DOI:10.19652/j.cnki.femt.2406168

基于ZYNQ图像加密算法的设计与实现

郝伟强[1,2] 张 鹏[1,2] 陈云鹏[1,2]
(1.中北大学仪器与电子学院 太原 030051;2.中北大学电子测试技术国家重点实验室 太原 030051)

摘 要:随着通信网络规模不断扩大、业务种类日益繁多以及对通信安全性要求越来越高,传统密码算法已经无法满足现代网络通信需求。如今,众多的通用密码算法体系标准因其各自独特的算法优点而被广泛应用于多个行业,它们已经变成了确保数据传输安全性的关键工具。目前的高级加密标准算法(AES)在处理大数据量时会存在加密效果差、抗攻击性弱等诸多缺陷。针对以上问题,对传统AES加密算法进行了优化,在AES加密算法上加入了Arnold置乱算法,通过分块Arnold置乱提高了加密算法的效果和抗攻击性。最后在ZYNQ板进行了功能验证,结果表明,优化后的AES算法实现了预期的功能。

关键词:图像加密;AES加密算法;Arnold变换
中图分类号:TN975;TN914 **文献标识码**:A **国家标准学科分类代码**:510.50

Design and implementation of ZYNQ image encryption algorithm

Hao Weiqiang[1,2] Zhangpeng[1,2] Chen Yunpeng[1,2]
(1. School of Instrumentation and Electronics, North University of China, Taiyuan 030051, China;
2. State Key Laboratory of Electronic Testing Technology, North University of China, Taiyuan 030051, China)

Abstract: With the continuous expansion of communication networks, the increasing variety of services, and the increasing requirements for communication security, traditional cryptographic algorithms can no longer meet the needs of modern network communication. Nowadays, many common cryptographic algorithm system standards are widely used in many industries due to their unique algorithm advantages, and they have become a key tool to ensure the security of data transmission. The current advanced encryption standard (AES) algorithm has many defects when processing large amounts of data, such as poor encryption effect and weak attack resistance. In order to solve the above problems, this paper optimizes the traditional AES encryption algorithm, adds the Arnold scrambling algorithm to the AES encryption algorithm, and improves the effect and attack resistance of the encryption algorithm by smashing Arnold scrambling in blocks. Finally, the functional verification is carried out on the ZYNQ board, and the results show that the optimized AES algorithm achieves the expected effect.

Keywords: image encryption; AES encryption algorithm; Arnold transform

0 引 言

加密算法涉及广泛的现代密码学知识,包括秘密共享、非对称加密、无意传输等[1]。在数据传输过程中,数据加密的需求是至关重要的。在加密过程中需要加密的数据段或消息,这种未处理的数据称为明文,加密后的安全信息称为密文[2]。依据不同的密钥类型,加密算法大致可以被分类为非对称加密方法和对称加密方法[3]。在实际应用中,非对称加密算法通常仅适用于处理少量数据,例如身份验证,而不适用于处理大量数据的场合中。在对大数据量的图像加密过程中,对称高级加密标准算法(advanced encryption standard,AES)[4]是美国政府和许多组织认可的可信算法。AES支持128、192和256 bits密钥长度。AES算法在对称加密领域内的应用非常广泛,成为了行业内使用最频繁的加密算法之一。关于AES算法,已经有多种相关的IP产品被开发出来,例如Helion和GMU开发的AES IP核等[5]。

国内在这方面也有相应的探索和实验,推出的很多相

收稿日期:2024-06-17

关的产品。目前国家密码管理局颁布的 SM 系列算法是中国特有的国密标准，包括 SM1、SM2、SM3 和 SM4 等算法[6]。文献[7]把 Logistics 的迭代次数与图像像素点的值结合起来，提高了置乱和扩散两个操作的关联性，但算法在鲁棒性方面还有一点缺陷。文献[8]在图像加密算法中对图像矩阵进行 Arnod 置乱，提高了算法的鲁棒性，但加密效果一般，算法只在抗涂改攻击做了验证，在抗裁剪攻击方面还有待提高。

本文主要为了增强 AES 加密算法的加密效果和抗裁剪攻击性，提出了一种改进的 AES 算法，即把原始图像分块 Arnold 置乱之后进行图像数字化，然后再进行 AES 加密。这种改进的 AES 加密算法可以提高图像的安全性和抗攻击性。

1 AES 加密算法原理

AES 是一种采用对称密钥的加密算法，在加密和解密过程中使用的是同一个密钥[9]，从而使得其处理速度通常超过非对称加密算法。但这同样要求密钥在发送方和接收方之间必须安全传输。在 AES 算法中，处理的数据块固定为 128 bits，用户可以根据需要选择 128、192 或 256 bits 的密钥长度。密钥长度的不同决定了加密的轮数：128 bits 密钥需要 10 轮，192 bits 密钥需 12 轮，而 256 bits 密钥则需要 14 轮。每一轮加密主要涉及 4 个步骤：字节替换(Sub Bytes)、行移位(Shift Rows)、列混合(Mix Columns)和添加轮密钥(Add Round Key)[10]。加密流程如图 1 所示。

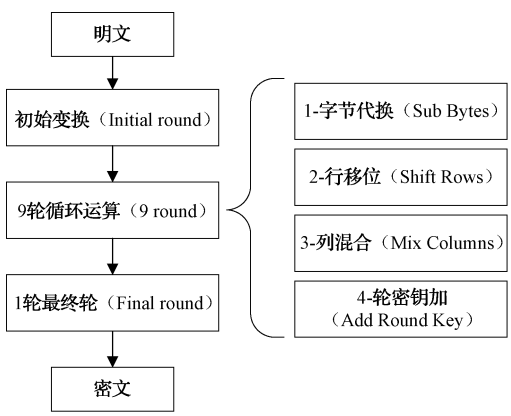


图 1 AES 加密流程

Fig. 1 AES encryption flowchart

1.1 字节替换

AES 字节替换步骤通过使用一个称为 S-box[11]（图 2）的查找表进行操作。该 S-box 是由 0x00～0xFF 的 256 个元素组成的 16×16 矩阵，用于将中间态 S 中的每个字节对应转换为加密过程中的新字节，实现混淆明文数据的目的。通过计算可以生成用于此转换的 S-box 查找表。

字体替换的流程如下：

63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

图 2 S-box 查找表

Fig. 2 S-box lookup table

1) 对 S-box 第 p 行 q 列元素初始化为 0xpq。

2) 将 S-box 中各个字节在有限域 GF(2)上进行取逆算法，0x00 对应为 0x00。AES 构造 GF(2)用 Z2[x]上的不可约多项式 $m(x)=x^8+x^4+x^3+x+1$。然后在 Z2[x]上运用欧几里得算法扩展求逆元素。

3) 将 S-box 中的元素按位记为 $(a_7a_6a_5a_4a_3a_2a_1a_0)$，例如，0xF8 记为(11111000)。再对 S-box 里各个字节和位进行式(1)运算。

$$b_i = a_i \oplus a_{i+4}bmod8 \oplus a_{i+6}bmod8 \oplus a_{i+7}bmod8 \oplus a_{i+8} \oplus c_i \tag{1}$$

式中：c_i 是值 0x63 字节的第 i 位；最终得到在 S 盒中的元素 $(b_7b_6b_5b_4b_3b_2b_1b_0)$。

状态矩阵中元素根据以上算法对应一个新的 byte，把该 byte 的低四位作为列值，高四位作为行值，取出 S-box 内对应的列行数值当成需要的数据结果，此数据结果为字节代换的输出。

1.2 行移位

当密钥设置为 128 bits 时，状态矩阵的行移位操作涉及简单的循环移位，从式(2)可知，经过移位，列的全部元素得到重新排列，但没有改变移位前的所有元素值。

$$\begin{bmatrix} A00 & A01 & A02 & A03 \\ A10 & A11 & A12 & A13 \\ A20 & A21 & A22 & A23 \\ A30 & A31 & A32 & A33 \end{bmatrix} \rightarrow \begin{bmatrix} A00 & A01 & A02 & A03 \\ A11 & A12 & A13 & A10 \\ A22 & A23 & A20 & A21 \\ A33 & A30 & A31 & A32 \end{bmatrix} \tag{2}$$

虽然行移位操作简单，却极具效用。状态矩阵的输入和输出数据格式相同，均由 4 列构成。加密过程中，数据直接从明文中以状态矩阵的形式提取，同时密钥操作也以 4×4 矩阵形式进行。通过一次行移位变换，可以将某一列的 4 个字节调整至另一列，其线性距离为 4 个字节的整数倍[12]，这样确保了每列的 4 个字节均分散到 4 个不同的列中。

1.3 列混合

列混合变化是通过矩阵之间的乘法做运算得到的，经过移位后的状态矩阵与约定好的矩阵相乘，得到混肴后的状态矩阵，如式(3)所示。

$$\begin{bmatrix} S'00 & S'01 & S'02 & S'03 \\ S'10 & S'11 & S'12 & S'13 \\ S'20 & S'21 & S'22 & S'23 \\ S'30 & S'31 & S'32 & S'33 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} S00 & S01 & S02 & S03 \\ S10 & S11 & S12 & S13 \\ S20 & S21 & S22 & S23 \\ S30 & S31 & S32 & S33 \end{bmatrix} \tag{3}$$

状态矩阵中的第 j 列 ($0 \leqslant j \leqslant 3$) 的列混合可以表示为：

$$\begin{cases} s(0,j)' = (\{02\} \times s(0,j)) \oplus (\{03\} \times s(1,j)) \oplus s(2,j) \oplus s(3,j) \\ s(1,j)' = s(0,j) \oplus (\{02\} \times s(1,j)) \oplus (\{03\} \times s(2,j)) \oplus s(3,j) \\ s(2,j)' = s(0,cj) \oplus s(1,j) \oplus (\{02\} \times s(2,j)) \oplus (\{03\} \times s(3,j)) \\ s(3,cj)' = (\{03\} \times s(0,j)) \oplus s(1,j) \oplus s(2,j) \oplus (\{02\} \times s(3,cj)) \end{cases} \tag{4}$$

在列混合中，矩阵系数的生成依据最大距离线性码[13]。这种方法增强了数据的扩散性，从而提升了列混合的效果。

1.4 轮密钥加

轮密钥加是每一轮运算的最后一个步骤，其中将前面步骤的结果与子密钥进行异或操作[14]，如式(5)所示。这标志着该算法一次迭代的完成。子密钥是通过对初始密钥进行扩展获得。

$$\begin{bmatrix} S'00 & S'01 & S'02 & S'03 \\ S'10 & S'11 & S'12 & S'13 \\ S'20 & S'21 & S'22 & S'23 \\ S'30 & S'31 & S'32 & S'33 \end{bmatrix} \oplus \begin{bmatrix} K00 & K01 & K02 & K03 \\ K10 & K11 & K11 & K13 \\ K20 & K21 & K22 & K23 \\ K30 & K31 & K32 & K33 \end{bmatrix} = \begin{bmatrix} D00 & D01 & D02 & D03 \\ D10 & D11 & D12 & D13 \\ D20 & D21 & D22 & D23 \\ D30 & D31 & D32 & D33 \end{bmatrix} \tag{5}$$

1.5 密钥扩展

在密钥扩展时，首先将原始密钥存储为 4×4 的状态矩阵，状态矩阵中的每一列构成一个字，这 4 个字分别记做 $w[0]$、$w[1]$、$w[2]$ 以及 $w[3]$，如图 3 所示。一个以字为单位的数组 w 由这四个列组成。然后，对数组进行扩充，即由 $w[0:3]$ 扩充到 $w[0:44]$，总共扩展了 40 个新列，组成 44 列的 Key expend 数组[15]。新列以递归方式产生。

1) 如果 i 不是 4 的倍数，那么第 i 列由如下等式确定：

$$w[i] = w[i-4] \oplus w[i-1]$$

2) 如果 i 是 4 的倍数，那么第 i 列由如下等式确定：

$$w[i] = w[i-4] \oplus T(w[i-1])$$

把 $w[i-1]$ 转化为 $T(w[i-1])$ 这种形式，这种形式包括这种形式包括字循环、字节代换和轮常量异或 3 方面内容，作用如下：

(1)字循环：循环地把 $w[i-1]$ 的元素移位，一次一字节，把 abcd 换成 bcda；

(2)字节代换：把 bcda 当成 S-box 的输入，输出另外的字节 efgh；

(3)轮常量异或：计算一轮的常量 $r(i) = 2(i-1)/4$；

(4)通过以上得到变化后的列：$[e \oplus r(i), f, g, h]$。

第 i 轮的轮密钥组成了 $w[4i]$、$w[4i+1]$、$w[4i+2]$、$w[4i+3]$。

2 AES 加密算法的优化

为了增强基于 AES 的数字图像加密技术的鲁棒性，本文提出了一种改进的加密方法。该方法融合了 Arnold 变换算法[16]，与 AES 加密算法相结合形成混合式加密方法。在该方法中，图像首先经过 Arnold 变换进行置乱处理，然后再应用 AES 加密。这种方法的优点在于，即使加密图像受到损坏，原始图像的像素值依然在整个图像中分布，任何错误信息在恢复过程中也会被相应地分散，这不仅确保了图像信息的安全性，而且还提升了加密算法的抗攻击能力。

2.1 Arnold 置乱算法原理

Arnold 变换是对数字图像的像素矩阵进行裁剪和拼接的过程[17]。二维 Arnold 变换矩阵表示如式(6)所示。

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \cdot \begin{bmatrix} x'' \\ y'' \end{bmatrix} mod(N) \tag{6}$$

式中：(x'', y'') 是像素的原始位置；(x', y') 是置乱后的位置；(a, b) 可以自己进行指定；$bmod(N)$ 是指对 N 取余，为图像的长或宽。

2.2 分块 Arnold 置乱算法流程

Arnold 置乱算法本质上是定义在正方形格点上的一个变换。例如当图像的尺寸为 $1\ 920\times1\ 080$，无所直接进行置乱，所以要先将图像分为 144 个 120×120 正方形块后再进行置乱，分块 Arnold 置乱算法流程如图 3 所示。

通过应用二维 Arnold 置乱算法，图片中的像素点位置发生了变化。Arnold 算法主要通过对原图像的每个像素点坐标进行变换实现，这涉及到使用一个参考映射矩阵与坐标进行矩阵乘法，然后对结果进行模除，以图像矩阵宽度为模。这样计算后，得到变换后图像的新坐标位置。

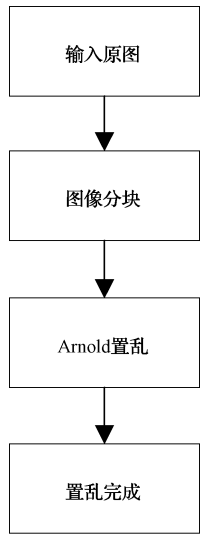
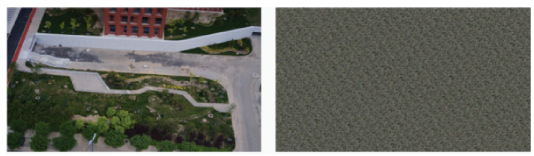


图 3　分块 Arnold 置乱算法流程

Fig. 3　Flow chart of the block Arnold scrambling algorithm

Arnold 置乱结果如图 4 所示。



(a) 原图
(a) Original image

(b) 加密后
(b) After encryption

图 4　Arnold 置乱结果

Fig. 4　Arnold scrambling result

一般来说，要解反 Arnold 变换，必须计算矩阵的周期。工作浪费了大量的资源，尤其是大程度的周期。利用其逆矩阵求解反 Arnold 变换，既节省了开销，又不需要计算图像的周期。恢复原始图像，只需使用 Arnold 变换迭代相同的次数。该算法的逆变换，即由置乱后的图像恢复到原图算法为：

$$\begin{bmatrix} x^n \\ y^n \end{bmatrix} = \begin{bmatrix} ab+1 & -b \\ -a & 1 \end{bmatrix} \cdot \begin{bmatrix} x' \\ y' \end{bmatrix} \bmod(N) \tag{7}$$

逆 Arnold 置乱流程如图 5 所示。

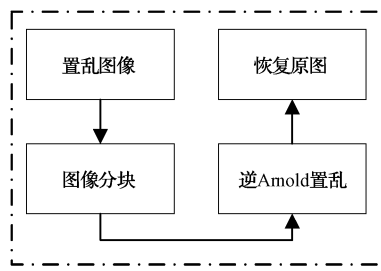
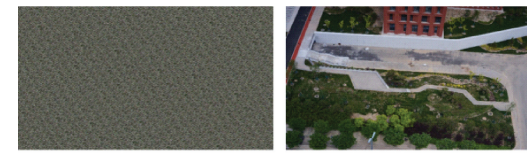


图 5　逆 Arnold 置乱流程

Fig. 5　Inverse Arnold scrambled flowchart

逆 Arnold 变换后的图如图 6 所示。



(a) 加密后
(a) After encryption

(b) 恢复
(b) Recovery

图 6　逆 Arnold 置乱结果

Fig. 6　Inverse Arnold scramble results

Arnold 置乱算法的实现相对简单，执行速度较快，适用于对图像进行快速的加密处理，并且该算法具有一定的非线性特性，能够增强图像的安全性，使得加密后的图像更难以被破解，同时 Arnold 置乱算法是可逆的，即通过逆向操作可以将加密后的图像恢复到原始状态。

2.3　改进后的加密和解密算法流程

加密算法流程图如图 7 所示。

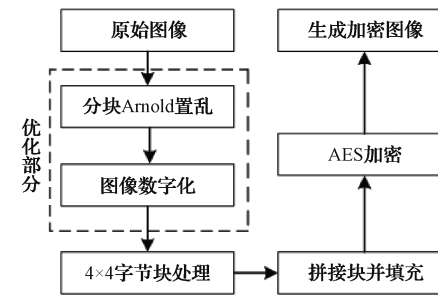


图 7　改进后加密算法流程

Fig. 7　Flow diagram of the improved encryption algorithm

1）输入需要加密的原始图像；

2）分块 Arnold 置乱；

3）图像数字化，将图像转为矩阵；

4）4×4 字节块处理，从左上角到右下角；

5）将每一个 4×4 块都进行 AES 加密；

6）拼接块，形成新的矩阵，如果为非 4 的倍数维度，则进行填充；

7）生成加密后的图像。

解密流程如图 8 所示。

1）输入需要解密的图像；

2）对数据进行 4×4 字节块的划分；

3）AES 对每个 4×4 块进行解密；

4）如果有填充则移除填充后进行拼接块，恢复到图像矩阵；

5）图像数字化逆过程，将矩阵转换回图像；

6）分块逆 Arnold 置乱；

7）输出解密后的图像。

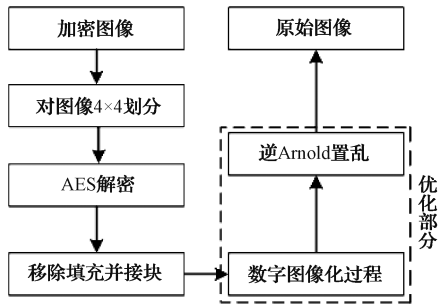


图 8　改进后解密算法流程

Fig. 8　Flow diagram of the improved decryption algorithm

3　实验验证

3.1　算法仿真验证

1)抗涂改剪裁攻击性分析

在图像加密中,涂改剪裁攻击是指对加密图像进行故意的修改和损害,这种攻击试图破坏图像的一部分信息,使得即使在解密后,图像的原始内容也无法被完整和正确地恢复。AES 算法与改进后 AES 算法受到局部涂改攻击后的效果如图 9 和 10 所示。

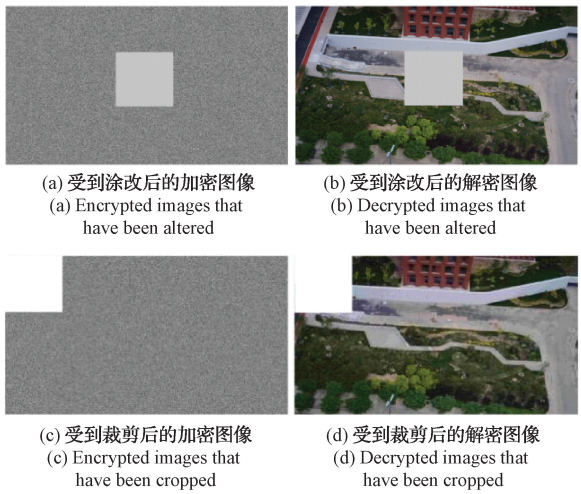


图 9　AES 加密算法局部涂改攻击

Fig. 9　AES encryption algorithm partial alteration attack

面对涂改和裁剪攻击,相较于传统的 AES 算法,经过改进的 AES 算法能够将图像的错误信息均匀分布到全图中。在解密过程中,这使得图像能够接近完整地恢复其最初的视觉特征和内容。这种改进的 AES 算法不仅在鲁棒性上得到加强,其抗攻击性和安全性也随之提升。

2)图像加密直方图和皮尔逊相关系数分析

在图像加密领域,直方图作为一种重要的分析工具,用于评估和验证加密算法的效果及其安全性。通过比较原始和加密图像的直方图分布,可以有效检验加密质量,确保加密后的图像直方图呈现出与随机噪声类似的均匀分布,从而验证算法在隐藏原始视觉信息和抵御基于统计

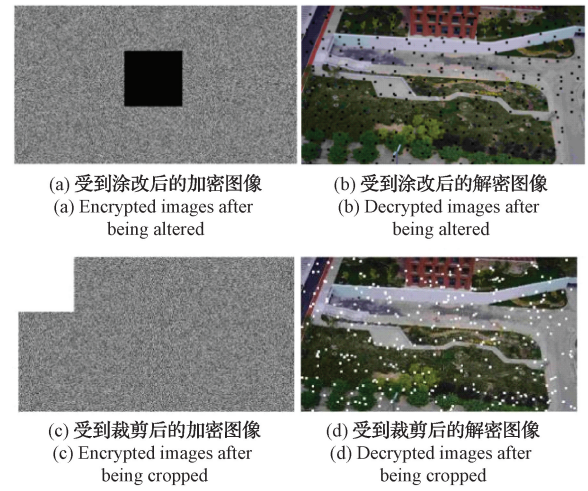


图 10　改进后的 AES 加密算法局部涂改攻击

Fig. 10　Improved AES encryption algorithm partial alteration attack

分析攻击的能力。

AES 图像加密算法直方图分布如图 11 所示。

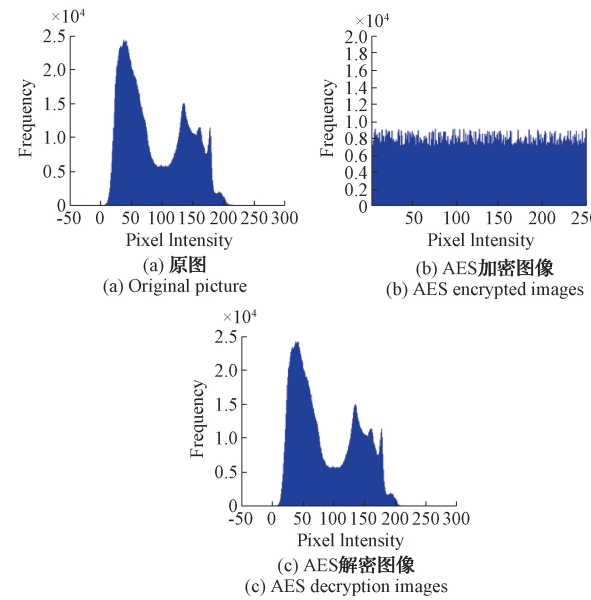


图 11　AES 算法直方图分布

Fig. 11　AES algorithm histogram distribution

改进后的 AES 加密算法真方图分布如图 12 所示。

从直方图可以看出,Arnold 置乱图像和原图的直方图完全相同,这是因为 Arnold 算法并不会改变图片像素点,只是将原有像素点进行打乱。数字图像本身是一个有限集,Arnold 变换在一定次数的迭代后能够实现图像的加密效果,同时由于其周期性,又能在一定周期后恢复原始图像。在此基础上融合 AES 加密算法,后者在矩阵内部调整像素值及其位置,使得图像的像素值和位置都发生变化。通过对比 AES 加密图像和改进后 AES 加密图像

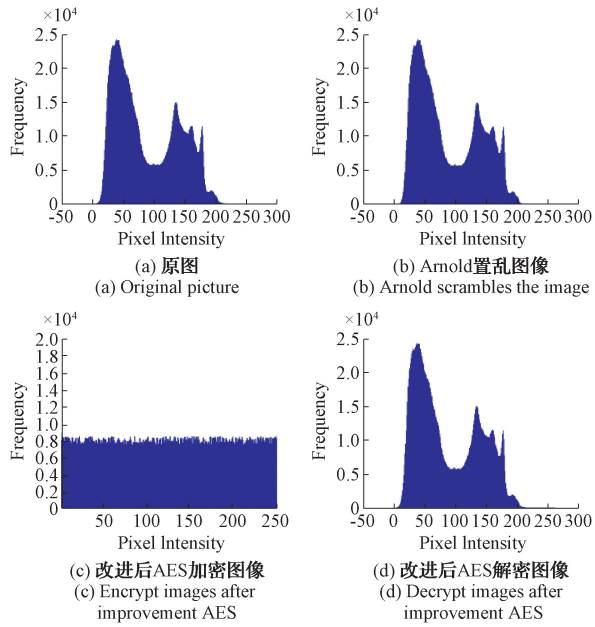


图 12 改进后 AES 算法的直方图分布

Fig. 12 Histogram distribution of the improved AES algorithm

的直方图，后者的直方图分布更加均匀，验证了改进之后的算法提高了图像的安全性和抗攻击能力。

再对图像进行皮尔逊相关性系数分析，原始图像与加密图像皮尔逊相关性比较如表 1 所示。

表 1 皮尔逊相关性系数

Table 1 Pearson correlation coefficient

方向	原始图像	AES 加密	改进后 AES 加密
水平	0.983 3	0.032 2	0.003 5
垂直	0.970 5	0.056 3	0.002 7
对角线	0.973 1	0.046 7	0.003 2

皮尔逊相关系数，也被称为皮尔逊积矩相关系数，是衡量两个变量线性相关强度的指标。从表中的皮尔逊相关系数可以看出，改进后 AES 加密算法的系数明显比 AES 加密算法系数低，说明前者在对比度和加密效果上具有很好的优越性。

3.2 算法功能验证

本文主要通过 ZYNQ—7020 开发板对算法进行了功能验证，ZYNQ 板主要是由处理系统(processing system，PS)和可编程逻辑(programmable logic，PL)部分两部分构成，简称为 PS 端和 PL 端。ZYNQ 板的简化模型如图 13 所示。

PS 端是 ZYNQ 板芯片中的 ARM Cortex-A9 处理器，包括双核或单核处理器、DMA 控制器、外设控制器等；PL 端是 ZYNQ 板芯片中的 FPGA 部分，包括可编程逻辑单元、I/O 控制器、I^2C 控制器等。本文主要在 ZYNQ 板

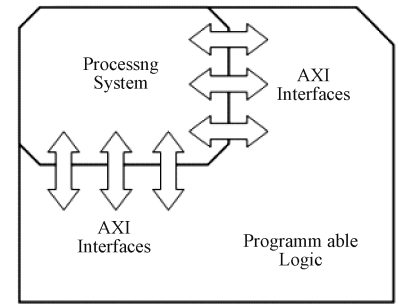


图 13 ZYNQ 简化模型

Fig. 13 ZYNQ simplified model diagram

的 PS 端运行加密算法程序，在 PL 端进行结果显示。

将需要加密的图像存入 SD 卡后，运行 Vitis 程序，通过 ZYNQ 开发板运行图像加密算法，加密和解密图像通过 HDMI 接口在显示屏中显示。结果如图 14 所示。

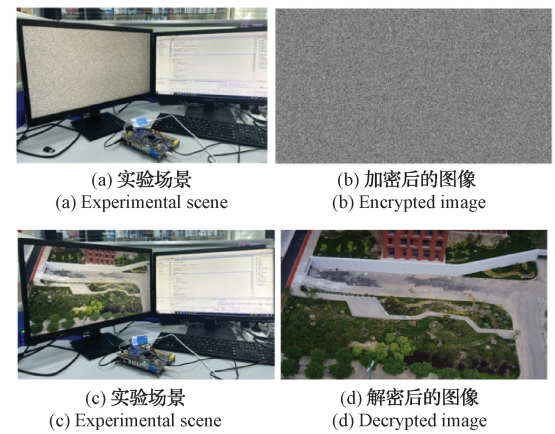


图 14 图像加密→解密的功能验证

Fig. 14 Verification of image encryption→ decryption

从加密结果可以看出经过加密的图像可识别的数据模式和结构被破坏，数据会呈现出随机分布，看起来更像是噪声。这不仅显示了加密系统在隐藏图像数据的特征、保持数据隐私和防止未授权访问方面的有效性，而且还表明了该系统在保护图像数据完整性和确保数据在传输或存储过程中不被篡改或解读的能力。从解密结果可以看出，图像已经恢复初始状态，可以看到图像中的所有信息。

4 结 论

通过分析实验结果，改进后的 AES 加密算法提高了图像的安全性和抗攻击性。经过仿真验证分析，加入 Arnold 置乱增强了算法的鲁棒性和抗裁剪攻击，同时也提高了加密效果；经过功能验证分析，改进的 AES 算法在 ZYNQ 板上实现了对图像加密和解密的功能，表明算法在硬件实现上具有很大的应用空间。这种改进的 AES 算法虽然提高了图像的安全性，但还是存在一些局限性，非对称性加密算法在安全性方面相较于对称加密算法有很大

的优势，因此后续的研究可以在对称算法 AES 的基础上引入非对称算法的安全性优势，比如通过对密钥进行非对称加密，进一步提高加密图像的安全性。

参考文献

[1] 闫娜. 基于系数融合与锯齿填充曲线的双图像加密算法[J]. 国外电子测量技术，2017，36(3)：11-15.
YAN N. Dual image encryption algorithm based on coefficient fusion and zigzag filling curve[J]. Foreign Electronic Measurement Technology，2017，36(3)：11-15.

[2] 程宁，王茜娟. 基于混沌 Gyrator 变换与矩阵分解的光学图像加密算法[J]. 电子测量与仪器学报，2019，33(1)：191-202.
CHEN N，WANG X J. Optical image encryption algorithm based on chaotic gyrator transform and matrix factorization [J]. Journal of Electronic Measurement and Instrumentation，2019，33(1)：191-202.

[3] 方应李. 基于 ECC 和 AES 图像加密算法的研究[D]. 南京：南京邮电大学，2023.
FANG Y L. Research on image encryption algorithm based on ECC and AES [D]. Nanjing：Nanjing University of Post and Telecommunications，2023.

[4] 王勤凡，翟江涛，陈伟，等. 一种基于图卷积神经网络的加密流量分类方法[J]. 电子测量技术，2022，45(14)：109-115.
WANG Q F，ZHAI J T，CHEN W，et al. An encryption traffic classification method based on graph convolutional neural network [J]. Electronic Measurement Technology，2022，45(14)：109-115.

[5] LI T，ZHOU X C，ZHANG Y，et al. Underwater image enhancement based on IMSRCR and CLAHE-WGIF[J]. Instrumentation，2023，10(2)：19-29.

[6] 弓国伟. 基于 PCIe 的 SM4 国密算法数据加密卡设计与研究[D]. 太原：中北大学，2023.
GONG G W. Design and research of SM4 national cryptography algorithm data encryption card based on PCIe[D]. Taiyuan：North University of China，2023.

[7] 谢国波，丁煜明. 基于 Logistic 映射的可变置乱参数的图像加密算法[J]. 微电子学与计算机，2020，32(4)：111-115.
XIE G B，DING Y M. Image encryption algorithm based on logistic mapping with variable scrambling parameters[J]. Microelectronics and Computer，2020，32(4)：111-115.

[8] 李倩倩，武一. 一种基于 AES 图像加密技术改进[J]. 电子设计工程，2015(18)：65-68.
LI Q Q，WU Y. Improvement of image encryption technology based on AES [J]. Electronic Design Engineering，2015(18)：65-68.

[9] WANG W Y，ZHOU X C，YANG L J. Multimodal medical image fusion based on parameter adaptive PCNN and latent low-rank representation [J]. Instrumentation，2023，10(1)：45-58.

[10] 杜鹏，崔琦，王思翔，等. 基于新型时空混沌系统的隐私图像加密算法[J]. 计算机工程，2024，50(2)：140-153.
DU P，CUI Q，WANG S Y，et al. Privacy image encryptionalgorithm based on novel spatiotemporal chaotic system [J]. Computer Engineering，2024，50(2)：140-153.

[11] LI T，ZHOU X C，ZHANG Y，et al. underwater image enhancement based on IMSRCR and CLAHE-WGIF[J]. Instrumentation，2023，10(2)：19-29.

[12] 李涵. 基于混沌系统的图像加密算法研究[D]. 淮南：安徽理工大学，2022.
LI H. Research on image encryption algorithm basedon chaotic system [D]. Huainan：Anhui University of Science and Technology，2022.

[13] 赵恩玄，何云勇，沈宽，等. 基于深度学习的铸件 CT 图像分割算法[J]. 仪器仪表学报，2023，44(11)：176-184.
ZHAO EN X，HE Y Y，SHEN K，et al. CT image segmentation algorithm for castings based on deep learning[J]. Chinese Journal of Scientific Instrument，2023，44(11)：176-184.

[14] PUTEAUX P，PUECH W. CFB-then-ECB mode-based image encryption for an efficient correction of noisy encrypted images [J]. IEEE Transactions on Circuits and Systems for Video Technology，2021，34(9)：338-351.

[15] YANG Y，XIAO X，CAI X，et al. A secure and privacy-preserving technique based on contrast-enhancement reversible data hiding and plaintext encryption for medical images [J]. IEEE Signal Processing Letters，2020，455(27)：256-260.

[16] 石金晶，陈添，陈淑慧，等. 基于 Arnold 变换的量子图像混沌加密方法[J]. 电子与信息学报，2022，44(12)：284-293.
SHI J J，CHEN T，CHEN SH H，et al. Quantum image chaotic cryptography scheme based on arnold transforms[J]. Journal of Electronics and Information Technology，2022，44(12)：284-293.

[17] 洪炎，王艺杭，苏静明，等. 基于行列异或的 Arnold 双置乱图像加密方法[J]. 科学技术与工程，2024，24(2)：649-657.
HONG Y，WANG Y H，SU J M，et al. Arnold double-

scramble image encryption method based on column and column XOR [J]. Science Technology and Engineering, 2024, 24(2): 649-657.

作者简介

郝伟强，硕士研究生，主要研究方向为 ZYNQ 平台的开发、图像传输与处理。
E-mail：1424165118@qq.com

张鹏，副教授，硕士生导师，主要研究方向为自动控制、嵌入式系统、存储测试等。
E-mail：sxyczhangpeng@126.com

陈云鹏，硕士研究生，主要研究方向为 ZYNQ 平台开发、硬件电路设计。
E-mail：17835412282@163.com