# การปรับปรุงการเข้ารหัสลับภาพโดยอาศัยเศษส่วนต่อเนื่องของจำนวนอตรรกยะกำลังสี่

# An Improvement of Image Encryption Based on Continued Fractions of Quartic Irrationals

ปูชิตา ธรรมวงศ์ และ ทศพร ทองจันทึก*

Puchita Thammawong and Thotsaphon Thongjunthug*

*สาขาวิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น*

*Department of Mathematics, Faculty of Science, Khon Kaen University*

Received : 27 July 2019

Revised : 3 December 2019

Accepted : 19 December 2019

## บทคัดย่อ

บทความวิจัยนี้นำเสนอวิธีการเข้ารหัสลับแบบกุญแจสมมาตรสำหรับภาพ โดยใช้เศษส่วนต่อเนื่องเชิงเดียวอนันต์ที่ได้จากจำนวนอตรรกยะกำลังสี่ในรูป $\sqrt{a}+\sqrt{b}$ (เมื่อ $a,b\in\mathbb{N}$) เป็นกุญแจลับ และวัดประสิทธิภาพของการเข้ารหัสลับในด้านของสัมประสิทธิ์สหสัมพันธ์ ส่วนเบี่ยงเบนจากอุดมคติ ค่าปรากฏการณ์หิมะถล่ม และอัตราส่วนสูงสุดของสัญญาณต่อสัญญาณรบกวน ภายหลังจากการเข้ารหัสลับภาพทดสอบมาตรฐาน 5 ภาพ (ได้แก่ ภาพเครื่องบิน ภาพลิงบาบูน ภาพผลไม้ ภาพลีนา และภาพพริกหยวก) ได้เปรียบเทียบวิธีการที่นำเสนอกับวิธีการของ Hamad *et al.* (2013) และวิธีการของ Pareek (2012) ผลการศึกษาพบว่า วิธีการที่นำเสนอนั้นมีประสิทธิภาพสูงกว่าวิธีการของ Pareek (2012) นอกจากนี้ เมื่อไม่พิจารณาประสิทธิภาพในด้านของสัมประสิทธิ์สหสัมพันธ์ พบว่าวิธีการที่นำเสนอนั้นยังมีประสิทธิภาพสูงกว่าวิธีการของ Hamad *et al.* (2013) อีกด้วย

**คำสำคัญ** : การเข้ารหัสลับภาพ, ภาพอาร์จีบี, เศษส่วนต่อเนื่อง, จำนวนอตรรกยะกำลังสี่

*Corresponding author. E-mail : thotho@kku.ac.th

## Abstract

In this paper, we propose a symmetric-key image encryption scheme using an infinite simple continued fraction derived from a quartic irrational number of the form $\sqrt{a}+\sqrt{b}$, where $a,b \in \mathbb{N}$, as the secret key. Efficiency of encryption is measured in terms of correlation coefficients, deviation from ideality, the avalanche effect, and peak signal-to-noise ratios. After encrypting five standard test images, namely, Airplane, Baboon, Fruits, Lena, and Peppers, our scheme is compared with the schemes of Hamad *et al.* (2013) and Pareek (2012). The results show that our scheme is more effective than the scheme of Pareek (2012). Moreover, except for the correlation coefficients, our scheme is slightly more effective than the scheme of Hamad *et al.* (2013).

**Keywords :** image encryption, RGB image, continued fraction, quartic irrational number

### Introduction

Image security is an application layer technology to guard the transmitted data against unwanted disclosure as well as to protect the data from modification while in transit. To achieve higher security to encrypted images, several image encryption schemes have been proposed based on various mechanisms. Those mechanisms may be classified into three major categories: position permutation, value transformation, and the combination form (Pareek, 2012).

Nowadays, there are a number of encryption schemes for RGB images. Liu *et al.* (2011) proposed an encryption scheme which uses Arnold transform and color-blend operation in discrete cosine transform domains. The Arnold transform scrambles the pixel sequence of a color image for several subimages at local area. The data of random angle is the main key of encryption, while the parameters of Arnold transform are the additional key for increasing security. Later, Pareek (2012) proposed an encryption scheme which uses a 144-bit secret key and utilizes both pixel substitution and pixel permutation, in which pixels in each subimage are reshuffled by using a key-dependent magic square matrix. His proposed scheme is sensitive to the secret key and requires less computation. Moreover, Hamad *et al.* (2013) modified the Playfair cipher for encrypting digital images. Rather than using the classical $5 \times 5$ key matrix, their proposed scheme relies on $16 \times 16$ key matrix for a better alignment with image pixel data and adopts an exclusive-or procedure to provide security to encrypted images.

A continued fraction is a representation of a real number as a sequence of integers, which can be obtained algorithmically. In particular, it is well known that every irrational number can be rewritten as an infinite continue fraction (Burton, 2007). This, therefore, can provide a convenient way to disguise digital data and reduces the need of memory to store all cipher keys. Özdemir and Yaprakdal (2010) introduced a cipher whose encryption algorithm relies on a periodic continued fraction although their cipher is more suitable for text encryption than image encryption. Thus, in this paper, we aim to develop a symmetric-key encryption scheme for RGB images using continued fractions associated to quartic irrational numbers. Furthermore, efficiency of our scheme will be compared with that of the schemes of Hamad *et al.* (2013) and Pareek (2012) in terms of correlation coefficients, deviation from ideality, the avalanche effect, and peak signal-to-noise ratios (PSNR).

## Methods

### *1. Aperiodic continued fractions and quartic irrational numbers*

Before we proceed to the development of our image encryption scheme, we shall first give a brief explanation on aperiodic continued fractions and quartic irrational numbers. An *infinite simple continued fraction* is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \frac{1}{\ddots}}}}} \tag{1}$$

where $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{N}$ for all positive integers $i$. The compact notation $[a_0; a_1, a_2, \dots]$ is normally used to denote such a fraction (Burton, 2007). Every irrational number $x$ can be expressed uniquely as an infinite simple continued fraction $[a_0; a_1, a_2, \dots]$, where $a_n = \lfloor x_n \rfloor$ for all $n \geq 0$ and

$$x_n = \begin{cases} x & \text{if } n = 0, \\ \dfrac{1}{x_{n-1} - a_{n-1}} & \text{if } n > 0. \end{cases} \tag{2}$$

A *quadratic irrational number* is an irrational number which is a root of an irreducible quadratic polynomial with integer coefficients (Havil, 2012). It is well known that the infinite simple continued fraction of a real number $x$ is periodic if and only if $x$ is a quadratic irrational number (Burton, 2007). Similarly, a *quartic irrational number* is an irrational number being a root of an irreducible quartic polynomial with integer coefficients.

From the above definitions, the irrational numbers $\sqrt{2}$ and $\sqrt{3}$ are therefore quadratic irrational numbers, for they are roots of the polynomial $x^2 - 2$ and $x^2 - 3$, respectively. Let $x_0 = \sqrt{2} + \sqrt{3}$. One can verify that $x_0$ is a root of the polynomial $x^4 - 10x^2 + 1 = 0$. Note that $x_0$ must be irrational since a rational root of the polynomial $x^4 - 10x^2 + 1$ would be $1$ or $-1$ if it existed (Young, 2010). It remains to show that the polynomial $x^4 - 10x^2 + 1$ is irreducible. Clearly, the polynomial has no linear factor since $1$ and $-1$ are not its roots. Suppose that

$$x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d) \tag{3}$$

for some $a, b, c, d \in \mathbb{Z}$. Equating the coefficients, we have

$$a + c = 0, \quad ac + b + d = -10, \quad ad + bc = 0, \quad bd = 1. \tag{4}$$

If $b = d = 1$, then we finally have $a^2 = 12$, which is impossible since $a \in \mathbb{Z}$. A similarly contradiction is also obtained if $b = d = -1$. Thus, the polynomial $x^4 - 10x^2 + 1$ is irreducible, so $x_0$ is a quartic irrational number. Moreover, it follows that the infinite simple continued fraction of $x_0$ is aperiodic.

## 2. Research methodology

Our research methodology for developing a new encryption scheme for RGB images consists of the following four main parts:

1. Develop an encryption algorithm which uses a quartic irrational number as the secret key.
2. Derive the decryption algorithm corresponding to our encryption algorithm.
3. Measure time consumption and the efficiency of our scheme in terms of correlation coefficients, deviation from ideality, the avalanche effect, and PSNR, using the five test images of size $512 \times 512$ as shown in Figure 1. All the three components of each test image are evaluated using all the four metrics.
4. Compare time consumption and the efficiency of our scheme to that of the schemes of Hamad *et al.* (2013) and Pareek (2012).

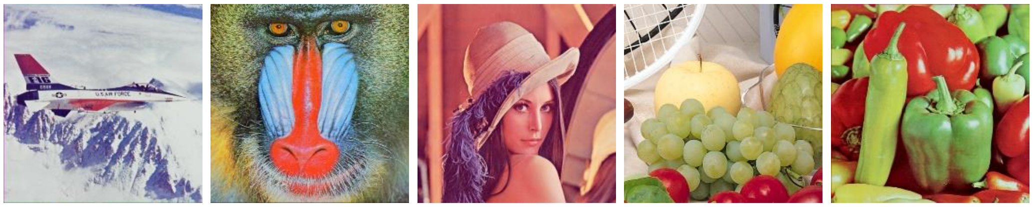

*Figure 1* The test images Airplane, Baboon, Fruits, Lena, and Peppers (University of Wisconsin-Madison, 2012).

### 2.1. The encryption algorithm

Our encryption algorithm consists of the following steps:

1. A sender and a recipient choose two positive integers $a, b$ such that $\sqrt{a} + \sqrt{b}$ is a quartic irrational number as their secret keys.

2. The sender then splits the red component of the plainimage into a number of sub-plainimages of size $4 \times 4$, say, $P_1, P_2, \ldots, P_N$.

3. For $i = 1, 2, \ldots, N$, repeat the following:

(a) Construct a $4 \times 4$ matrix $K_i$ which is invertible modulo $256$ from the infinite simple continued fraction expansion of $\sqrt{a}+\sqrt{b}$. For $K_1$, we form a $4 \times 4$ matrix rowwise using the first $16$ partial quotients of $\sqrt{a}+\sqrt{b}$. If the matrix is still singular modulo $256$, then we discard the first partial quotient, shift the remaining partial quotients, and insert a new partial quotient. Continue this process until the matrix is invertible modulo $256$. After that, all matrices $K_i$ are formed in a similar way for all $i \geq 2$.

(b) Let $C_i = P_i K_i^5 \bmod 256$, where $P_i$ is the $i^{\text{th}}$ sub-plainimage.

4. Arrange all matrices $C_i$ to form the red component of the cipherimage.

5. The green and blue components of the cipherimage can be obtained in a similar way by applying steps 2-4 to the corresponding components of the plainimage.

### 2.2. The decryption algorithm

Corresponding to our encryption algorithm, our decryption algorithm consists of the following steps:

1. The recipient splits the red component of the cipherimage into $N$ sub-cipherimages of size $4 \times 4$.

2. For $i = 1, 2, \ldots, N$, repeat the following:

(a) Construct $K_i$ as in the encryption algorithm.

(b) Calculate $P_i = C_i\left(K_i^5\right)^{-1} \bmod 256.$

3. Arrange all matrices $P_i$ to form the red component of the plainimage.

4. The green and blue components of the plainimage can be obtained in a similar way by applying steps 1-3 to the corresponding component of the cipherimage.

## 3. Encryption evaluation metrics

In this paper, the following four metrics are used for comparing the efficiency of our scheme with that of the schemes of Hamad *et al.* (2013) and Pareek (2012); see Abd El-Samie *et al.* (2014) for more details.

### 3.1. Correlation coefficients

Let $X = [x_{ij}]$ be an $m \times n$ matrix. Let $E(X)$ be the average of all entries of $X$ and define

$$D(X) = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(x_{ij} - E(X)\right)^2. \tag{5}$$

Moreover, for any $m \times n$ matrices $X = [x_{ij}]$ and $Y = [y_{ij}]$, we define

$$\operatorname{cov}(X,Y) = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(x_{ij} - E(X)\right)\left(y_{ij} - E(Y)\right). \tag{6}$$

According to Goldberg (1960), the *correlation coefficient* between entries at the same indices in $X$ and $Y$, denoted by $r_{XY}$, is defined by

$$r_{XY} = \begin{cases} \dfrac{\operatorname{cov}(X,Y)}{\sqrt{D(X)D(Y)}} & \text{if } D(X)D(Y) \neq 0, \\ 0 & \text{if } D(X)D(Y) = 0. \end{cases} \tag{7}$$

It can be proved that $-1 \leq r_{XY} \leq 1$ (Goldberg, 1960). The correlation $1$ indicates a perfect positive linear association, whereas the correlation $-1$ indicates a perfect negative linear association (Peat *et al.*, 2008). For a plainimage $P$ with the corresponding cipherimage $C$ of the same size, the value of $r_{PC}$ closer to zero indicates better quality of the encryption scheme (Abd El-Samie *et al.*, 2014).

*3.2. Histogram uniformity and deviation from ideality*

Abd El-Samie *et al.* (2014) suggests that an image encryption scheme should yield the cipherimage whose histogram is totally different from that of the plainimage and reveals a uniform distribution. To measure such uniformity numerically, one can use the *deviation from ideality*, which is defined by

$$D = \frac{1}{mn}\sum_{i=0}^{255}\left|h_i(C) - \frac{mn}{256}\right| \tag{8}$$

where $h_i(C)$ is the number of occurrences of pixels with intensity $i$ in the cipherimage $C$ of size $m \times n$. Clearly, the lower value of $D$ indicates better encryption quality of the scheme.

*3.3. PSNR*

In addition to visual inspection, one can measure the difference between a plainimage $P = [p_{ij}]$ and its cipherimage $C = [c_{ij}]$ of size $m \times n$ using the *peak signal-to-noise ratio* (PSNR), which is normally expressed in terms of decibel unit (Liu *et al.*, 2011). The PSNR is defined by

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{255^2 mn}{\sum_{i=1}^{m}\sum_{j=1}^{n}\left(c_{ij} - p_{ij}\right)^2}\right) \tag{9}$$

An image encryption scheme should maximize the difference between the plainimage and the cipherimage; this is indicated by the smaller PSNR.

*3.4. The avalanche effect*

Let $P$ be a plainimage and let $P'$ be a modified plainimage obtained by making a single bit change to $P$. Let $C$ and $C^{'}$ be the cipherimage associated to $P$ and $P'$, respectively. The *avalanche effect* is defined as the percentage of different bits between $C$ and $C'$. According to Abd El-Samie *et al.* (2014), an encryption algorithm is considered to possess good diffusion if $C$ and $C'$ differ from each other in half of their bits.

## Results

In our experiment, all test images are encrypted and their corresponding cipherimages are decrypted using the schemes of Hamad *et al.* (2013), Pareek (2012), and our scheme. We use $\mathbf{10}$ as the secret key for the scheme of Hamad *et al.* (2013), the vector

$$k = [119, 40, 161, 213, 216, 63, 224, 115, 130, 81, 118, 35, 175, 190, 131, 32, 130, 81] \tag{10}$$

as the secret key for the scheme of Pareek (2012), and $a = 2, b = 3$ as the secret keys for our scheme. Recall that $\sqrt{a} + \sqrt{b}$ is a quartic irrational number.

*1. Encrypted and decrypted test images*

Applying the schemes of Hamad *et al.* (2013), Pareek (2012), and our scheme to all five test images (*left*), the corresponding encrypted images (*center*) and decrypted images (*right*) are as shown in Figures 2-4.

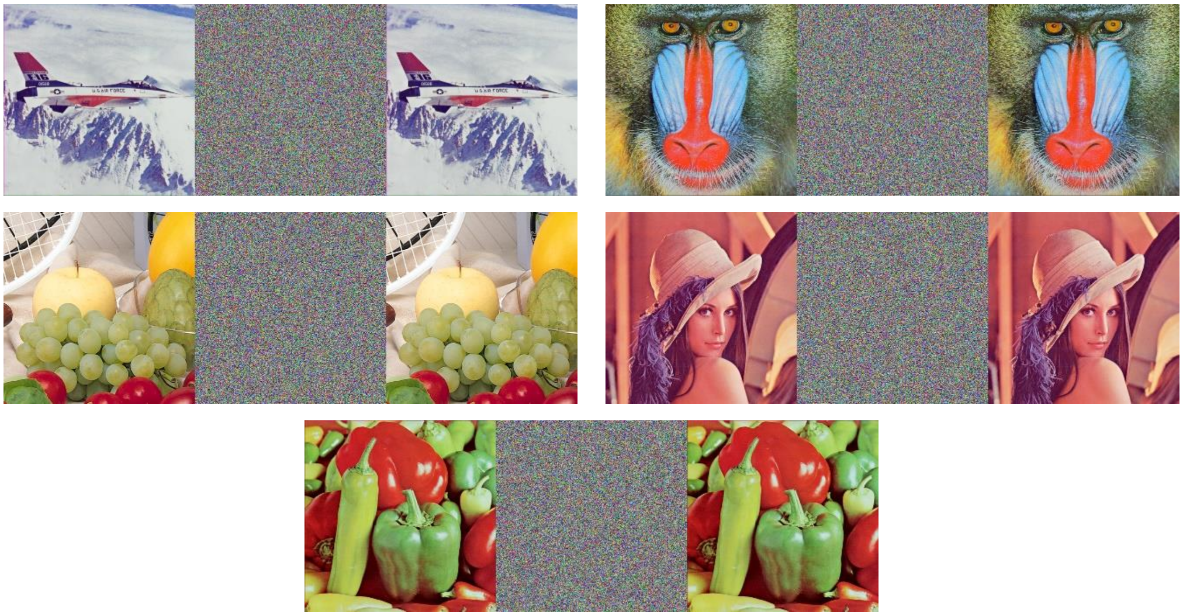

*Figure 2* Airplane, Baboon, Fruits, Lena, and Peppers images after applying the scheme of Hamad *et al.* (2013).

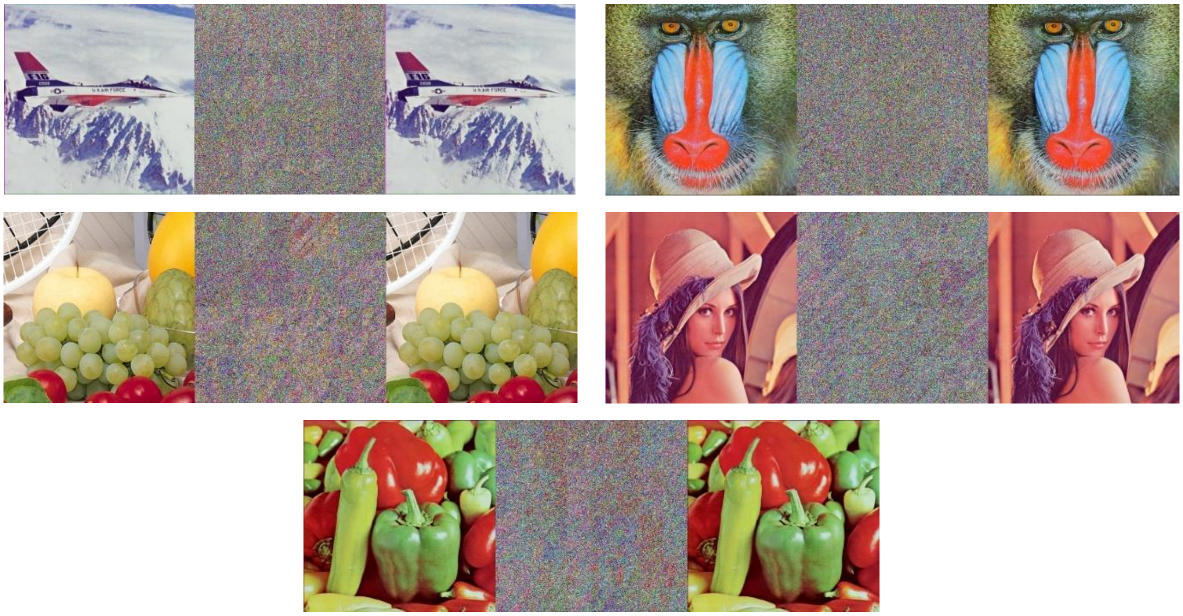

*Figure 3* Airplane, Baboon, Fruits, Lena, and Peppers images after applying the scheme of Pareek (2012).

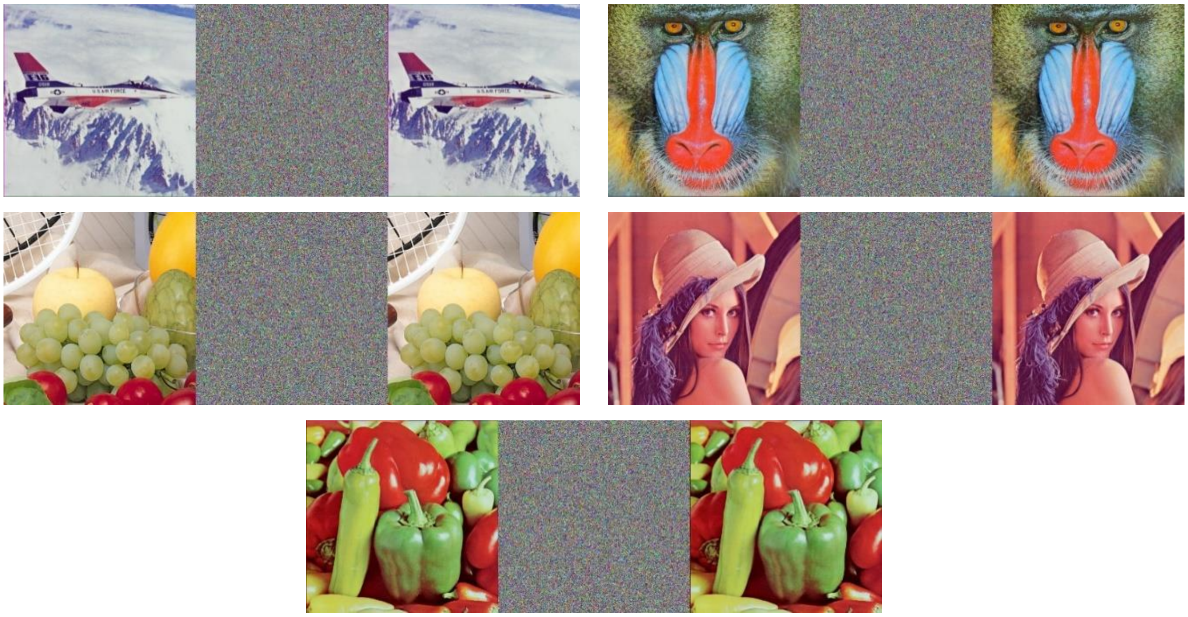

*Figure 4* Airplane, Baboon, Fruits, Lena, and Peppers images after applying our scheme.

*2. Elapsed time for encryption and decryption*

In our experiment, each test image is timed thrice and the average time is calculated for both encryption and decryption. The average time consumption for encrypting and decrypting each test image using the schemes of Hamad *et al.* (2013), Pareek (2012), and our scheme is shown in Table 1. Our computation is done on a 64-bit computer with 2.20 GHz microprocessor and 8 GB random access memory.

*Table 1* Average time consumption for encryption and decryption.

| Image | Average time consumption after applying each scheme (second) | | | | | |
|---|---|---|---|---|---|---|
| | Hamad *et al.* (2013) | | Pareek (2012) | | Our scheme | |
| | Encryption | Decryption | Encryption | Decryption | Encryption | Decryption |
| Airplane | 337.80 | 329.45 | 12670.70 | 12995.03 | 165.23 | 165.93 |
| Baboon | 329.82 | 326.13 | 12691.49 | 12640.31 | 178.51 | 178.65 |
| Fruits | 348.70 | 353.29 | 12387.89 | 12511.17 | 162.15 | 162.00 |
| Lena | 372.23 | 408.04 | 12329.16 | 14548.93 | 162.32 | 162.43 |
| Peppers | 324.36 | 320.50 | 12305.00 | 12249.68 | 166.79 | 166.67 |

*3. Correlation between original and encrypted test images*

The correlation coefficients between the original test images and their associated encrypted versions obtained from the schemes of Hamad *et al.* (2013), Pareek (2012), and our scheme are shown in Table 2.

***Table 2*** Correlation coefficients for each color component of the test images.

| Image | Color component | Correlation coefficients for each scheme | | |
|---|---|---|---|---|
| | | Hamad *et al.* (2013) | Pareek (2012) | Our scheme |
| Airplane | Red | 0.000008 | 0.002602 | 0.000689 |
| | Green | -0.000676 | 0.001874 | -0.002629 |
| | Blue | -0.001857 | 0.000258 | 0.001665 |
| Baboon | Red | 0.002721 | -0.002271 | -0.000507 |
| | Green | 0.002724 | 0.007182 | 0.000251 |
| | Blue | -0.000581 | -0.003501 | -0.001747 |
| Fruits | Red | 0.000614 | -0.033039 | 0.002441 |
| | Green | 0.002633 | -0.014993 | -0.001519 |
| | Blue | 0.001529 | -0.017250 | -0.001257 |
| Lena | Red | 0.001720 | 0.011027 | 0.001309 |
| | Green | 0.002564 | 0.001478 | -0.004718 |
| | Blue | 0.000976 | -0.002466 | 0.000008 |
| Peppers | Red | 0.000530 | 0.003246 | 0.004026 |
| | Green | 0.000094 | 0.001132 | 0.003660 |
| | Blue | 0.001373 | -0.002291 | -0.001422 |

*4. Deviation from ideality*

The deviation from ideality of each encrypted image is calculated per component as shown in Table 3

*Table 3* Deviation from ideality for each color component of the test images.

| Image | Color component | Deviation from ideality for each encrypted method | | |
|---|---|---|---|---|
| | | Hamad *et al.* (2013) | Pareek (2012) | Our scheme |
| Airplane | Red | 0.024590 | 0.200020 | 0.024750 |
| | Green | 0.023727 | 0.060425 | 0.025391 |
| | Blue | 0.024887 | 0.037704 | 0.027664 |
| Baboon | Red | 0.026085 | 0.103020 | 0.025925 |
| | Green | 0.023842 | 0.044930 | 0.027382 |
| | Blue | 0.025742 | 0.031227 | 0.025162 |
| Fruits | Red | 0.024979 | 0.185608 | 0.025017 |
| | Green | 0.024101 | 0.057060 | 0.022896 |
| | Blue | 0.025063 | 0.048294 | 0.025124 |
| Lena | Red | 0.026321 | 0.128967 | 0.024635 |
| | Green | 0.025551 | 0.093933 | 0.023689 |
| | Blue | 0.024429 | 0.145180 | 0.025200 |
| Peppers | Red | 0.025330 | 0.151375 | 0.024971 |
| | Green | 0.023697 | 0.038773 | 0.024078 |
| | Blue | 0.022957 | 0.082321 | 0.024147 |

Moreover, the histograms of each intensity (the $x$-axis) against the number of pixels having that intensity (the $y$-axis) are obtained for each encrypted test image as shown in Figures 5-9.

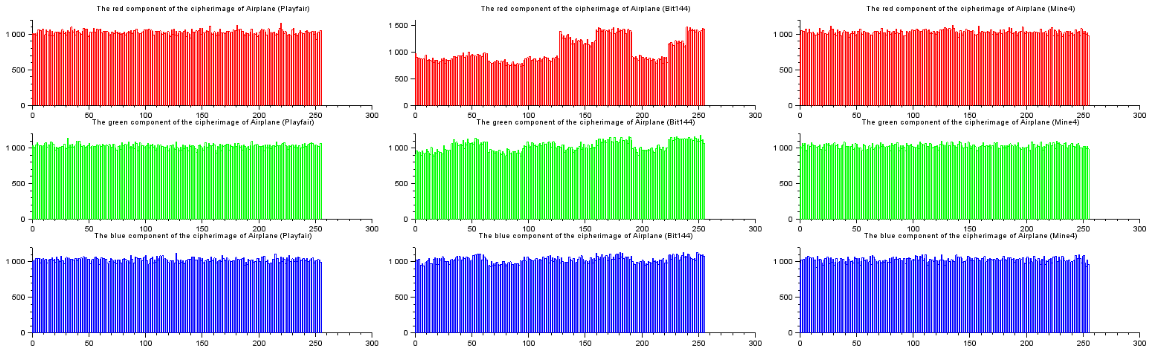

*Figure 5* Histograms of encrypted Airplane by Hamad *et al.* (2013), Pareek (2012), and our scheme.

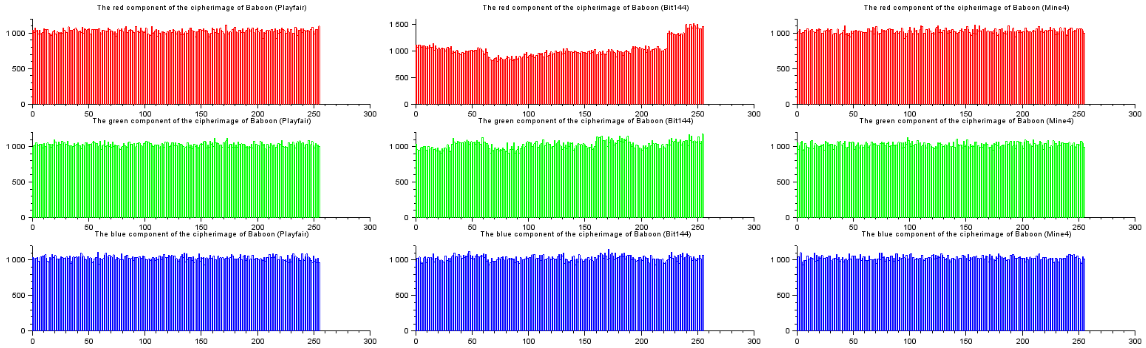

*Figure 6* Histogram of encrypted Baboon by Hamad *et al.* (2013), Pareek (2012), and our scheme.

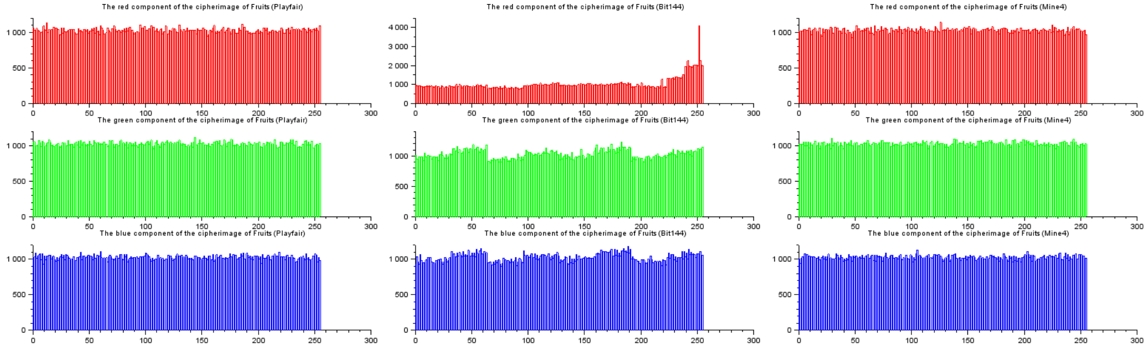

*Figure 7* Histogram of encrypted Fruits by Hamad *et al.* (2013), Pareek (2012), and our scheme.

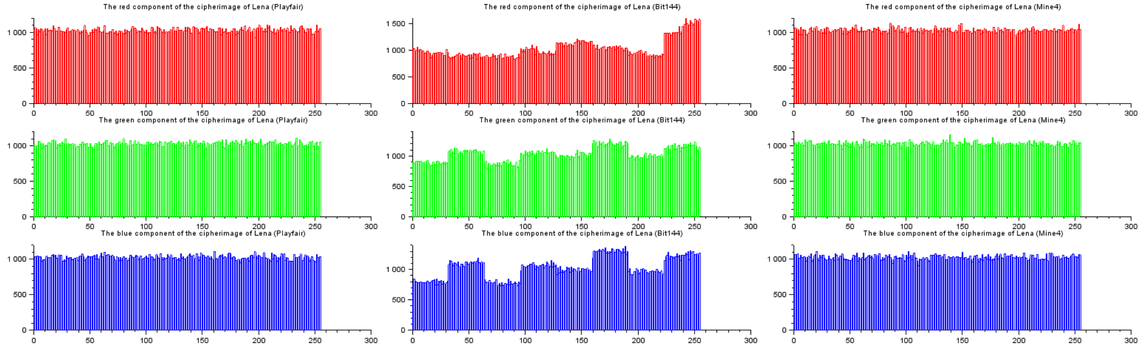

*Figure 8* Histogram of encrypted Lena by Hamad *et al.* (2013), Pareek (2012), and our scheme.

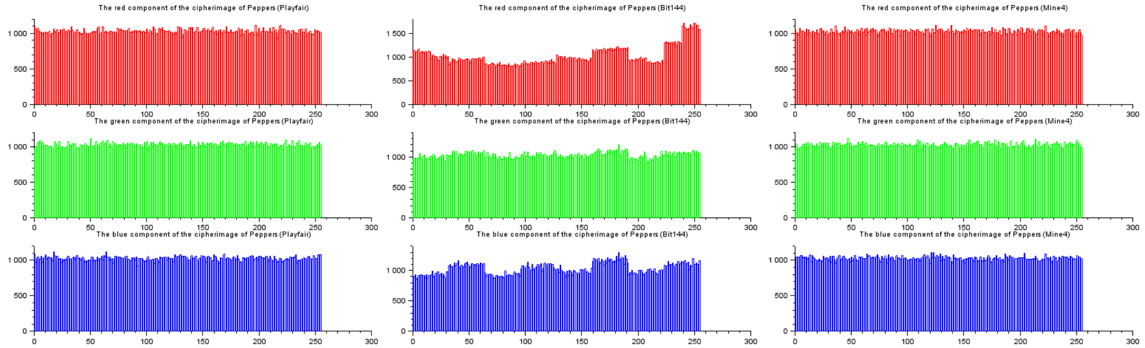

*Figure 9* Histogram of encrypted Peppers by Hamad *et al.* (2013), Pareek (2012), and our scheme.

## 5. The PSNR between original and encrypted test images

The PSNR between each test image and its associated encrypted version is shown in Table 4.

*Table 4* The PSNR for each color component of the test images.

| Image | Color component | The PSNR for each scheme | | |
|---|---|---|---|---|
| | | Hamad *et al.* (2013) | Pareek (2012) | Our scheme |
| Airplane | Red | 8.149508 | 8.602409 | 8.163664 |
| | Green | 7.829343 | 7.931056 | 7.842437 |
| | Blue | 7.933073 | 7.989850 | 7.963416 |
| Baboon | Red | 8.769794 | 8.551803 | 8.769361 |
| | Green | 9.247017 | 9.269383 | 9.241378 |
| | Blue | 8.366375 | 8.349004 | 8.366512 |
| Fruits | Red | 7.655114 | 7.880764 | 7.673852 |
| | Green | 8.163299 | 8.115256 | 8.155233 |
| | Blue | 8.550865 | 8.477424 | 8.537750 |
| Lena | Red | 7.873181 | 8.117700 | 7.856224 |
| | Green | 8.561918 | 8.442597 | 8.544412 |
| | Blue | 9.626719 | 9.426465 | 9.604580 |
| Peppers | Red | 9.106543 | 8.981876 | 9.121116 |
| | Green | 7.628512 | 7.623320 | 7.641187 |
| | Blue | 7.666607 | 7.535952 | 7.659207 |

*6. Percentage of the avalanche effect*

The avalanche effect is calculated for three random bit changes and the average is shown in Table 5.

*Table 5* The average avalanche effect towards the test images.

| Image | The average avalanche effect for each scheme (%) | | |
|---|---|---|---|
| | Hamad *et al.* (2013) | Pareek (2012) | Our scheme |
| Airplane | 0.000148 | 19.291 | 0.000244 |
| Baboon | 0.000095 | 19.500 | 0.000238 |
| Fruits | 0.000148 | 19.500 | 0.000297 |
| Lena | 0.000159 | 19.412 | 0.000244 |
| Peppers | 0.000133 | 19.509 | 0.000244 |

## Discussion

From Figure 4, it is evident that our proposed image encryption scheme can be reversed to recover the original five test images. Recall our encryption and decryption algorithms. One can easily verify that

$$C_i\left(K_i^5\right)^{-1} = \left(P_iK_i^5\right)\left(K_i^5\right)^{-1} = P_i\left(K_i^5\left(K_i^5\right)^{-1}\right) = P_iI = P_i \mod 256 \tag{11}$$

for all $i = 1, 2, \ldots, N$, where $I$ is the $4 \times 4$ identity matrix and $N$ is the number of sub-plainimages of size $4 \times 4$.

Based on visual inspection, one can see from Figures 2 and 4 that the scheme of Hamad *et al.* (2013) and our scheme can provide visually unrecognizable encrypted images. Unfortunately, one can see from Figure 3 that the encrypted images obtained from the scheme of Pareek (2012) are partially recognizable, particularly for the test images Fruits, Lena, and Peppers. Thus, further analysis is required in order to compare the efficiency of our scheme with that of the scheme of Hamad *et al.* (2013).

In terms of time consumption, one can see from Table 1 that the average encryption time using the schemes of Hamad *et al.* (2013), Pareek (2012), and our scheme is between 324.36-372.23, 12305.00-12691.49, and 162.15-178.51 seconds, respectively. The average decryption time using the schemes of Hamad *et al.* (2013), Pareek (2012), and our scheme is between 320.50-408.04, 12249.68-14548.93, and 162.00-178.65 seconds, respectively. Therefore, our scheme clearly uses the least amount of time for encryption and decryption.

For the correlation coefficients, one can see from Table 2 that the scheme of Hamad *et al.* (2013) provides the correlation coefficients whose magnitude ranges between 0.000008-0.002724, while the magnitude of the correlation coefficients obtained from the scheme of Pareek (2012) and our scheme ranges between 0.000258-

0.033039 and 0.000008-0.004718, respectively. Thus, our scheme yields the correlation coefficients which are closer to zero than those provided by the scheme of Pareek (2012). However, the range of magnitude of our correlation coefficients is slightly wider than that obtained from the scheme of Hamad *et al.* (2013).

From Figures 5-9, one can easily see that, unlike the scheme of Pareek (2012), our scheme and the scheme of Hamad *et al.* (2013) yield a uniformly-distributed histogram of intensities for all encrypted test images. In addition, one can see from Table 3 that the deviation from ideality of all encrypted test images obtained from the schemes of Hamad *et al.* (2013), Pareek (2012), and our scheme ranges between 0.022957-0.026321, 0.031227-0.200020, and 0.022896-0.027664, respectively. Hence, our scheme provides the range of deviation from ideality which is close to zero and almost similar to that provided by the scheme of Hamad *et al.* (2013).

In terms of the PSNR, one can see from Table 4 that the ranges of PSNR obtained from the schemes of Hamad *et al.* (2013), Pareek (2012), and our scheme are between 7.628512-9.626719, 7.535952-9.426465, and 7.641187-9.604580, respectively. Therefore, the scheme of Pareek (2012) gives the smallest PSNR, whereas our scheme provides a range of the PSNR which lies within the one provided by the scheme of Hamad *et al.* (2013).

Finally, from Table 5, one can see that the average avalanche effect obtained from the schemes of Hamad *et al.* (2013), Pareek (2012), and our scheme ranges between 0.000095%-0.000159%, 19.291%-19.509%, and 0.000238%-0.000297%, respectively. Therefore, it is obvious that the scheme of Pareek (2012) yields the highest average percentage of the avalanche effect, whereas the percentage of the avalanche effect provided by our scheme is approximately twice the one provided by the scheme of Hamad *et al.* (2013).

## Conclusions

The scheme of Hamad *et al.* (2013) relies heavily on encrypting each color component of the plainimage using a modified version of the Playfair cipher with $16 \times 16$ table, whose entries are randomly generated by a given seed. After that, the exclusive disjunction (exclusive-or) of the scrambled image and the generated random mask of the size is then computed. In contrast, the scheme of Pareek (2012) uses a secret key of 144 bits and divides the plainimage into a number of blocks of the same length. Each block is then passed through substitution process, before the permutation process is applied for five iterations. Although both schemes yield high-quality cipherimages, one of their main disadvantages is the time consumption during encryption and decryption.

In this paper, we develop an image encryption scheme which uses an infinite simple continued fraction of a quartic irrational number as the secret key. The efficiency of our scheme is measured in terms of correlation coefficients, deviation from ideality, the avalanche effect, and PSNR. Using the test images Airplane, Baboon, Fruits, Lena, and Peppers, our scheme is compared with the ones of Hamad *et al.* (2013) and Pareek (2012). In overall, we find that our image encryption scheme requires the least amount of computational time and is more effective in providing visually-unrecognizable encrypted images than the scheme of Pareek (2012). Finally, except for the correlation coefficients, our scheme is also slightly more effective than the scheme of Hamad *et al.* (2013).

## Acknowledgements

The authors would like to thank the Department of Mathematics, Faculty of Science, Khon Kaen University for its support towards this research.

## References

Abd El-Samie, F.E., Ahmed, H.E.H., Elashry, I.F., Shahieen, M.H., Faragallah, O.S., El-Rabaie, E.-S.M., & Alshebeili, S.A. (2014). *Image Encryption: A Communication Perspective*. Boca Raton: CRC Press.

Burton, D.M. (2007). *Elementary Number Theory*. (6th ed.). New York: McGraw-Hill.

Goldberg, S. (1960). *Probability: An Introduction*. Englewood Cliffs: Prentice-Hall.

Hamad, S., Khalifa, A., Elhadad, A., & Rida, S.Z. (2013). A modified Playfair cipher for encrypting digital images. *Journal of Communication and Computer Engineering*, *3*(2), 1-9.

Havil, J. (2012). *The Irrationals: A Story of the Numbers You Can't Count on*. Princeton: Princeton University Press.

Liu, Z., Xu, L., Liu, T., Chen, H., Li, P., Lin, C., Liu, S. (2011). Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. *Optics Communications*, *284*, 123-128.

Özdemir, A.S., & Yaprakdal, A.B. (2010). Using the relationship between periodic continued fraction and quadratic irrationals: ASAB-II cipher. *Istanbul Aydın Üniversitesi Dergisi*, *2*, 131-149.

Pareek, N.K. (2012). Design and analysis of a novel digital image encryption scheme. *International Journal of Network Security & Its Applications*, *4*(2), 95-108.

Peat, J., Barton, B., & Elliott, E. (2008). *Statistics Workbook for Evidence-based Health Care*. Chichester: Wiley.

University of Wisconsin-Madison. (2012). *Public-domain Test Images for Homework and Projects*. Retrieved June 11, 2018, from http://homepages.cae.wisc.edu/~ece533/images/index.html

Young, C.Y. (2010). *Precalculus*. Hoboken: Wiley.