计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190100051

基于快速置换和可选择像素扩散的医疗图像加密算法的安全性分析

禹 峰 龚馨慧 王世红
北京邮电大学理学院 北京 100876
(feng_yu@bupt.edu.cn)

摘 要 图像加密算法的安全性是最基本和最重要的。医疗图像加密是保护患者隐私的一种手段,分析医疗图像加密算法的安全性,对设计医疗图像加密算法、增强算法的安全性和促进医疗图像加密算法的应用非具有常重要的意义。最近,Hua等提出了一种基于快速置换和可选择像素扩散的医疗图像加密方案。加密方案的一个关键操作是在图像的四周插入随机值,然后通过置乱使得随机值分散到整幅图像,最后通过扩散混乱等操作加密整幅图像。每次加密都会产生不同的随机值,即使加密相同的图像,每次加密得到的密文也不一样,这就保证了"一次一密"的加密效果。文中采用差分分析和选择密文攻击,从理论上详细地分析了Hua等提出的算法。首先分析解密过程,通过差分分析构造明文-密文的线性关系,并根据构造的线性关系建立密码本;然后使用密码本攻击便可破解该算法。密码本的大小与图像尺寸相关,若密文图像的尺寸为$M\times N$,则构造的密码本包含$(M\times N+1)$个明文-密文对。仿真实验验证了理论分析的正确性。为了提高该算法的安全性,抵抗文中提出的密码本攻击,进一步提出了一种基于差分分析的改进方案。该方案引入了与明文相关的置换矩阵。仿真实验结果和统计分析结果表明,改进方案不仅继承了原算法的优点,而且具有很好的抗差分攻击能力。

关键词:医疗图像;图像加密;混沌加密;差分分析;密码本攻击
中图法分类号 TP391

Cryptanalysis of Medical Image Encryption Algorithm Using High-speed Scrambling and Pixel Adaptive Diffusion

YU Feng,GONG Xin-hui and WANG Shi-hong
School of Science,Beijing University of Posts and Telecommunications,Beijing 100876,China

Abstract Security is essential and important for every image encryption algorithm. Medical image encryption is a means to protect patients' privacy. Analyzing the security of medical image encryption algorithm is very meaningful for the design of medical image encryption algorithm,enhancing the security of algorithm and promoting the application of medical image encryption algorithm. Recently,Hua et al. proposed a medical image encryption algorithm using high-speed scrambling and pixel adaptive diffusion. The key operation of the scheme is insertion of a random sequence around an image,then the random values are dispersed to the whole image by scrambling,finally,the whole image is scrambled by diffusion. Because different random values are generated in each encryption,even for one unchanged image,the cipher-image is different in every encryption such that Hua et al's scheme is similar to one time one pad system. In this paper,the security of the algorithm was analyzed by differential cryptanalysis and chosen ciphertext attack in detail. The decryption process is analyzed theoretically by differential cryptanalysis and linear relationship is constructed between plain-images and cipher-images. Based on the linear relationship,a codebook is established,and the codebook attack breaks Hua et al's algorithm. The size of the codebook is determined by the size of the cipher-image. If the size of the cipher-image is,the constructed codebook contains pairs of plain-image/cipher-image. The experimental results verify the theoretical analysis. To improve the security of Hua et al's algorithm and to resist the differential cryptanalysis,an improved scheme was proposed. In the improved scheme,plaintext-related permutation matrices are introduced. The simulation and statistical results show that the improved scheme not only inherits the advantages of the original algorithm,but also resist the differential cryptanalysis and the codebook attack.

Keywords Medical image,Image encryption,Chaotic encryption,Differential cryptanalysis,Codebook attack

到稿日期:2019-01-07 返修日期:2019-04-15 本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
通信作者:王世红(shwang@bupt.edu.cn)

1　引言

随着计算机网络和通信技术的飞速发展，世界已经进入信息时代，因此保护开放网络环境下的信息传输和存储成为了当前的热门话题。信息安全的复杂性和密码分析能力的增强，迫使人们需要研究更加安全有效的加密算法。由于混沌具有伪随机、遍历、对初始值和控制参数敏感等特性，自 Matthews[1] 提出基于混沌的加密方案以来，基于混沌的密码研究就逐渐发展成为了密码学的一个新分支。继 Fridrich[2] 在图像加密中应用置乱-扩散结构之后，图像加密研究便得到了广泛关注[3-4]。研究者提出了多种基于混沌的图像加密方案，包括改进扩散方案[5]、不同的密钥流生成方法[6]、比特级置乱算法[7]、与明文相关的置乱等[8]。然而，一些方案被证明是不安全的。Li 等[9] 首次指出对于置乱扩散的图像加密方案，密码分析的目标是重建置换矩阵。他们提出任何只有置换的图像加密方法都无法抵抗已知/选择明文攻击，破解只需 $O(\mathrm{Log}_L(M\times N))$ 张已知/选择的明文图像，其中 $M\times N$ 是图像的大小，L 是像素值的数目。Li 等[10] 破解了只有扩散的图像加密方案，破解该方案只需要一张或两张已知的明文图像。Solak 等[11] 用选择密文攻击破解了多轮加密的 Fridrich 算法，但此分析方法不适用于有足够轮数的方案。Fu 等提出的基于混沌的医疗图像加密方案[12] 和 Zhou 等提出的多轮置换扩散加密系统[13] 也分别在 2015 年[14] 和 2016 年[15] 被 Chen 等破解。

近日，Hua 等提出了一种使用快速置换和可选择像素扩散的医疗图像加密算法[16]，并指出该算法具有较高的安全性和很好的抵抗差分攻击的能力。然而，我们发现该方案也是不安全的。通过差分分析，我们构造了密文和明文间的线性关系，并基于此使用密码本攻击破解了该加密系统。

2　本文算法描述

图 1 为基于快速置换和可选择像素扩散的医疗图像的加密算法（本文称为原算法），解密过程是加密的逆过程。

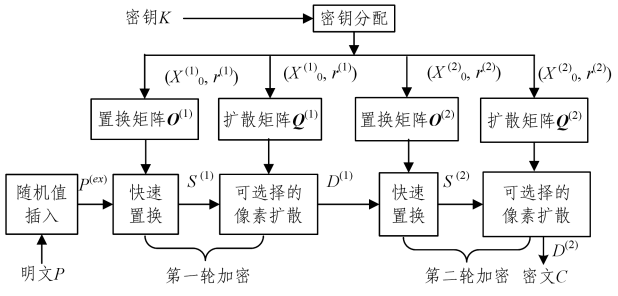


图 1　原算法的加密过程

Fig. 1　Encryption process of Hua et al's original algorithm

加密过程分为 3 个模块：随机值插入、第一轮加密和第二轮加密。两轮加密都由快速置换和可选择像素扩散构成。图中 P 是明文；$P^{(ex)}$，$S^{(1)}$，$D^{(1)}$，$S^{(2)}$ 和 $D^{(2)}$ 分别为随机值插入、第一轮置换和扩散、第二轮置换和扩散后的图像；输出的密文为 C，$C=D^{(2)}$。子密钥 $(X_0^{(i)}, r^{(i)}, i=1,2)$ 用于控制两轮加密过程中的置乱矩阵 $\boldsymbol{O}$ 和扩散矩阵 $\boldsymbol{Q}$ 的生成（见图 1）。本文中，大写字母代表图像，小写字母代表像素值或者矩阵中的一个元素，例如，P 代表明文图像，$p(x,y)$ 代表坐标为 (x,y) 的像素值。置乱矩阵 $\boldsymbol{O}$ 和扩散矩阵 $\boldsymbol{Q}$ 的生成可以参考原算法[16]。

1）随机值插入。给定一幅明文 P，假设明文的尺寸为 $(M-1)\times(N-1)$，在明文 P 的四周加上一圈随机值，随机值的数据类型与明文 P 相同。明文扩展为 $P^{(ex)}$，尺寸变为 $M\times N$。每次加密的随机值都不相同，即使用相同的密钥加密同一张图像，得到的密文也不相同，因此该过程可以近似看成“一次一密”。

2）快速置换。快速置换可以快速打乱图像像素位置，因此能够减弱相邻像素间的强相关性。子密钥 $(X_0^{(i)}, r_i)(i=1,2)$ 控制生成置换矩阵 $\boldsymbol{O}$，通过置换矩阵 $\boldsymbol{O}$ 将 $P^{(ex)}$ 进行全局置换。

3）可选择像素扩散。为了适应不同的软硬件环境，扩散采用不同的操作，称之为可选择像素扩散。原算法按列、以“И”字形顺序对像素进行扩散。面对软件环境，采用异或操作，扩散操作为：

$$c(i,j)=\begin{cases} s(i,j)\oplus s(M,N)\oplus Q(i,j), & i=1,j=1\\ s(i,j)\oplus c(M,j-1)\oplus Q(i,j), & i=1,j\neq 1\\ s(i,j)\oplus c(i-1,j)\oplus Q(i,j), & i\neq 1 \end{cases} \tag{1}$$

扩散操作的逆过程为：

$$s(i,j)=\begin{cases} c(i,j)\oplus s(M,N)\oplus Q(i,j), & i=1,j=1\\ c(i,j)\oplus c(M,j-1)\oplus Q(i,j), & i=1,j\neq 1\\ c(i,j)\oplus c(i-1,j)\oplus Q(i,j), & i\neq 1 \end{cases} \tag{2}$$

面对硬件环境，采用模加操作，扩散操作为：

$$c(i,j)=\begin{cases} (s(i,j)+s(M,N)+Q(i,j)) \bmod F, & i=1,j=1\\ (s(i,j)+c(M,j-1)+Q(i,j)) \bmod F, & i=1,j\neq 1\\ (s(i,j)+c(i-1,j)+Q(i,j)) \bmod F, & i\neq 1 \end{cases} \tag{3}$$

扩散操作的逆过程为：

$$s(i,j)=\begin{cases} (c(i,j)-s(M,N)-Q(i,j)) \bmod F, & i=1,j=1\\ (c(i,j)-c(M,j-1)-Q(i,j)) \bmod F, & i=1,j\neq 1\\ (c(i,j)-c(i-1,j)-Q(i,j)) \bmod F, & i\neq 1 \end{cases} \tag{4}$$

其中，F 为图像的灰度级别。例如，像素值为 8 比特的图像，$F=256$。

3　预备知识

命题 1　定义 $E(a_i)=(a_i+q) \bmod F(i=0,1,2)$，则有差分满足下列等式：$E((a_1+a_2-a_0) \bmod F)=(E(a_1)+E(a_2)-$

$E(a_0))\bmod F$。

证明：$E((a_1+a_2-a_0)\bmod F)$

$=(a_1+a_2-a_0+q)\bmod F$

$=((a_1+q)+(a_2+q)-(a_0+q))\bmod F$

$=(E(a_1)+E(a_2)+E(a_0))\bmod F$

命题 2 根据命题 1，可以构造一个更一般的差分，其满足下列等式：$E((\sum_{i=1}^{n}a_i-(n-1)a_0)\bmod F)=(\sum_{i=1}^{n}E(a_i)-(n-1)E(a_0))\bmod F$。

证明：$E((\sum_{i=1}^{n}a_i-(n-1)\ a_0)\bmod F)$

$=(\sum_{i=1}^{n}a_i-(n-1)\ a_0+q)\bmod F$

$=(\sum_{i=1}^{n}(a_i+q)-(n-1)(a_0+q))\bmod F$

$=(\sum_{i=1}^{n}E(a_i)-(n-1)E(a_0))\bmod F$

将命题 1 和命题 2 中的模加操作替换为异或操作，命题 1 和命题 2 仍然成立。

4 原算法分析

本节将通过差分分析从理论上构造原算法解密操作的线性关系，并给出灰度图像的仿真结果，以验证理论分析的正确性。

4.1 解密过程的差分分析

任意选取 3 张密文图像 C_i，$i=1,2,3$。输入密文 C_i，解密是加密的逆过程（见图 1）。经过扩散逆过程、置换逆过程和去掉随机值后的输出图像分别为 $D_i^{(2)}$，$S_i^{(1)}$，$D_i^{(1)}$，$P_i^{(ex)}$，P_i。由于两轮解密操作相同，因此本文只讨论扩散逆过程、置换逆过程和去掉随机值过程。

1）扩散逆过程。由于矩阵 $\boldsymbol{Q}$ 的存在，根据命题 1，我们选择 3 张密文图像进行差分分析。这里仅分析模加（硬件）操作，其对异或（软件）操作也是可行的。构造差分密文图像为：

$$\Delta C=(C_1+C_2-C_3)\bmod F \tag{5}$$

差分 ΔC 的扩散逆过程定义为：$Dec_d(\Delta C)=\Delta S$。由式(5)和命题 1 可以得到 3 张图像的差分表达式为：

$$Dec_d((C_1+C_2-C_3)\bmod F)=(S_1+S_2-S_3)\bmod F \tag{6}$$

式(6)表明，通过 3 张图像，可以构造一个扩散逆过程的差分线性等式。

2）置换逆过程。假设 $P_i^{(ex)}$ 图像在 (x,y) 处的像素值通过置换被映射到图像 S_i 的 (x_1,y_1) 处，则该逆过程可以表示为：

$$Dec_s(s_i(x_1,y_1))=p_i^{(ex)}(x,y) \tag{7}$$

根据置换操作的特点，即置换操作只改变像素的位置，不改变像素值，可以构造下列差分等式：

$$Dec_s((S_1+S_2-S_3)\bmod F)=(P_1^{(ex)}+P_2^{(ex)}-P_3^{(ex)})\bmod F \tag{8}$$

式(8)表明，通过 3 张图像，可以构造一个置换逆过程的差分线性等式。

3）随机值插入逆过程。在加密过程中，使用相同密钥加密同一张图像时，随机值的插入使得同一幅图像在每次加密后输出的密文图像都不同，因此加密过程可以近似于“一次一密”。我们定义随机值插入过程为 $E_r(P_i,r_i)=P_i^{(ex)}$，其中 r_i 为插入的随机值。由于每次插入的随机值都不相同，可以得到 $(E_r(P_1,r_1)+E_r(P_2,r_2)-E_r(P_3,r_3))=(P_1^{(ex)}+P_2^{(ex)}-P_3^{(ex)})\bmod F\neq E_r((P_1+P_2-P_3)\bmod F,r)$。但在解密过程中，通过扩散逆过程 Dec_d 和置换逆过程 Dec_s 可以得到扩展图像 $P^{(ex)}$，去掉四周的随机值即可恢复唯一对应的原图 P。我们定义去掉四周随机值的操作为 $Dec_r(P_i^{(ex)},r_i)=P_i$，则可以得到：

$$Dec_r((P_1^{(ex)}+P_2^{(ex)}-P_3^{(ex)})\bmod F,r)=(P_1+P_2-P_3)\bmod F \tag{9}$$

式(9)表明，通过 3 张图像，可以构造一个随机值插入逆过程的差分线性等式。

综合 1）—3）可知整个解密过程。通过 3 张图像 C_0，C_1，C_2，可以构建扩散逆过程的差分线性等式(6)、置换逆过程的差分线性等式(8)和随机值插入逆过程的差分线性等式(9)。考虑整个解密过程，通过随机值插入逆过程、两轮逆扩散和两轮逆置乱，可以得到如下的密文和明文差分线性等式：

$$Dec_r(Dec_s(Dec_d(Dec_s(Dec_d((C_1+C_2-C_3)\bmod F)))))=(P_1+P_2-P_3)\bmod F \tag{10}$$

4.2 差分仿真结果

本节将通过仿真验证密文和明文差分线性等式(10)。如图 2 所示，选择 3 张密文图像 C_1，C_2 和 C_0，其中 C_1，C_2 是像素值为 8 比特的医疗图像对应的密文，C_0 为全零图像对应的密文，尺寸都为 512×512 像素。使用原算法对 C_1，C_2，C_0 进行解密，得到对应的明文图像 P_1，P_2，P_0。为了验证差分等式(10)，计算密文的差分图像 $\Delta C=(C_1+C_2-C_0)\bmod F$，然后对其解密。密文 ΔC 对应的明文为 ΔP。通过计算 3 张明文的差分 $\Delta P'=(P_1+P_2-P_0)\bmod F$，比较 $\Delta P'$ 和 ΔP，可以发现 $\Delta P'=\Delta P$。仿真结果证实了本文的理论分析，即对于任意 3 对密文/明文图像，可以构造密文与明文之间的线性差分关系（式(10)）。

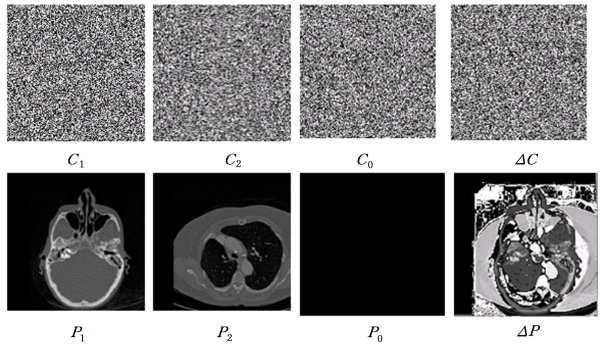


图 2 线性差分关系式(10)的仿真结果

Fig. 2 Simulation results of equation (10)

5 密码本攻击

本节将任意 3 对密文/明文图像之间的线性差分关系推

广到多对密文/明文之间的差分关系，从而方便我们构造密码本，然后使用密码本破解 Hua 等设计的图像加密系统。这里主要对原算法的硬件加密方案（软件加密方案类似）进行分析和仿真。

5.1　理论分析

假设密文的尺寸为 $M\times N$，像素值为$[0,F)$。选择一张全零图像 C_0 和 $M\times N$ 张只有一个非零像素值的密文图像，非零像素值 $c(i,j)=1,i=1,2,\cdots,M,j=1,2,\cdots,N$。将这些图像输入解密机，可以得到对应的密文/明文对 C_n 和 P_n，$n=0,1,2,\cdots,M\times N$。这些密文/明文对将构成密码本，可用于破解任何密文图像。

对于任意的密文图像 C，现将其转换为如下形式：

$$C=\sum_{n=1}^{M\times N}k_n\cdot C_n \tag{11}$$

其中，$k_n\in[0,F)$。

对式(11)进行进一步变换，得：

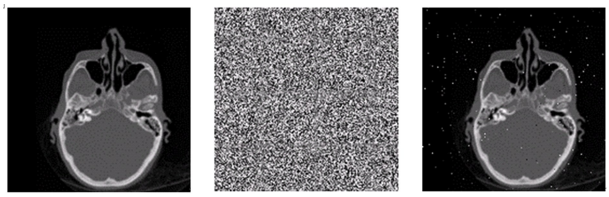
$$C=\sum_{n=1}^{M\times N}k_n\cdot C_n-\left(\sum_{n=1}^{M\times N}k_n-1\right)\cdot C_0 \tag{12}$$

根据式(10)的差分关系和命题 2，可以得出密文图像 C 恢复的明文表达式为：

$$P=\sum_{n=1}^{M\times N}k_n\cdot P_n-\left(\sum_{n=1}^{M\times N}k_n-1\right)\cdot P_0 \bmod F \tag{13}$$

5.2　仿真结果

为了不失一般性，本节选择大小为 64×64 像素、灰度级为 8 比特的图像作为示例展示密码本攻击。选择一张全零图像和 64×64 张只有一个非零像素值 1 的图像。通过解密机，构造了 64×64+1 个密文/明文图像对的密码本。给定一个密文图像，根据式(12)和式(13)，能够成功地恢复原始图像。图 3(a)是原始的医疗图像，图 3(b)和图 3(c)分别是密文图像和由密码本分析恢复的明文图像。本文的仿真结果验证了密码本攻击的正确性。



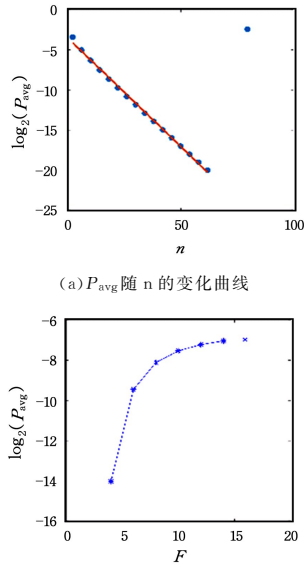
(a)原始图像　(b)加密图像　(c)恢复图像

图 3　密码本攻击结果

Fig. 3　Results of codebook attack

6　算法改进

由于原算法的加密过程仅与密钥相关，且可以通过差分分析构造线性关系，为了提高原算法的抗差分和抵抗密码本攻击的能力，本文引入了与明文相关的置换矩阵 $\boldsymbol{O}$。本文在图像进行置换操作前对其求像素平均值，并使用像素平均值更新置换操作的子密钥$(X_0^{(1)},r^{(1)})$和$(X_0^{(2)},r^{(2)})$，生成与明文相关的置换矩阵 $\boldsymbol{O}^{(1)}$ 和 $\boldsymbol{O}^{(2)}$。与明文相关的置换矩阵 $\boldsymbol{O}^{(1)}$ 和 $\boldsymbol{O}^{(2)}$ 的引入使得密码本无法构造，从而导致密码本攻击失效。但不同的随机图像的像素平均值会在$(F-1)/2$ 上下波动，存在一定的概率 P_{avg} 使得图像像素平均值相同，这将导致式(8)和式(10)的线性关系仍可构造。求解像素平均值相等的概率 P_{avg}，可以等价为求解不定方程整数解个数的问题，即对于 n 个未知数 x_i，其中 $x_i\in[0,F)$，且 $\sum_1^n x_i=sum$，求 $sum=n*(F-1)/2$ 时解的个数。本文使用递归算法进行数值求解，图 4 分别给出了 P_{avg} 随 n，F 变化的曲线。n 一定时，随着 F 的增加，P_{avg} 趋于饱和；F 一定时，P_{avg} 随 n 的增大呈指数减小，拟合曲线 $P_{\text{avg}}\propto 2^{-0.2674n}$。由图 4 可以看到，选取 3 张尺寸为 13×13 像素的灰度图像，构造满足式(8)和式(10)的难度约为 2^{135}。这表明通过选取相同像素平均值的图像构造差分等式(10)是不可能的，因此本文的改进算法具有很强的抗差分能力。



(a)P_{avg}随 n 的变化曲线

(b)P_{avg}随 F 的变化曲线

图 4　P_{avg}随 n 和 F 的变化曲线

Fig. 4　Dependence of on P_{avg} on n and F

本文使用改进方案解密图 2 中的 4 张图像 C_1，C_2，C_0 和 $\Delta C=(C_1+C_2-C_0) \bmod F$，获得的对应明文图像分别为 P_1，P_2，P_0 和 $P_{\Delta C}$。计算差分图像 $\Delta P=(P_1+P_2-P_0) \bmod F$，得到 $\Delta P\neq P_{\Delta C}$，且 $\Delta P'=\Delta P-P_{\Delta C} \bmod F$ 具有良好的随机性。

本文继续使用 National Institute of Standards an Technology (NIST) SP800-22 Statistical Test Suite[17-18] 对改进方案进行统计性测试，其中有效值 α 设置为 0.01，二进制序列的长度 s 设置为 $M\times N\times L$，其中 L 为比特数。本文从 BOWS-2 数据库中选取了 120 张大小为 512×512 像素的图像，使用改进方案进行加密，并将得到的密文分解为二进制序列。实验结果表明，使用改进方案加密得到的 120 张密文均通过了 15 个子测试项。

结束语　本文分析了一种使用快速置换和可选择像素扩散的医疗图像加密方案。虽然原算法的加密过程为非线性，但本文通过差分分析构造了密文/明文的线性关系，并利用线性关系构建密码本，只需要$(M\times N+1)$对密文/明文便可以破解加密系统。为了抵抗差分分析和密码本攻击，本文提出

了改进措施，在原算法的基础上引入与明文相关的扩散矩阵，使得加密过程不只受密钥控制，还与明文相关，提高了算法的抗差分攻击能力。图像加密的安全性分析，不仅能够评估算法本身的安全性，还对算法的设计有着重要的指导意义。

参 考 文 献

[1] ROBERT A M. On the derivation of a "chaotic" encryption algorithm[J]. Cryptologia, 1989, 13(1): 29-42.

[2] FRIDRICH J. Image encryption based on chaotic maps [C]// IEEE International Conference on Systems. IEEE, 1997.

[3] CHAI X, ZHENG X, GAN Z, et al. An image encryption algorithm based on chaotic system and compressive sensing[J]. Signal Processing, 2018, 148: 124-144.

[4] CHEN J, ZHU Z L, ZHANG L B, et al. Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption[J]. Signal Processing, 2018, 142: 340-353.

[5] ZHANG L Y, LIU Y, WONG K W, et al. On the security of a class of diffusion mechanisms for image encryption[J]. IEEE Transactions on Cybernetics, 2017, PP(99): 1-13.

[6] QIWEN R, LING W, JING M, et al. A quantum color image encryption scheme based on coupled hyper-chaotic Lorenz system with three impulse injections[J]. Quantum Information Processing, 2018, 17(8): 188.

[7] CAO C, SUN K, LIU W. A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map[J]. Signal Processing, 2017, 143: 122-133.

[8] CHEN J, ZHU Z L, ZHANG L B, et al. Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption[J]. Signal Processing, 2018, 142: 340-353.

[9] LI S, LI C, CHEN G, et al. A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks [J]. Signal Processing: Image Communication, 2008, 23(3): 212-223.

[10] LI C Q, LIU Y S, XIE T, et al. Breaking a novel image encryption scheme based on improved hyperchaotic sequences[J]. Nonlinear Dynamics, 2013, 73(3): 2083-2089.

[11] SOLAK E, COKAL C, YILDID O T, et al. Cryptanalysis of fridrich's chaotic image encryption[J]. International Journal of Bifurcation & Chaos, 2010, 20: 1405-1413.

[12] FU C, MENG W, ZHAN Y, et al. An efficient and secure medical image protection scheme based on chaotic maps[J]. Computers in Biology & Medicine, 2013, 43(8): 1000-1010.

[13] ZHOU G, ZHANG D, LIU Y, et al. A novel image encryption algorithm based on chaos and Line map[J]. Neurocomputing, 2015, 169: 150-157.

[14] CHEN L, WANG S H. Differential cryptanalysis of a medical image cryptosystem with multiple rounds[M]. British: Pergamon Press, 2015.

[15] CHEN L, MA B, ZHAO X, et al. Differential cryptanalysis of a novel image encryption algorithm based on chaos and Line map [J]. Nonlinear Dynamics, 2016, 87(3): 1-11.

[16] HUA Z Y, YI S, ZHOU Y C. Medical image encryption using high-speed scrambling and pixel adaptive diffusion[J]. Signal Processing, 2017, 144: 134-144.

[17] RUKHIN A L, SOTO J, NECHVATAL J R, et al. SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications[J]. Applied Physics Letters, 2010, 22(7): 1645-1796.

[18] PARESCHI F, ROVATTI R, SETTI G. On Statistical Tests for Randomness Included in the NIST SP800-22 Test Suite and Based on the Binomial Distribution[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 491-505.

YU Feng, born in 1993, postgraduate. His main research interests include chaotic encryption.

WANG Shi-hong, born in 1966, Ph. D, professor. Her main research interests include chaotic encryption