考虑隐私信息安全性的极少样本条件指纹图像细节加密算法

刘展鹏，马振超

（中国人民公安大学 国家安全学院，北京 100038）

摘　要：为保证指纹信息的安全性和隐私性，提出了一种考虑隐私信息安全性的极少样本条件指纹图像细节加密算法。在极少数样本条件下，通过四方定理的分块原则，将指纹明文图像分为多个正方形图像块，以组建置乱所需的幻方矩阵。将各矩阵展开置乱处理后，再展开拼接和转置等操作，充分扩散全部像素，使其还原为原始指纹图像大小，经过多次置乱得到预加密后的指纹图像。将明文图像组成指纹图像立方体，通过明文图像的哈希值和外部参数形成初始密钥，将其代入混沌系统形成所需序列。利用混沌序列形成掩膜和规则矩阵，对掩膜矩阵和置乱结果展开动态DNA编码。同时通过规则矩阵对编码后的图像立方体和掩膜矩阵展开DNA运算，经过DNA动态解码即可获取最终的指纹图像细节加密图像。实验结果表明：本文算法可以更加高效地保证在极少样本条件下指纹图像的隐私信息安全性。

关键词：考虑隐私信息安全性；极少样本条件；指纹图像；细节加密

中图分类号：TP309　　**文献标志码**：A　　**文章编号**：1671-5497(2025)02-0687-06

DOI：10.13229/j.cnki.jdxbgxb.20231450

A few sample condition fingerprint image detail encryption algorithm considering privacy information security

LIU Zhan-peng，MA Zhen-chao

（*National Security Academy*，*Chinese People's Public Security University*，*Beijing* 100038，*China*）

Abstract：To ensure the security and privacy of fingerprint information，a very few sample conditional fingerprint image detail encryption algorithm considering privacy information security is proposed. Under extremely few sample conditions，the fingerprint plaintext image is divided into multiple square image blocks using the block principle of the square theorem to construct the magic square matrix required for scrambling. After unfolding and scrambling each matrix，operations such as stitching and transposing are carried out to fully diffuse all pixels and restore them to the original fingerprint image size. After multiple scrambling operations，the pre encrypted fingerprint image is obtained. Compose a fingerprint image cube from plaintext images，form an initial key through the hash value and external parameters of the plaintext image，and substitute it into a chaotic system to form the desired sequence. Using chaotic sequences to form masks and rule matrices，dynamic DNA encoding is performed on the mask matrix and scrambling

收稿日期：2023-12-28.

基金项目：国家社会科学基金重大项目(22ZDZA122).

作者简介：刘展鹏(1985-)，男，博士研究生.研究方向：国家安全.E-mail：liuzhanpeng20232@163.com

results. At the same time, DNA operations are performed on the encoded image cube and mask matrix through a rule matrix, and the final encrypted fingerprint image details can be obtained through DNA dynamic decoding. The experimental results show that the proposed algorithm can more efficiently ensure the privacy information security of fingerprint images under very few sample conditions.

Key words: consider privacy information security; very few sample conditions; fingerprint images; detail encryption

0 引 言

在当今的数字时代,信息隐私和安全性已经成为一项基本人权,同时也是企业和政府机构关注的核心。尤其是生物识别领域,例如指纹识别等,信息安全的重要性不言而喻。在现实应用中,会出现训练样本极少的情况,给传统的机器学习加密算法带来了全新的挑战。尤其是在样本数量十分稀少的情况下,如何实现指纹图像的高效加密[1,2]成为当前研究的热点话题。

王佳等[3]优先将图像划分为多个规格相同的图像子块,生成混沌相位模板和混沌振幅模板,将子图像和混沌相位模板展开混沌卷积,然后采用混沌振幅模板展开混沌下采样,得到压缩加密后的图像子块,最终将加密处理后的图像子块复原为最终的加密图像;李春彪等[4]将正弦反馈加入经典Logistic映射中,获取全新映射关系,混沌映射经过推导获取离散混沌加密序列,对加密序列展开放大取整。同时将伪随机序列和原始图像展开异或计算,最终实现图像加密处理[5],通过动态密钥更新方案摆脱一次一密的密钥系统,对三维循环移位置乱方法展开改进;然后通过混沌序列动态选择DNA编码规则和编码顺序,在上述基础上将图像矩阵逐像素动态交错编码为DNA序列,将编码后的DNA序列和给定序列展开碱基运算,最终实现图像加密处理。在以上几种加密算法的基础上,提出一种考虑隐私信息安全性的极少样本条件指纹图像细节加密算法。实验结果表明:本文算法可以更好地保护指纹图像细节信息的安全性。

1 算 法

1.1 考虑隐私信息安全性的极少样本条件指纹图像预加密

基于四方定理和幻方的矩形图像置乱方法的基本思想为:在极少样本条件下,将指纹图像划分为4个正方形图,对各图像块展开幻方置乱和拼接等操作,同时将图像恢复为原始指纹图像大小。

采用四方定理可以将一个自然数分解为4个自然数的方差和。因此,将四方定理应用于图像分块处理,可以优先将像素总数展开分解,然后选取对应数量的像素,最终实现分块处理。

考虑到不同幻方生成方法的差异性,分别采用不同的方式形成不同的幻方。使用幻方置乱主要存在以下问题:无法对高度和宽度不相等的矩形展开处理,同时置乱参数也比较少,算法的安全性能也比较低。为了有效增强置乱效果,可以将幻方置乱和其他方法有效结合。

设定灰度图像大小为$n\times n$,将其表示为$P_{n\times n}$,传统的幻方置乱方法是将图像$P_{n\times n}$和n阶方B的行列相互对应,按照式(1)展开变换,获取$B(a_{ij})$:

$$B(a_{ij})=\begin{cases}n^2, (a_{ij}+1)\bmod n^2=0\\ a_{ij}+1 \bmod n^2, \text{其他}\end{cases} \tag{1}$$

式中:a_{ij}为变换矩阵中的元素。

结合上述分析,提出一种四分块幻方置乱FMSS算法,设定原始指纹图像大小为$N\times M$,对图像分块处理后,再对各个指纹图像块展开幻方置乱处理,再将块拼接恢复成$N\times M$的图像。其中,常用的置乱方法有:

(1)完成分块处理后直接展开置乱拼接处理。

(2)在图像块置乱[6,7]后,经过拼接形成原始图像,对其展开转置处理并且改变图像形状,然后将其恢复至原始指纹图像大小;最后对各分块展开置乱处理。

通过对以上两种方法的分析,需要利用方法(2)重复展开置乱处理,直至达到设定的置乱次数则终止操作,同时输出置乱处理后的指纹图像。在以上操作过程中需要特别注意一个问题,当前变化形状得到的指纹图像和前期转置的指纹图像存在十分明显的差异,将形状变化表示为以下形式:

$$H=\begin{pmatrix}1&2&3\\4&5&6\end{pmatrix}\rightarrow\begin{pmatrix}1&4\\2&5\\3&6\end{pmatrix}\rightarrow\begin{pmatrix}1&3&5\\2&4&6\end{pmatrix} \tag{2}$$

在极少数样本条件下,采用四方块幻方置乱方法对指纹图像展开预加密处理,操作步骤如下:

(1)通过输入指纹图像尺寸,利用四方定理将指纹图像划分为4个正方形块(I_1, I_2, I_3, I_4)。

(2)利用正方形指纹图像尺寸,通过幻方生成算法组成幻方矩阵组合$\boldsymbol{S}$,如式(3)所示:

$$\boldsymbol{S}=(S_1, S_2, S_3, S_4) \tag{3}$$

(3)采用(S_1, S_2, S_3, S_4)依次对各个指纹图像块展开幻方置乱处理,得到置乱图像块(I_1', I_2', I_3', I_4')。

(4)将(I_1', I_2', I_3', I_4')按照事先设定好的顺序展开拼接处理,即可获取尺寸为$N\times M$的图像U_1,再将U_1转置处理后得到$N\times M$的图像U_2,最后变化形状得到大小为$N\times M$的一次置乱指纹图像U_3。

(5)假设当前置乱次数少于设定的迭代次数,则继续执行以上操作步骤。

(6)最终输出置乱处理后的指纹图像,在考虑隐私信息安全性的情况以及极少样本条件下,完成指纹图像预加密处理。

1.2　考虑隐私信息安全性的极少样本条件指纹图像细节加密

为确保指纹图像细节的安全性,在极少数样本条件下,还需要对指纹图像细节展开加密处理[8,9],操作流程如图1所示。

考虑隐私信息安全性的极少样本条件指纹图像细节加密[10]算法主要包含两个阶段:

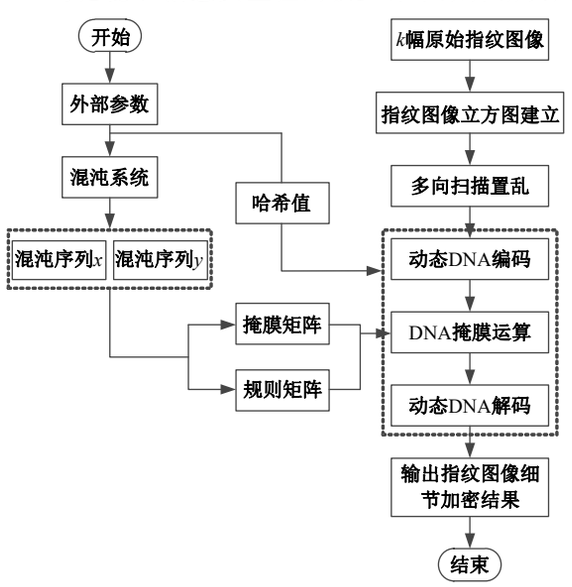

图1　考虑隐私信息安全性的极少样本条件指纹图像细节加密流程图

Fig. 1　Flow chart of fingerprint image detail encryption with few sample conditions considering privacy information security

1.2.1　置乱阶段

利用多向扫描对多图像立方体展开像素置乱处理。

1.2.2　扩散阶段

对置乱结果展开动态DNA编码、掩膜运算和解码,最终获取加密图像。加密的详细流程如下:

(1)形成密钥流。将k幅尺寸为$m\times n$的指纹明文图像组建成一幅大图像$\boldsymbol{R}^b$,然后采用SHA-256函数计算出R^b的256比特哈希值Z_k。将多幅指纹明文图像按照一定顺序建立大图像,对于图像幅数k,假设存在$k=k_1\times k_2$,且k_1和k_2均为正整数,则大图像R^b的组成顺序如式(4)所示:

$$\boldsymbol{R}^b_{k_1m\times k_2n}=\begin{bmatrix} R^1 & R^2 & \cdots & R^{k_2} \\ R^{k_2+1} & R^{k_2+2} & \cdots & R^{2k_2} \\ R^{2k_2} & \vdots & & \vdots \\ R^{(k_1-1)k_2+1} & R^{(k_1-1)k_2+2} & \cdots & R^{(k_1-1)2k_2} \end{bmatrix} \tag{4}$$

完成上述操作后,随机选取外部参数,通过式(5)即可获取两组2D-LACM混沌系统的初值x^0、y^0和控制参数ϕ:

$$\begin{cases} x^0=\mathrm{mod}\left((p_1+p_3)\times 10^{14}, 1\right) \\ y^0=\mathrm{mod}\left((p_2+p_4)\times 10^{14}, 1\right) \\ \phi=\mathrm{mod}\left((p_1+p_2+p_3+p_4)\times 10^{14}, 1\right) \end{cases} \tag{5}$$

式中:p_1、p_2、p_3和p_4为散列函数。

(2)形成混沌序列。采用初始值和控制参数对2D-LACM混沌系统展开l_0+kmn次迭代处理,获取两个混沌序列X^1和Y^1,长度均为kmn。

(3)组建指纹图像立方体。将k幅指纹明文图像按照序号的先后排序,组建指纹图像立方体G,将规格设定为$k\times m\times n$。

(4)对指纹图像立方图展开多向扫描。按照设定好的步骤对指纹图像立方体展开多向扫描处理,首先,建立G的三维坐标系;然后,选择扫描顺序E_{order},如下所示:

$$E_{\mathrm{order}}=\mathrm{mod}\left(floor\left(\frac{(p_1+p_2+p_3+p_4)}{4}\right)\times 10^{14}, 6\right)+1 \tag{6}$$

式中:$floor(\cdot)$为向下取整函数。对指纹图像立方体分别按照3个坐标轴方向展开扫描处理。

接下来,分别为各个扫描方向制定规则三元

组。最后,通过三元组的约束对G展开多向扫描处理,获取置乱立方体L,并且组建多向扫描模型。

(5)展开动态DNA编码。对置乱立方体L在x轴方向的第k层指纹图像细节展开动态DNA编码,对于第k层图像,利用$Enc(i)$规则展开DNA编码,具体的计算规格如下所示:

$$Enc(i)=\mathrm{mod}\left(floor\left(x^{0}(i+mn)\times 10^{14},8\right)\right)+1 \tag{7}$$

将各层完成编码处理后,获取DNA编码立方体T。然后,对于掩膜矩阵$\boldsymbol{U}$,使用规则$Rule$展开编码处理,如下所示:

$$Rule=\mathrm{mod}\left(floor\left(p_1+p_4\right)\times 10^{14},8\right) \tag{8}$$

完成以上操作即可获取DNA编码后的掩膜矩阵T^d。

(6)展开DNA掩膜运算。对置乱立方体展开DNA掩膜运算。首先,对置乱图像立方体展开DNA编码处理;然后,采用掩膜矩阵编码获取T^d和规则矩阵。

(7)展开动态DNA解码。对置乱图像立方体的x轴方向第k层指纹图像展开动态DNA编码,对于第k层图像,利用$Dec(i)$规则展开DNA编码,具体的计算规则如下所示:

$$Dec(i)=\mathrm{mod}\left(floor\left(y^{0}\left(p_1+p_4\right)\right)\times 10^{14},8\right)+1 \tag{9}$$

完成上述操作后获取解码立方体,将解码立方体的第k层指纹图像展开拆分,同时按照式(4)的规则展开组合,进而获取加密图像,实现考虑隐私信息安全性的极少样本条件指纹图像细节加密。

2 实验分析

为验证本文所提考虑隐私信息安全性的极少样本条件指纹图像细节加密算法的有效性,采用Matlab 2016a软件展开实验分析,利用图2给出部分指纹图像测试样本。

(1)加密性能测试

分别采用3种不同加密算法对图2展开加密处理,实验结果如图3所示。

分析图3可以看出,分别采用不同算法对选定的指纹图像细节进行加密处理后,本文算法具

图2 测试指纹图像

Fig. 2 Test fingerprint image

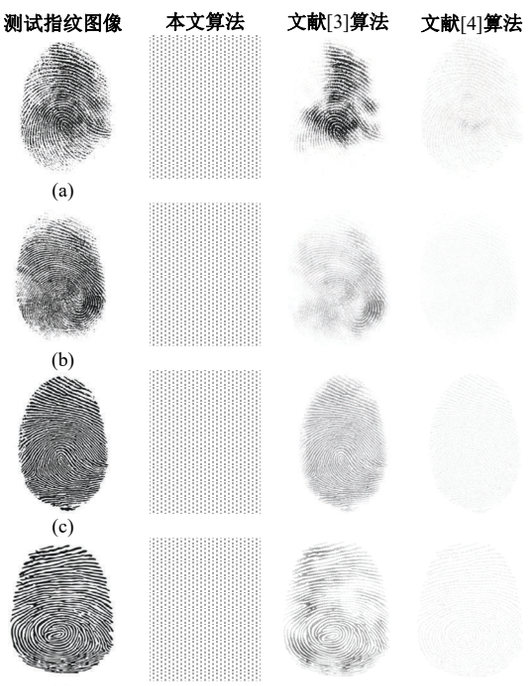

图3 3种不同加密算法的指纹图像细节加密结果比较

Fig. 3 Comparison of fingerprint image detail encryption results using three different encryption algorithms

有良好的加密性能,即使是在极少样本条件下,也可以更好地保护指纹图像的隐私性,有效防止隐私信息被泄露,安全指数较高。采用文献[3]算法只可以对部分指纹图像加密,仍有一些细节部分被暴露在外面,不利于保护隐私信息的安全性;文献[4]算法虽然可以较好地对指纹图像细节部分进行加密,但是指纹的轮廓仍然可以看见,还需要进一步提升其加密性能。由此可见,在3种加密算法中,本文算法可以更好地实现指纹图像细节加密,确保隐私信息的安全性。

(2)信息熵。信息熵$I(x)$是评估指纹图像细

节加密安全性的一项重要指标,具体计算式如下:

$$I(x)=-\sum_{i=1}^{n}f(x_i)lbf(x_i) \tag{10}$$

式中:$f(x_i)$为x_i发生的概率。

通过表1给出本文算法的信息熵测试结果,可以看出,在极少样本条件下,采用本文算法对指纹图像细节进行加密处理,加密图像的信息熵会随着载体信息熵的变化而变化,且两者取值十分接近,可以有效躲避攻击者的攻击,同时还能够更好地保护指纹图像隐私信息的安全性。

(3)通过图像相邻像素的相关性可以反映相邻位置像素间的相关性,加密性能越好,取值越接近0。相关系数r_{xy}计算式如下:

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

式中:$\mathrm{Cov}(x,y)$为相邻像素灰度均值;$D(x)$和$D(y)$为像素点x和y的灰度值。

利用表2给出相关系数测试结果,从表2可知,在3种图像加密算法中,本文算法的相关系数取值更低且更加接近0,说明其在极少样本条件下也可以确保图像的安全性。

表1　信息熵实验结果分析

Table 1　Analysis of information entropy experimental results

测试图像编号	明文图像	载体图像	加密图像
01	7.810	7.911	7.915
02	7.455	7.659	7.642
03	7.152	7.357	7.261
04	7.369	7.571	7.568
05	7.117	7.319	7.224
06	7.556	7.758	7.660
07	7.225	7.526	7.429

表2　3种加密算法的图像相关系数实验结果对比

Table 2　Comparison of experimental results of image correlation coefficients for three encryption algorithms

测试算法	相关系数
本文算法	0.000 14
文献[3]算法	0.001 85
文献[4]算法	0.038 50

3　结束语

随着信息技术的快速发展和普及,指纹识别技术在人类生活和工作中占据越来越重要的地位。为此,提出一种考虑隐私信息安全性的极少样本条件指纹图像细节加密算法。实验测试表明:本文算法可以有效实现对指纹图像的隐私保护,并且在极少样本条件下,依然能够获取比较满意的加密效果。未来将对本文算法展开更加深入的研究,使其可以更好地应对不同类型的攻击。

参考文献:

[1] 史进, 蔡竞, 徐锋. 傅里叶变换耦合DNA编码的图像加密算法[J]. 计算机工程与设计, 2021, 42(7): 1874-1881.
Shi Jin, Cai Jing, Xu Feng. Image encryption algorithm based on Fourier transform and DNA coding [J]. Computer Engineering and Design, 2021, 42(7): 1874-1881.

[2] 周红亮, 刘洪娟. 结合DNA编码的快速混沌图像加密算法[J]. 东北大学学报: 自然科学版, 2021, 42(10): 1391-1399.
Zhou Hong-liang, Liu Hong-juan. Fast chaotic image encryption algorithm combined with DNA encoding [J]. Journal of Northeastern University (Natural Science), 2021, 42 (10): 1391-1399.

[3] 王佳, 刘丽. 基于混沌卷积的光学图像分块加密方法[J]. 激光与光电子学进展, 2023, 60(4): 101-109.
Wang Jia, Liu Li. Optical image block encryption method based on chaotic convolution[J]. Laser & Optoelectronics Progress, 2023, 60(4): 101-109.

[4] 李春彪, 赵云楠, 李雅宁, 等. 基于正弦反馈Logistic混沌映射的图像加密算法及其FPGA实现[J]. 电子与信息学报, 2021, 43(12): 3766-3774.
Li Chun-biao, Zhao Yun-nan, Li Ya-ning, et al. An image encryption algorithm based on logistic chaotic mapping with sinusoidal feedback and its FPGA implementation[J]. Journal of Electronics & Information Technology, 2021, 43(12): 3766-3774.

[5] 陈善学, 杜文正, 任丽丹. 一种动态密钥与DNA交错编码的多图像加密算法[J]. 电讯技术, 2023, 63(4): 529-535.
Chen Shan-xue, Du Wen-zheng, Ren Li-dan. A multi-image encryption algorithm based on dynamic key and DNA interleaved coding[J]. Telecommunication Engineering, 2023, 63(4): 529-535.

[6] 石玲玉, 吴雁南, 周铭, 等. 基于点阵行列变换的图像置乱算法[J]. 南昌大学学报: 理科版, 2022, 46(6): 674-681.

Shi Ling-yu, Wu Yan-nan, Zhou Ming, et al. Image scrambing algorithm based on row and column transformation of lattice[J]. Journal of Nanchang University (Natural Science), 2022, 46(6): 674-681.

[7] 杨盼盼, 赵继春. 基于状态视图的流媒体图像信息置乱隐藏算法[J]. 计算机应用, 2021, 41(6): 1729-1733.
Yang Pan-pan, Zhao Ji-chun. Scrambling and hiding algorithm of streaming media image information based on state view[J]. Journal of Computer Applications, 2021, 41(6): 1729-1733.

[8] 靳旭文, 李国东, 刘雯. 基于3D-CS混沌系统的双DNA编码图像加密算法[J]. 包装工程, 2021, 42(3): 259-269.
Jin Xu-wen, Li Guo-dong, Liu Wen. Image encryption algorithm based on 3D-CS chaotic system and dual DNA coding[J]. Packaging Engineering, 2021, 42(3): 259-269.

[9] 张军朋, 向菲. 基于DNA随机置换的新型图像加密算法研究[J]. 计算机仿真, 2022, 39(7): 355-361.
Zhang Jun-peng, Xiang Fei. A novel image encryption algorithm based on DNA random permutation[J]. Computer Simulation, 2022, 39(7): 355-361.

[10] 王一诺, 宋昭阳, 马玉林, 等. 基于DNA编码与交替量子随机行走的彩色图像加密算法[J]. 物理学报, 2021, 70(23): 32-41.
Wang Yi-nuo, Song Zhao-yang, Ma Yu-lin , et al. Color image encryption algorithm based on DNA code and alternating quantum random walk[J]. Acta Physica Sinica, 2021, 70(23): 32-41.