 华南理工大学, 2015.
YANG Yang. A Digital Image Encryption Algorithm Based on Arnold Transformation[D]. Guangzhou: South China University of Technology, 2015.

[7] 任洪娥, 尚振伟, 张健. 一种基于 Arnold 变换的数字图像加密算法[J]. 光学技术, 2009, 35(3): 385—390.
REN Hong-e, SHANG Zhen-wei, ZHANG Jian. An Algorithm of Digital Image Encryption Based on Arnold Transformation[J]. Optical Technique, 2009, 35(3): 385—390.

[8] 罗竟毅. 基于小波变化的盲水印算法研究[D]. 长沙: 中南大学, 2007.
LUO Jing-yi. Study on Blind Watermarking Image Based on DCT[D]. Changsha: Central South University, 2007.

[9] 钱华明, 于鸿越. 基于 SVD-DWT 域数字图像水印算法[J]. 计算机仿真, 2009, 26(8): 104—107.
QIAN Hua-ming, YU Hong-yue. A Digital Image Watermarking Algorithm Based on SVD-DWT[J]. Computer Simulation, 2009, 26(8): 104—107.

[10] 王晓红, 魏代海, 刘玄玄, 等. 一种彩色 QR 码嵌入彩色图像的数字水印技术[J]. 光电子 • 激光, 2016(10): 1094—1100.
WANG Xiao-hong, WEI Dai-hai, LIU Xuan-xuan, et al. Digital Watermarking Technique of Color Image Based on Color QR Code[J]. Journal of Optoelectronics Laser, 2016(10): 1094—1100.

[11] AHMAD A M. RGB Color Image Encryption-decryption Using Gray Image[J]. IJCSI International Journal of Computer Science Issues, 2015, 12(3): 137—140.

[12] 张博. 基于新型 Arnold 反变换的双彩色图像水印算法研究[J]. 计算机与数字工程, 2013, 41(11): 1819—1834.
ZHANG Bo. Double Color Image Watermarking Algorithm Based on New Anti-Arnold Transformation[J]. Computer &Digital Engineer, 2013, 41(11): 1819—1834.

[13] WANG Z, BOVIK A C, SHEIKH H R. Image Quality Assessment: from Error Visibility to Structural Similarity [J]. IEEE Trans on Image Processing, 2004, 13(4): 600—612.

[14] 邓晓衡, 廖春龙, 朱从旭, 等. 像素位置与比特双重置乱的图像混沌加密算法[J]. 通信学报, 2014, 35(3): 216—223.
DENG Xiao-heng, LIAO Chun-long, ZHU Cong-xu, et al. Image Encryption Algorithms Based on Chaos Through Dual Scrambling of Pixel Position and Bit[J]. Journal on Communications, 2014, 35(3): 216—223.

[15] 陈国亮. 基于混沌理论的的彩色图像加密算法研究[D]. 兰州: 兰州大学, 2012.
CHEN Guo-liang. The Study of Color Image Encryption Algorithm Based on Chaos Theory[D]. Lanzhou: Lanzhou University, 2012.