彩色图像中文字的加密和隐藏

徐畅凯[1*]，徐文华[1]，姜　威[2]
（1. 重庆工商大学派斯学院，重庆 401520；
2. 贵州民族大学，贵州 贵阳 550018）

摘　要：针对公众在网上交流时，身份，账号等重要文字信息被窃取的问题，提出了一种将文字进行加密，并隐藏于彩色图像的方法。首先引入一种改进的 Logistic 映射，以密钥 a 和 x_0 产生混沌序列，以混沌序列对文字的 Unicode 编码进行比特级置乱，然后对图像红色通道进行 FFT 变换得到频谱图，构造密钥 Q，R 对频谱图实施逆变换得到纹理图，以纹理图为参数，利用改进的 LSB 算法将置乱的文字编码隐藏到图像的绿色和蓝色通道中。对于密图，利用密钥（a，x_0，Q，R）反向操作，即可解密隐藏信息。通过实验模拟和数据分析表明：密钥 a 和 x_0 对文字信息加密敏感；Q，R 对信息隐藏位置加密敏感；密钥空间为 10^{60}；密图峰值信噪比约为 50 dB。由此实现了对文字信息和文字隐藏位置的双重加密，提高了文字信息传输的安全性。

关键词：文字；Logistic 映射；加密；隐藏；彩色图像
中图分类号：TP391　　**文献标识码**：A　　**文章编号**：1673-629X(2021)05-0126-05
doi：10.3969/j.issn.1673-629X.2021.05.022

Encryption and Hiding of Text in Color Image

XU Chang-kai[1*]，XU Wen-hua[1]，JIANG Wei[2]
（1. Pass College of Chongqing Technology and Business University，Chongqing 401520，China；
2. Guizhou Minzu University，Guiyang 550018，China）

Abstract：Aiming at the problem of identity，account number and other text information theft when the public communicates online，a method of encrypting and hiding text in color image is proposed. Firstly，an improved Logistic map is introduced to scramble the binary of text Unicode coding with chaotic sequences generated by keys a and x_0，then transform the red channel of the image to get the spectrum by using FFT，construct key Q，R and invert the spectrum to get texture map. Taking texture map as parameter，the improved LSB algorithm is used to hide the scrambled text code in the green and blue channels of image. For the secret graph，the secret information can be decrypted by the reverse operation and the key（a，x_0，Q，R）. Through the experimental simulation and data analysis，it is concluded that the key a and x_0 are sensitive to text information encryption；Q and R are sensitive to the location of information hiding. The key space is 10^{60}. The peak signal-to-noise ratio of the secret image is about 50 dB. Thus，the proposed algorithm realizes the double encryption of text and hiding location and improves the security of text information transmission.

Key words：text；Logistic map；encryption；hiding；color image

0　引　言

如今随着网络的高速发展，网络安全问题变得突出，如电信诈骗、网络诈骗等。人们在享受网络便捷的同时，也面临信息被泄露、窃取和篡改的风险。因此，如何保障信息安全是一个重要的问题，而文字信息又是人们在网上使用最多的一种信息。

目前，针对文字信息的加密隐藏研究并不多，但是文字信息的加密隐藏实际上包含加密技术和隐写术两种技术，对这两种技术的研究有很多研究成果。文字信息的加密就是结合密码学对文字信息进行加密，使得窃密者能够检测出载体有载密信息而无法破解信息。目前大多数研究是利用混沌模型加密信息，因为其对初始条件的高度敏感性、有界性、系统的整体稳定性和随机性，使得在保密通信中得到了极大的应用[1-6]。比较著名的混沌模型有 Logistic 映射、Lorenz 模型和 Rossler 模型等，其中 Logistic 映射是结构最简单的一种混沌模型。文献[1]对 Logistic 映射的安全性进行了分析，并在此基础上提出一个改进的混沌模

收稿日期：2020-06-29　　**修回日期**：2020-10-30
基金项目：国家自然科学基金青年项目(61901131)
作者简介：徐畅凯(1983-)，男，讲师，硕士，从事图形图像处理算法研究。

型,模型计算量小且有两个参数可用作密钥,在一定的参数条件下迭代可直接进入混沌状态,克服了一般混沌模型都有的空白窗和稳定窗问题,迭代值在[0,1]区间均匀分布。文献[2]针对含有指数函数的改进 Lorenz 映射存在溢出的不足进行了改进。文献[3]结合 Sine 和 Tent 混沌映射,构造了一个二维超混沌映射,相比 2D-Logistic 和 2D-Henon 映射有更优秀的混沌性能,但分支参数不能作为密钥,需要选取合适的值,依然存在明显的空白窗口和稳定窗的问题。文献[4]提出通过公钥加密的方法,利用 LWE 算法加密后的信息冗余设计了一种多层加密隐藏方案,可以实现在载体图像中嵌入多重隐藏信息并且带有多重数据隐藏密钥,实现在特定层次的密钥只能解开特定层次的隐藏信息。

隐藏术又发展为可逆数据隐藏和非可逆数据隐藏[5-9]。对于可逆数据隐藏目前主要有 4 种方法:基于量化的方法、基于直方图修正的方法、基于压缩的方法、双图像的方法。其中双图像可逆数据隐藏方法是最近由学者提出的[9],即在嵌入隐藏数据的过程中生成两个相似的密图。该方法和之前的方法相比具有较高的数据嵌入能力和较低的图像失真率。LSB 算法是最常用的一种量化方法,文献[10]的论证表明该方法易于实现,不可感知性好,且隐藏容量较大。对于 LSB 算法对载体的不可逆性,且易检测攻击和破解等问题,文献[10]提出一种基于相邻灰度值对互补嵌入的 LSB 匹配隐写改进算法。

文献[11]利用差值扩展和直方图平移的思想,给出了一种可逆数据隐藏的方法;文献[12]利用离散余弦变换和 JPEG 图像编码特征给出一种在 JPEG 图像中的可逆数据隐藏方法;文献[13-17]针对嵌入效率和嵌入容量提出了改进的可逆数据隐藏方法。

尽管已经有了很多的数据隐藏和加密技术,将这些技术具体应用到文本保密的实例却不多,大多数数据隐藏和加密技术都应用在数字水印、数字认证和版权保护等方面。该文针对文字信息给出了一种加密并隐藏的方法。首先利用文献[1]中改进的 Logistic 映射加密文字,然后利用傅里叶变换,构造两个参数产生图像的一组随机纹理,以纹理为参数将文字隐藏到图像对应的纹理部分,达到文字信息加密、隐藏位置加密的效果。

1　文字加密方法

由于平常使用的大多文字包括符号数字都有国际通用的 Unicode 码,而 Unicode 码采用 16 进制数编码,因此每一个文字都和一个 16 位二进制码是一一映射的关系,加密文字就是加密 Unicode 码。其过程是首先将每个文字转化为 Unicode 码对应的 16 位二进制比特流,然后利用给定的初值,通过改进的 Logistic 映射产生一个相应长度的混沌序列,在混沌序列的基础上产生一个等长的比特流,将两组比特流进行异或运算达到置乱原文字比特流的目的,从而实现加密。文中算法均使用 Matlab 自带函数描述和实现,具体方法如下:

(1)输入文本字符,利用函数 abs( )将文字转化为 10 进制,然后用函数 dec2bin( )将每个文字转化为 16 位二进制。将每个文字的二进制存为矩阵的一行。假设输入文字的个数为 n ,则得到文字信息的二进制流矩阵 $\boldsymbol{D}_{n\times 16}$,其中矩阵的元素为 0 或 1,每一行为一个文字的 16 位二进值编码。

(2)采用文献[1]中改进的 Logistic 映射产生混沌序列,其定义为:

$$x_{n+1} = ax_n(1 - x_n)\bmod 1 \tag{1}$$

其中,a 为分支参数,mod1 表示取小数部分,初值 $x_0 \in (0,1)$ 。文献[1]充分论证了当 $a \geqslant 4$ 时,a 值可以作为密钥,混沌序列无“稳定窗”和空白窗口问题,离散序列在 [0,1] 内处于均匀分布。从式(1)可以看出,该模型是在 Logistic 映射的基础上,扩充了 a 值的范围,当 $a \in (3.57,4]$ 时,产生 Logistic 混沌序列,序列非均匀分布;当 $a \in (4, +\infty)$ 时,产生改进的 Logistic 混沌序列,序列直接进入混沌状态,因此,信息更加安全。

(3)给定初值 x_0, a ,其中 $x_0 \in (0,1)$, $a \in [4, +\infty)$,由式(1)迭代产生 $16n$ 个值,构成 $n \times 16$ 维的行向量 $\boldsymbol{I}$,即:

$$\boldsymbol{I} = (x_1, x_2, \cdots, x_{n\times 16}) \tag{2}$$

(4)利用模 3 同余,将向量 $\boldsymbol{I}$ 中的元素转化为 0 或 1 的二进制数 y_i ,并用元素 y_i 构造 $n \times 16$ 的二进制流矩阵 $\boldsymbol{K}$,方法如下,令:

$$y_i = \begin{cases} 0 & \lceil 10x_i \rceil \equiv 2(\bmod 3) \\ 1 & \text{else} \end{cases} \tag{3}$$

$$\boldsymbol{K} = \begin{pmatrix} y_1 & y_2 & \cdots & y_{16} \\ y_{17} & y_{18} & \cdots & y_{32} \\ \vdots & \vdots & \cdots & \vdots \\ y_{16n-15} & y_{16n-14} & \cdots & y_{16n} \end{pmatrix} \tag{4}$$

其中,符号⌈ ⌉表示实数向上取整, $i = 1,2,\cdots,n \times 16$。

(5)将步骤(1)中矩阵 $\boldsymbol{D}$ 和步骤(4) 中矩阵 $\boldsymbol{K}$ 对元素进行异或运算得到矩阵 $\boldsymbol{H}$,即:

$$\boldsymbol{H} = \boldsymbol{D} \oplus \boldsymbol{K} \tag{5}$$

其中, $\oplus$ 为异或运算符。则矩阵 $\boldsymbol{H}$ 中数据流即为加密的文字信息,此时 $\boldsymbol{H}$ 中每行二进制对应的文字必定跟原文不同。

2 文字隐藏方法

文字隐藏是将加密的文字二进制流矩阵 $\boldsymbol{H}$ 中的数据嵌入到 RGB 格式彩色图像中。为了提高加密信息被统计检测的能力,构造 2 个参数,利用快速傅里叶变换将彩色图像中红色灰度纹理部分提取出来,以红色纹理图像的空间位置为参照,利用改进的 LSB 方法将数据隐藏在图像纹理部分对应的另外两个通道的低两位中,即 LSB 和 LSB+1 中,也就是四个像素存储一个文字的 16 位二进制编码。文字隐藏是在文字加密的基础上进行的,在加密方法步骤(5)之后,过程如下:

(6)给定一幅 $M \times N \times 3$ 的彩色图像 $f(x,y,\lambda)$,λ 为彩色图像三个通道的分量值,当 $\lambda = 1,2,3$ 时,$f(x,y,\lambda)$ 为图像在空间 (x,y) 处红、绿、蓝的灰度值。对于图像红色通道 $f(x,y,1)$,利用二维快速傅里叶变换(FFT)将其转化为频谱图。二维 FFT 变换是二维离散傅里叶变换(DFT)的改进,$f(x,y,1)$ 的 DFT 变换可定义为:

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y,1)\,e^{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)} \tag{6}$$

利用式(6)将红色通道 $f(x,y,1)$ 灰度图像转化为频谱图 $F(u,v)$,然后将低频数据移到区域中心,令:

$$F_1(u,v) = F\left(u - \frac{M}{2}, v - \frac{N}{2}\right) \tag{7}$$

则得到低频位于中心的傅里叶频谱图 $F_1(u,v)$。

(7)给定一个阈值 R,将傅里叶低频部分置为零,得到高频图像。R 为频谱图中点 (u,v) 距频谱中心的半径。设变换后的频谱为 $F_2(u,v)$,对频谱图像建立如图 1 所示的坐标系,则有:

$$F_2(u,v) = \begin{cases} 0 & \sqrt{(u - M/2)^2 + (v - N/2)^2} < R \\ F_1(u,v) & \text{else} \end{cases} \tag{8}$$

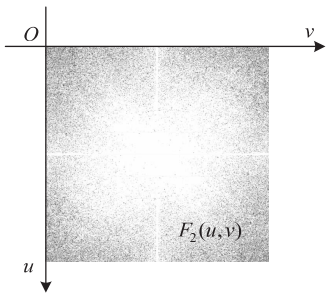


图 1 坐标系

(8)对频谱图 $F_2(u,v)$ 再做一次逆变换(式(7))得到频谱图 $F_3(u,v)$,即:

$$F_3(u,v) = F_2\left(u + \frac{M}{2}, v + \frac{N}{2}\right) \tag{9}$$

(9)对频谱图 $F_3(u,v)$ 做傅里叶逆变换,得到原图 $f(x,y,1)$ 的纹理图像 $f_1(x,y)$。由傅里叶逆变换可知:

$$f_1(x,y) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} F_3(u,v)\,e^{j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)} \tag{10}$$

(10)给定一个阈值 Q,$Q \in [0,40]$,令 $k = 0$,遍历纹理图像 $f_1(x,y)$ 的每个像素,若 $f_1(x,y) > Q$ 则 $k = k + 1$。这样便得到原图像中能隐藏信息的像素个数 k,则图像中能存储的比特位数为 $4 \times k$,存储量取决于图像质量、阈值 R 和 Q。

(11)若 $4 \times (k - 12) < n \times 16$,表示图像存储信息的空间不够,则执行(1)或执行(6),否则,再次遍历纹理图像 $f_1(x,y)$ 中的每个像素,若 $f_1(x,y) > Q$,则将原图像 $f(x,y,2)$ 和 $f(x,y,3)$ 的灰度值的二进制码的低两位替换为 $\boldsymbol{H}$ 中的元素,加密信息矩阵 $\boldsymbol{H}$ 中元素读取的顺序是按行从左到右,若 $f_1(x,y) \leqslant Q$ 则原图像 $f(x,y,2)$ 和 $f(x,y,3)$ 的灰度值不变。

(12)若 $\boldsymbol{H}$ 中数据存储完毕,将满足隐藏条件位置的灰度值二进制码的低两位都替换为 0,直到 12 个像素为止。

3 密图信息提取及解密

密图信息的提取和解密就是隐藏和加密的逆过程。假设载密图像为 $f(x,y,\lambda)$,利用式(6)对其红色通道图像 $f(x,y,1)$ 进行傅里叶变换,然后利用式(7)得到低频位于中心的频谱图,利用阈值 R,将频谱图的低频置零,将高频部分利用式(10)得到纹理图 $f_1(x,y)$,对纹理图像 $f_1(x,y)$,利用阈值 Q,若 $f_1(x,y) > Q$,则对原图像 $f(x,y,2)$ 和 $f(x,y,3)$ 的灰度值的二进制码的低两位进行提取,并构造 $m \times 16$ 的矩阵 $\boldsymbol{H}$。同时记录提取编码个数 n_1 和两通道低两位连续为 00 的像素个数 n_2,当 $n_2 = 12$ 时,停止提取编码。提取文字数量 m 可由下式计算:

$$m = \lceil \frac{n_1}{16} \rceil - 3 \tag{11}$$

其中,$\lceil\ \rceil$ 代表向上取整。得到加密的信息编码矩阵 $\boldsymbol{H}$ 后,利用信息加密的方法构造矩阵 $\boldsymbol{K}$。由式(5)知,若矩阵 $\boldsymbol{K}$ 和 $\boldsymbol{H}$ 已知,不难证明:

$$\boldsymbol{D} = \boldsymbol{H} \oplus \boldsymbol{K} \tag{12}$$

由此得到原信息编码矩阵 $\boldsymbol{D}$。然后将利用函数 bin2dec( ) 和 char( ) 将编码矩阵 $\boldsymbol{D}$ 中每行编码转化文本,即解密出隐藏文本信息。

4 实验结果与分析

实验中,文字加密、隐藏和解密在双核 2.0 GHz CPU,4G 内存的 PC 机和 Win7 系统下利用 MATLAB R2016b 编程实现;信息加密需要使用密钥 a, x_0, R 和 Q 四个值,令:

$$a = 3.58, x_0 = 0.1, R = 20, Q = 0 \quad (13)$$

由上述算法可知,参数 a, x_0 主要影响加密信息的编码方式, R, Q 主要影响信息隐藏的位置。为了说明算法对文字信息的隐藏效果,实验中,隐藏文字选用朱自清散文《荷塘月色》全文,并将其复制 5 遍包括标点符号共计 6 785 个文字分别隐藏到 lena 图、monarch 图、pepper 图和 baboon 图中,给出了原图、载密图和载密位置图,如图 2 所示。其中载密位置图中灰度不等零的位置是所有能载密的位置,上部分突出的白色像素为 6 785 个文字信息的隐藏位置。

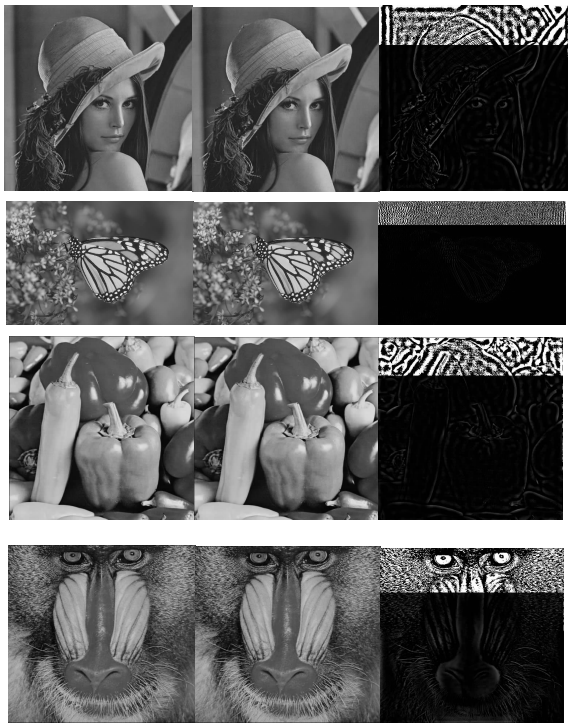


图 2　文本信息隐藏效果图

(从左至右依次是原图、载密图和载密位置图;从上至下依次是 lena 图、monarch 图、pepper 图和 baboon 图)

由于一个文字的信息需要 4 个像素位,因此 6 785 个文字在四张图中隐藏的像素位个数为 27 140。表 1 给出了四张图像的尺寸,最后一个文字在图像中的位置,以及读取 6 785 个文字信息到输出密图的时间。

表 1　信息隐藏的最后位置和时间

图像	尺寸(宽×高)	行位置	列位置	时间/s
lena	512×512	111	143	38.28
monarch	768×512	36	272	38.17
pepper	512×512	109	371	38.17
baboon	500×480	123	227	38.10

从图 2 可以看出,载密图和原图在视觉上无差异,从文字在图像中隐藏的位置可以看出,6 785 个文字信息在图像中隐藏的位置只占用了图像很少的一部分。从表 1 可以计算出 6 785 个文字信息在图像占用的空间,最多是 baboon 图,约 25.6%,最少是 monarch 图,约 7%,隐藏的文字速率约为每秒 178 个文字。数据说明算法可以实现在图像中隐藏大量信息并具有较高的速率。

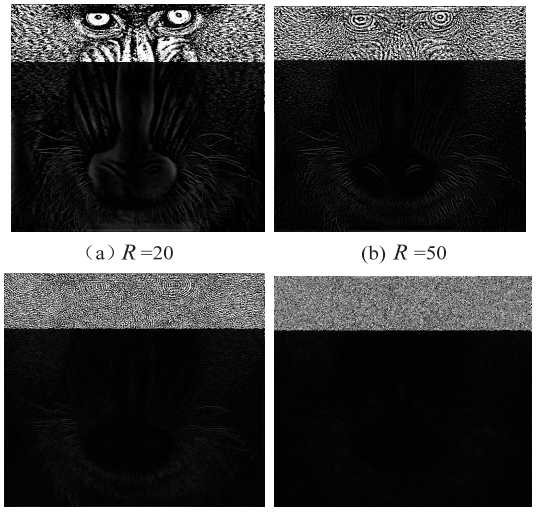
为了说明密图的质量,计算隐藏信息位置和原图位置两灰度通道之间的峰值信噪声比 PSNR,并给出了几组文献对比,如表 2 所示。

表 2　载密图的信噪比(PSNR)

图像隐藏比特位	绿色通道 54 280	蓝色通道 54 280	文献[10] 8 000	文献[11] 8 000	文献[13] 10 000
lena	50.80	50.45	45.24	45.53	59.86
monarch	50.81	50.36	——	——	——
pepper	50.84	50.47	——	——	——
baboon	51.24	51.07	——	——	——

从表 2 可以看出,文中隐藏的方法,即文字隐藏方法(6)至(12)中给出的四个像素嵌入 16 位二进制比特编码的方法,PNSR 值较高,图像可以很好地满足隐蔽性的要求(PSNR>28),载密图能保持很高的图像质量。

为了说明 R 值对信息隐藏位置的影响,对于同一幅 baboon 图像,在式(13)的条件中,其他不变,改变 R 值,给出当 R 为 20,50,100,200 时的信息位置图(突出的白色部分),如图 3 所示。



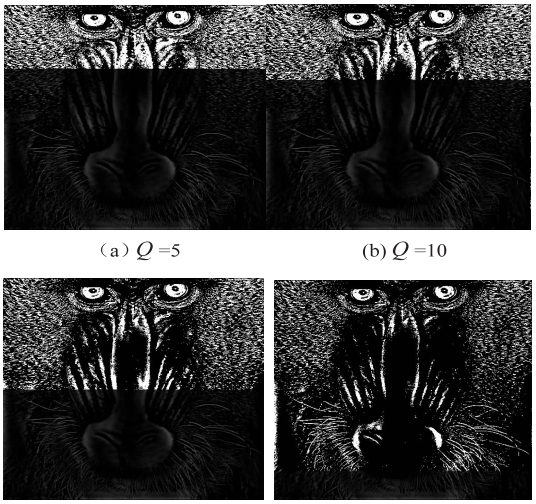
(a) R=20　(b) R=50

(c) R=100　(d) R=200

图 3　R 取不同值时的信息隐藏位置图

从图 3 可以看出,信息在图像中隐藏位置随 R 值的改变而改变,且 R 值越大,隐藏位置在水平方向越分散。

为了说明 Q 值对信息隐藏位置的影响,在式(13)中,其他值不变仅更改 Q 值,给出了当 Q 为 5,10,20,30 时 baboon 图像中信息隐藏的位置图(突出白色部分),如图 4 所示。



(a) Q =5 (b) Q =10

(c) Q =20 (d) Q =30

图 4 Q 取不同值时信息隐藏位置图

从图 4 可以看出,隐藏位置随 Q 的改变而改变,且 Q 值越大,隐藏位置在竖直方向越分散。

为了说明参数 a,x_0 对信息的加密效果,引入书写错误率指标,简记 WER,即 Writing Error Rate,定义如下:

$$\mathrm{WER}=\frac{1}{N}\sum_{t=1}^{N}\begin{cases}1 & g(t)\neq g'(t)\\ 0 & g(t)=g'(t)\end{cases} \tag{14}$$

其中,N 为解密的文字总数,$g(t)$ 和 $g'(t)$ 分别表示原文中第 t 个文字和解密文字中第 t 个文字,N = 6 789。

令 R = 20,Q = 0,a,x_0 取不同值,对图 2 中 lena 图像的密图进行解密,解密的正确文字数,解密错误率(WER)如表 3 所示。

表 3 密钥对应的误码率

x_0 取值	总文字数	正确文字数	WER
a =3.58, x_0 =0.1	6 789	6 789	0
a =3.58, x_0 =0.11	6 789	67	99.01%
a =3.58, x_0 =0.101	6 789	545	91.97%
a =3.58, x_0 =0.100 1	6 789	595	91.23%
a =3.581, x_0 =0.1	6 789	488	92.81%
a =3.580 1, x_0 =0.1	6 789	590	91.3%
a =3.580 01, x_0 =0.1	6 789	573	91.55%

从表 3 可以看出,密钥 a 和 x_0 对解密信息是极其敏感的,万分位的差异,WER 都是 90% 以上,从实际解密出的文字可以看出密码错误时,解密出的文字没有语义信息。

综上实验和分析可知,算法利用四个密钥对信息加密和隐藏,两个密钥影响信息的编码,两个密钥影响隐藏位置,因此,若对密图解密时,没有取得信息隐藏的准确位置,加密信息便无法提取,没有编码的密钥,信息便无法解密,四个密钥缺一不可,一个密钥不正确便无法破解信息。由于密钥都是实数,理论上密钥空间是无穷大,考虑到计算数值是有精度的,若密钥采用 15 位有效数字的双精度实数表示,由于一个实数的可能性为 10^{15} 个,则四个参数构成的密钥空间有 $10^{15}\times10^{15}\times10^{15}\times10^{15}=10^{60}$ 个元素,因此密钥空间足够大,信息安全性有了保障。另外,由于隐藏位置是由两个密钥通过傅里叶变换生成的,从实验中可以看出,这些位置呈现出随机性,它随两个密钥和载体图像的不同而不同,密图具有防检测性。因此,该方法在隐秘信息传输领域,如军事、财务等领域有现实意义。

5 结束语

针对文本传输的安全问题,该文提出一种在彩色图像中加密和隐藏文字的方法。提出了构造 2 个参数生成混沌序列加密文字 Unicode 编码,然后构造 2 个参数,对彩色图像的一个通道进行快速傅里叶变换,生成图像的隐藏位置,根据隐藏位置,利用改进的 LSB 算法将文字编码隐藏到图像另外两个通道。通过实验和分析证明,通过该算法能在彩色图像中隐藏大量文字,生成的密图有很高的图像质量,PSNR 约为 50 dB,密钥空间为 10^{60}。信息隐藏到图像以后具有防检测和抵御穷举攻击的能力,有效提高了文字信息隐秘传输的安全性。

参考文献:

[1] 谢建全,谢 勋,阳春华,等. 基于 Logistic 映射的加密算法的安全性分析与改进[J]. 小型微型计算机系统,2010,31(6):1073-1076.

[2] 官国荣,吴成茂,贾 倩. 一种改进 Lorenz 混沌系统构造及其加密应用[J]. 小型微型计算机系统,2015,36(4):830-835.

[3] 朱和贵,蒲宝明,朱志良,等. 二维 Sine-Tent 超混沌映射及其在图像加密中的应用[J]. 小型微型计算机系统,2019,40(7):1510-1518.

[4] KE Y,ZHANG M Q,LIU J,et al. A multilevel reversible data hiding scheme in encrypted domain based on LWE[J]. Journal of Visual Communication and Image Representation,2018,54:133-144.

[5] YONG Z H. The fast image encryption algorithm based on lifting scheme and chaos[J]. Information Sciences,2020,520:177-194.

[6] MANSOURI A,WANG X Y. A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme[J]. Information Sciences,2020,520:46-62

[7] NI Z C,SHI Y Q,ANSARI N,et al. Reversible data hiding[J]. IEEE Transactions on Circuits Systems for Video Technology,2006,16(3):354-362.

[8] NISSAR A, MIR A H. Classification of steganalysis tech-

(下转第 136 页)