International Journal of Mathematical, Engineering and Management Sciences
Vol. 7, No. 3, 399-416, 2022
https://doi.org/10.33889/IJMEMS.2022.7.3.027

Image Cryptography Based On A Second-Order QRT Difference Equation

Agus Sutrisno
Department of Mathematics,
Faculty of Mathematics and Natural Science,
Universitas Lampung, Bandar Lampung, Indonesia.
E-mail: agus.sutrisno@fmipa.unila.ac.id

Aang Nuryaman
Department of Mathematics,
Faculty of Mathematics and Natural Science,
Universitas Lampung, Bandar Lampung, Indonesia.
Corresponding author: aang.nuryaman@fmipa.unila.ac.id

Muslim Ansori
Department of Mathematics,
Faculty of Mathematics and Natural Science,
Universitas Lampung, Bandar Lampung, Indonesia.
E-mail: muslim.ansori@fmipa.unila.ac.id

Ahmad Faisol
Department of Mathematics,
Faculty of Mathematics and Natural Science,
Universitas Lampung, Bandar Lampung, Indonesia.
E-mail: ahmadfaisol@fmipa.unila.ac.id

(Received on September 11, 2021; Accepted on February 02, 2022)

Abstract

The use of mathematical concepts of mapping in cryptography provides advantages in securing text or image data. The qualitative properties of mapping can preserve data that is kept confidential. Two of the essential properties in the mapping are the reversible and the preserving area. In this article, besides constructing a linear mapping derived from a second-order QRT difference equation and examining its qualitative properties, the coding procedure is used to encrypt text and fractal images based on the two-dimensional linear maps. For the digital text and image security algorithms, we developed the pseudo code algorithm implemented in Mathematica®. The proposed encoding technique will be compared with a 2D mKdV linear map to demonstrate its efficacy.

Keywords- Fractal image, Cryptography, 2D QRT linear map, 2D mKdV linear map.

1. Introduction

Cryptography is the science and study of methods for protecting data in computer and communication systems from unauthorized disclosure and modification (Denning, 1982). Mathematical principles, which are used in operating systems, database systems, and computer networks, play an important role in cryptography. There are many algorithms for securing data that involve mathematics; one of which can be found in (ElGamal, 1985). In addition to mathematical principles, maps can be involved in encryption-decryption algorithms. A cryptographic encoding algorithm for a digital image was studied in (Munir, 2015) that utilized

Arnold's Cat Map (ACM), whereas, in (Hidayat & Afrianto, 2017), the Logistic Map was employed. The Nonlinear Chaotic Algorithm (NCA) has also been featured (Ronsen et al., 2014). Recently, a number of different encoding algorithms have emerged. Two of these approaches were developed in 2017 in (Abbadi et al., 2017) and (Fu et al., 2017). In (Abbadi et al., 2017), the authors proposed an algorithm based on scrambling pixel positions and changing the pixels' intensities. The algorithm results in adjacent pixels in the encrypted image that are highly uncorrelated, yielding high entropy and a mostly uniform distribution. It provides better results than prior algorithms. In (Fu et al., 2017), the authors suggested a fast color image encryption scheme employing both permutation and substitution key streams that is quantified from a sequence extracted from the orbit of Chen's chaotic system.

In principle, chaos dynamics have various advantages applicable to cryptography, such as pseudo-randomness, ergodic property, sensitivity to initial values, and controlling. Therefore, many researchers have proposed many image encryption algorithms in recent years. For example, the image encryption schemes based on a random walk and hyperchaotic systems (Fan et al., 2022), the hyper-chaotic Lorenz system and hash function (Z. Li et al., 2018), the chaotic APFM (Amplitude Phase Frequency Model) nonlinear Adaptive Filter (Fan et al., 2018), and the novel 2D sine–cosine cross-chaotic map (M. Li et al., 2021). For classic maps, an encoding algorithm for digital images can be studied through a chaotic cryptosystem for images that is based on Hènon and ACM (Soleymani et al., 2014), image encryption based on 2D linear sine-Gordon and mKdV maps (Zakaria et al., 2021), and image encryption based on independent component analysis and ACM (Abbas, 2016). A cryptographic encoding algorithm using a map was studied in (Revanna & Keshavamurthy, 2017), (Ali Abaas & Kareem Shibeeb, 2015), and (Munir, 2012) for all data files. In this article, a mapping application for cryptographic encoding algorithms for digital images will be described (see (Notiragayu & Zakaria, 2019) for an application for digital texts using a different map). Our proposed encryption-decryption algorithm uses a linear map derived from the QRT (Quispel, Robert, and Thomson) map. The QRT map is a symmetric, integrable, and measure-preserving 12-parameter family map (see (Zakaria & Tuwankotta, 2016), (Quispel & Roberts, 1988), and (Quispel & Roberts, 1989)).

This article consists of four sections. In section 1, the previous research results related to the use of mathematical concepts and algorithms in cryptography are provided. In section 2, a case study of an encryption-decryption algorithm for textual data based on a 2D map derived from a QRT mapping is provided. Section 3 discusses implementing the encryption-decryption algorithm for image data in the Mathematica® programming language. In section 4, the results are provided, along with concluding remarks.

2. Methods and Materials

2.1 A Cryptographic Encryption-Decryption Method: An Algorithm Based on A 2D Linear Map (An Illustration Utilizing Textual Data)

Consider the following linear map:

$$\mathbf{x}_{n+1} = \mathbf{f}_{\alpha}(\mathbf{x}_n). \tag{1}$$

Where

$$\begin{aligned} \mathbf{f}_{\alpha}:\ & \mathbb{R}^2 \to \mathbb{R}^2 \\ & (x, y) \mapsto (-\alpha y, x) \end{aligned} \tag{2}$$

The 2D map in Eq. (1) is a linear map with an arbitrary parameter $\alpha \neq 0$. Based on this map, we will construct a standard encryption-decryption algorithm for textual data. The coding algorithm for textual data is created as follows:

Encryption:

(a) The text must be divided into two datasets, for example, $F(l)$ and $G(m)$; $l, m \in \mathbb{N}$ are the text lengths (in characters). Note that we must assume the same number of characters, i.e., $l = m = n \in \mathbb{N}$, when a rational map is used.
(b) Convert the text data in F and G into numerical data using ASCII code. Note that a different code could be used.
(c) The value of $\alpha \neq 0$ is fixed and used as the key value.
(d) The map **f** is iterated *r* times; $\mathbf{f}^0 < \mathbf{f}^r; r \in \mathbb{N}$.

Decryption:

(a) Re-use the parameter value $\alpha \neq 0$. Due to the reversible map, the inverse of the map, i.e., $\mathbf{f}^{-r}; r \in \mathbb{N}$, can be used to obtain the original numerical data.
(b) Re-use the ASCII code to change the numerical data into textual data.

To show how our proposed encryption-decryption algorithm works, the following textual data (*in italics*) will be hidden in numerical format using the mapping in Eq. (1)
"*In the next section, we will use the map in Eq. (7) to construct a cryptographic algorithm for the digital image. We will use Mathematica® scripts to implement our proposed encryption-description algorithm. In addition, we will compare the encryption-decryption results for the map in Eq. (7) with the ACM results.*"

Encryption:

(a) Divide the textual data into two parts, F_{text} and G_{text} ,

$$F_{\text{text}} = \begin{pmatrix} \text{In the next section, we will use the map in Eq. } (7) \text{ to} \\ \text{construct a cryptographic algorithm for the digital} \\ \text{image. We use Mathematica® scripts to implement our} \end{pmatrix}$$

and

$$G_{\text{text}} = \begin{pmatrix} \text{proposed encryption-description algorithm. In addition,} \\ \text{we compare encryption-decryption results} \\ \text{between the map in Eq. } (7) \text{ and ACM.} \end{pmatrix}$$

Notethat F_{text} and G_{text} have $l = 158$ and $m = 159$ characters, respectively. We have to add one particular character to $l = m = 159$. Then, so that the text does not change the meaning, we can choose the unique character "space" (ASCII code = 32) at the end of the F_{text}.

(b) Using ASCII code to convert the elements of F_{text} and G_{text} into numerical data, we arrive at

$$F_{\text{num}}=\begin{pmatrix} 73,110,32,116,104,101,32,110,101,120, \\ 116,32,115,101,99,116,105,111,110,32, \\ \vdots, \\ 116,115,32,116,111,32,105,109,112,108, \\ 101,109,101,110,116,32,111,117,114,32 \end{pmatrix}$$

and

$$G_{\text{num}}=\begin{pmatrix} 112,114,111,112,111,115,101,100,32,101, \\ 110,99,114,121,112,116,105,111,110,45, \\ \vdots, \\ 111,108,100,39,115,32,67,97,116,32, \\ 77,97,112,32,40,65,67,77,41,46 \end{pmatrix}$$

(c) Consider $x_i \in F_{\text{num}}$ and $y_i \in G_{\text{num}}$, $i = 1,2,\dots,l = m$. Therefore, we can rewrite Eq. (2) with $(x_i, y_i) \mapsto (-\alpha\, y_i, x_i)$.

(d) Choose values of α and r for the key value and number of iterations, respectively. For example, let $\alpha = \tan 0.123451123$ and $r = 66$.

(e) Compute $\mathbf{f}$ for Eq. (1) as follows

$$\mathbf{f}^0 = identity = (x, y)$$
$$\mathbf{f}^1 = \mathbf{f}(x, y) = (-\alpha y, x)$$
$$\mathbf{f}^2 = \mathbf{f}\left(\mathbf{f}^1(x, y)\right) = \mathbf{f}(-\alpha y, x) = (-\alpha x, -\alpha y)$$
$$\mathbf{f}^3 = \mathbf{f}\left(\mathbf{f}^2(x, y)\right) = \mathbf{f}(-\alpha x, -\alpha y) = \left(\alpha^2 y, -\alpha x\right)$$
$$\mathbf{f}^4 = \mathbf{f}\left(\mathbf{f}^3(x, y)\right) = \mathbf{f}\left(\alpha^2 y, -\alpha x\right) = \left(\alpha^2 x, \alpha^2 y\right)$$
$$\vdots$$
$$\mathbf{f}^r = \mathbf{f}\left(\mathbf{f}^{r-1}(x, y)\right) = \begin{cases} \left((-\alpha)^{\left\lceil \frac{r}{2} \right\rceil} y, (-\alpha)^{\left\lfloor \frac{r}{2} \right\rfloor} x\right), r = odd \\ \left((-\alpha)^{\left\lceil \frac{r}{2} \right\rceil} x, (-\alpha)^{\left\lfloor \frac{r}{2} \right\rfloor} y\right), r = even \end{cases}$$

(f) Thus, for $r = 66$ and $\alpha = \tan 0.123451123$, we have $\mathbf{f}^{66}(x, y)$ in which

$$x = \begin{pmatrix} -1.3855446\times 10^{(-28)}, -1.4102865\times 10^{(-28)}, -1.3731737\times 10^{(-28)}, \\ -1.3855446\times 10^{(-28)}, -1.3731737\times 10^{(-28)}, -1.4226574\times 10^{(-28)}, \\ -1.2494643\times 10^{(-28)}, -1.2370934\times 10^{(-28)}, -3.9586988\times 10^{(-29)}, \\ ,\cdots, \\ -1.1999806\times 10^{(-28)}, -1.3855446\times 10^{(-28)}, -3.9586988\times 10^{(-29)}, \\ -4.9483735\times 10^{(-29)}, -8.0411070\times 10^{(-29)}, -8.2885257\times 10^{(-29)}, \\ -9.5256191\times 10^{(-29)}, -5.0720829\times 10^{(-29)}, -5.6906296\times 10^{(-29)}. \end{pmatrix}$$

and

$$y = \begin{pmatrix} 7.2780692\times 10^{(-28)}, 1.0966954\times 10^{(-27)}, 3.1903865\times 10^{(-28)}, \\ 1.1565151\times 10^{(-27)}, 1.0368756\times 10^{(-27)}, 1.0069657\times 10^{(-27)}, \\ 3.1903865\times 10^{(-28)}, 1.0966954\times 10^{(-27)}, 1.0069657\times 10^{(-27)}, \\ ,\cdots, \\ 1.0867254\times 10^{(-27)}, 1.0069657\times 10^{(-27)}, 1.0966954\times 10^{(-27)}, \\ 1.1565151\times 10^{(-27)}, 3.1903865\times 10^{(-28)}, 1.1066653\times 10^{(-27)}, \\ 1.1664851\times 10^{(-27)}, 1.1365752\times 10^{(-27)}, 3.1903865\times 10^{(-28)} \end{pmatrix}$$

Decryption:

(a) Re-use the parameter $\alpha = \tan 0.123451123$.

(b) Consider the inverse map for the map in Eq. (1), namely,

$$\mathbf{w}_{n+1} = \mathbf{f}_{\alpha}\left(\mathbf{w}_n\right), \tag{3}$$

where

$$\begin{aligned} \boldsymbol{f}_{\alpha}^{-1}\colon \quad \mathbb{R}^2 \quad &\rightarrow \quad \mathbb{R}^2 \\ (w_1, w_2) \quad &\mapsto \quad (w_2, -\alpha^{-1} w_1) \end{aligned} \tag{4}$$

(c) Compute $\mathbf{f}_{\alpha}^{-r}$ for Eq. (4) as following

$$\mathbf{f}_{\alpha}^{-1} = \mathbf{f}_{\alpha}^{-1}\left(w_1, w_2\right) = \left(w_2, -\alpha^{-1} w_1\right)$$

$$\mathbf{f}_{\alpha}^{-2} = \mathbf{f}_{\alpha}^{-1}\left(\mathbf{f}_{\alpha}^{-1}\left(w_1, w_2\right)\right) = \mathbf{f}_{\alpha}^{-1}\left(w_2, -\alpha^{-1} w_1\right) = \left(-\alpha^{-1} w_1, -\alpha^{-1} w_2\right)$$

$$\mathbf{f}_{\alpha}^{-3} = \mathbf{f}_{\alpha}^{-1}\left(\mathbf{f}_{\alpha}^{-2}\left(w_1, w_2\right)\right) = \mathbf{f}_{\alpha}^{-1}\left(-\alpha^{-1} w_1, -\alpha^{-1} w_2\right) = \left(-\alpha^{-1} w_2, \alpha^{-2} w_1\right)$$

$$\mathbf{f}_{\alpha}^{-4} = \mathbf{f}_{\alpha}^{-1}\left(\mathbf{f}_{\alpha}^{-3}\left(w_1, w_2\right)\right) = \mathbf{f}_{\alpha}^{-1}\left(-\alpha^{-1} w_2, \alpha^{-2} w_1\right) = \left(\alpha^{-2} w_1, \alpha^{-2} w_2\right)$$

$$\vdots$$

$$\mathbf{f}_{\alpha}^{-r} = \mathbf{f}_{\alpha}^{-1}\left(\mathbf{f}^{r-1}\left(w_1, w_2\right)\right) = \begin{cases} \left(\left(-\alpha\right)^{-\left\lfloor \frac{r}{2} \right\rfloor} w_2, \left(-\alpha\right)^{-\left\lceil \frac{r}{2} \right\rceil} w_1\right), r = odd \\ \left(\left(-\alpha\right)^{-\left\lfloor \frac{r}{2} \right\rfloor} w_1, \left(-\alpha\right)^{-\left\lceil \frac{r}{2} \right\rceil} w_2\right), r = even \end{cases}$$

Therefore, for $\mathbf{f}_{\alpha}^{-66}$ and after applying common Round(.), we have the following data

$$w_1 = \begin{pmatrix} 73,110,32,116,104,101,32,110,101,120, \\ 116,32,115,101,99,116,105,111,110,32, \\ \vdots, \\ 116,115,32,116,111,32,105,109,112,108, \\ 101,109,101,110,116,32,111,117,114,32 \end{pmatrix} = F_{\text{num}}$$

and

$$w_2 = \begin{pmatrix} 112,114,111,112,111,115,101,100,32,101, \\ 110,99,114,121,112,116,105,111,110,45, \\ \vdots, \\ 111,108,100,39,115,32,67,97,116,32, \\ 77,97,112,32,40,65,67,77,41,46 \end{pmatrix} = G_{\text{num}}$$

(d) Converting the numerical data in w_1 and w_2 into textual data using ASCII code, we arrive back at the original textual data (F_{text} and G_{text}).

(e) Finish.

2.2 Mathematica® Programming for Implementing the Encryption-Decryption Algorithm Based on 2D Mapping: An Illustration

The Mathematica® system spans most technical computing areas, including neural networks, machine learning, image processing, geometry, data science, and visualization. The system is used in many technical, scientific, engineering, mathematical, and computing fields (Wolfram Research Inc., 2019), (Shifrin, 2008), and (Wellin, 2016). Wolfram Research, the creators of Mathematica®, always make phenomenal changes when updating. In version 9 or later,Mathematica® can be used to analyze and process 2D and 3D images using highly optimized algorithms. For example, it can be used to analyze orientations in an image, which requires computing and plotting an image's orientation distribution. In this subsection, Mathematica® v.9 software will be used to implement our proposed encryption-decryption algorithm from subsection 2.1 (see (Wellin, 2016) for general coding procedures used in Mathematica®). The following Mathematica® instructions can be used to implement the decryption algorithm (see (Notiragayu & Zakaria, 2019)) for an alternative map.

```
str1=StringTake[text,{1,Round[StringLength[text]/2]}]
str2=StringTake[text,{Round[StringLength[text]/2]+1,StringLength[text]}]
F=ToCharacterCode[str1] ;
G= ToCharacterCode[str2] ;
AccountingForm[Grid[Partition[F,9]]];
AccountingForm[Grid[Partition[G,9]]];
X=F;
Y=G;
iter=66;
α =Tan[0.12345112];
coding1 = NestList[Apply[Function[{x, y}, {−α y, x}], #]&, {x, y}, iter];
```

```
w1= SetPrecision[coding1[[iter,1]] ,9];
w2= SetPrecision[coding1[[iter,2]] ,9];
ScientificForm[w1,9];
ScientificForm[w2,9];
α1 = α;
recoding1= NestList[Apply[Function[{w1, w2}, {w2, α^(−1)w1}], #]&, {w1, w2}, iter];
StringJoin[Flatten[FromCharacterCode[Round[recoding1[[iter]]]]]]
```

3. Results and Discussion

3.1 A 2D Linear Map Derived from a Second Order QRT Difference Equation

Consider a second-order QRT difference equation that can be written in the following form (Quispel et al., 1991):

$$x_{n+2} = \frac{g_0\left(x_{n+1}\right) - x_n\ g_1\left(x_{n+1}\right)}{g_1\left(x_{n+1}\right) - x_n\ g_2\left(x_{n+1}\right)}, \tag{5}$$

where the $g_j,\ j = 0,1,2$ can be expressed as

$$\begin{pmatrix} g_0\left(x_{n+1}\right) \\ g_1\left(x_{n+1}\right) \\ g_2\left(x_{n+1}\right) \end{pmatrix} = A_0 \begin{pmatrix} x_n^2 \\ x_n \\ 1 \end{pmatrix} A_1 \begin{pmatrix} x_n^2 \\ x_n \\ 1 \end{pmatrix} \tag{6}$$

Note that A_0 and A_1 in Eq. (6) are 3×3 symmetric matrices defined as follows:

$$A_i = \begin{pmatrix} \alpha_i & \beta_i & \gamma_i \\ \beta_i & \epsilon_i & \zeta_i \\ \gamma_i & \zeta_i & \kappa_i \end{pmatrix}; i = 0,1. \tag{7}$$

Eq. (6) has an invariant/integral G, which means that $G(x_n, x_{n+1}) = G(x_{n+1}, x_{n+2})$. It can be expressed as the biquadratic polynomial ratio

$$G(x,y) = \frac{(\alpha_0 x^2 y^2 + \beta_0 (x^2 y + x y^2) + \gamma_0 (x^2 + y^2) + \varepsilon_0 (x^2 + y^2) + \sigma_0 (x + y) + \kappa_0)}{(\alpha_1 x^2 y^2 + \beta_1 (x^2 y + x y^2) + \gamma_1 (x^2 + y^2) + \varepsilon_1 (x^2 + y^2) + \sigma_1 (x + y) + \kappa_1)} \tag{8}$$

It should be noted that the properties of the QRT symmetric mapping above are reversible and (anti) measure-preserving.

Focus now on the second order QRT difference equation in Eq. (5) in the following special form

$$x_{n+2} = \frac{(\lambda - \mu\ x_{n+1}^2)}{x_n (x_{n+1}^2 - \mu)}; \quad \lambda, \mu \in \mathbb{R}. \tag{9}$$

Suppose that the symmetric matrices A_0 and A_1 in Eq. (7) are as follows:

$$A_0 = \begin{pmatrix} -1 & 0 & \mu \\ 0 & 0 & 0 \\ \mu & 0 & -\lambda \end{pmatrix}; \ A_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}. \tag{10}$$

Thus, the functions $g_i, i = 0,1,2$, in Eq. (6) are:

$$\begin{pmatrix} g_0\left(x_{n+1}\right) \\ g_1\left(x_{n+1}\right) \\ g_2\left(x_{n+1}\right) \end{pmatrix} = \begin{pmatrix} \lambda\, x_{n+1} - \mu\, x_{n+1}^3 \\ 0 \\ \mu\, x_{n+1} - x_{n+1}^3 \end{pmatrix} \tag{11}$$

Consider now a different case where the symmetric matrices A_0 and A_1 are as follows:

$$A_0 = \begin{pmatrix} 0 & -1 & \mu \\ -1 & 1 & -1 \\ \mu & -1 & 1 \end{pmatrix};\; A_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \tag{12}$$

Then the functions $g_j, j = 0,1,2$, are:

$$\begin{pmatrix} g_0\left(x_{n+1}\right) \\ g_1\left(x_{n+1}\right) \\ g_2\left(x_{n+1}\right) \end{pmatrix} = \begin{pmatrix} \lambda\, x_{n+1}^2 - \mu\, x_{n+1}^3 \\ 0 \\ \mu\, x_{n+1} - x_{n+1}^2 \end{pmatrix} \tag{13}$$

Using Eq. (12) and the function vector in Eq. (13), the special form of Eq. (5) becomes

$$x_{n+2} = \frac{x_{n+1}(\lambda - \mu\; x_{n+1})}{x_n(x_{n+1} - \mu)};\quad \lambda, \mu \in \mathbb{R} \tag{14}$$

Consider the second order QRT difference equation in Eq.(9). Let us write the equation as the map:

$$\mathbf{x}_{n+1} = \mathbf{f}_{(\mu,\lambda)}\left(\mathbf{x}_n\right), \tag{15}$$

where

$$\begin{aligned} \boldsymbol{f}_{(\lambda,\mu)}:\quad & \mathbb{R}^2 && \rightarrow \quad \mathbb{R}^2 \\ & (x_1, x_2) && \mapsto \quad \left(\frac{\lambda - \mu\; x_1^2}{x_2(x_1^2 - \mu)}, x_1\right) \end{aligned} \tag{16}$$

Consider the dynamic system in Eq.(16). Suppose $\left(x_1^*, x_2^*\right)$ is a fixed point of the dynamic system. Therefore, we have the following condition

$$\begin{pmatrix} x_1^* \\ x_2^* \end{pmatrix} = \begin{pmatrix} \left(\dfrac{\left(\lambda - \mu(x_1^*)^2\right)}{x_2^*\left((x_1^*)^2 - \mu\right)}\right) \\ x_1^* \end{pmatrix}. \tag{17}$$

Thus, there are two fixed points for the dynamic system in Eq.(16), namely:

$$\left(x_1^*, x_2^*\right) = \left\{\left(\lambda^{1/4}, \lambda^{1/4}\right), \left(-\lambda^{1/4}, -\lambda^{1/4}\right)\right\}, \tag{18}$$

The form of the Jacobian matrix for the dynamic system in Eq.(16) for fixed points in Eq.(18) is,

$$A=\begin{pmatrix} \dfrac{2\left(-\lambda+\mu^2\right)}{\left(\sqrt{\lambda}-\mu\right)^2} & \dfrac{-\lambda+\sqrt{\lambda}\mu}{\sqrt{\lambda}\left(\sqrt{\lambda}-\mu\right)} \\ 1 & 0 \end{pmatrix}, \qquad (19)$$

where the eigenvalues of the matrix A, $|\xi I-A|=0$, are

$$\xi_1=-\left(\frac{\lambda^{1/4}-\sqrt{\mu}}{\lambda^{1/4}+\sqrt{\mu}}\right) \text{ and } \xi_2=-\left(\frac{\lambda^{1/4}+\sqrt{\mu}}{\lambda^{1/4}-\sqrt{\mu}}\right), \qquad (20)$$

For the eigenvalues ξ_1 and ξ_2 in Eq. (20), the stability of the dynamical system in Eq. (16) can be explained as follows.

- If $\mu,\lambda>0$ and $0<\sqrt{\mu}<\lambda^{1/4}$, then $-1<\xi_1<0$ and $\xi_2<-1$ or $-1<\xi_2<0$ and $\xi_1<-1$. Thus the dynamic system in Eq.(16) is of type saddle (unstable).
- If $\mu,\lambda>0$ and $0<\lambda^{1/4}<\sqrt{\mu}$, then $1<\xi_1$and $0<\xi_2<1$or $1<\xi_2$ and $0<\xi_1<1$. Thus, the dynamical system in Eq. (16) is of type saddle and is unstable.
- If $\lambda>0$ and $\mu=0$ (or $\lambda=0$ and $\mu>0$), then $\xi_1=\xi_2=\pm1$. In other words, the eigenvalues ξ_1 and ξ_2 are exactly on the real axis of the unit circle in the complex plane. Thus, the dynamical system in Eq. (16) cannot be declared stable.
- If $\lambda>0$ and $\mu<0$, then ξ_1 and ξ_2 both are conjugate complex numbers with opposite modulus values. Thus, the dynamical system in Eq. (16) is of type centere and is stable.

Let $F\left(x_1,x_2\right)$ be a solution function γ_n for all $n\in\mathbb{N}$ for a dynamic system (16). It means that solution γ_n is at level set $F\left(x_1,x_2\right)$. The orbit of the solution for the dynamic system (16) is strongly influenced by the values of parameters λ and μ. For the value of parameter λ, we can check that the characteristics differ at the set level only at λ = -1, λ = 0, and λ = 1. Meanwhile, the value of the parameter μ gives a change in properties at a fixed point. We can check that, together with λ = 1, the value of μ varies from negative to positive, giving a change in the properties at a fixed point from the saddle point to the center point as it passes through zero.

Consider the matrix form of the Jacobian Equation (19). Select the parameter value λ =1. We do not discuss the other parameter values, λ = -1 and λ = 0, because they are imaginary and undefined values. Therefore, we obtain a special case of mapping in Equation (16), i.e.,

$$\begin{aligned} \boldsymbol{f}_{(1,\mu)}:\quad \mathbb{R}^2 &\rightarrow \mathbb{R}^2 \\ (x_1,x_2) &\mapsto \left(\frac{1-\mu\, x_1^2}{x_2(x_1^2-\mu)},x_1\right) \end{aligned} \qquad (21)$$

It is easy to check that the mapping in Eq. (17) has the integral

$$F(x_1,x_2)=\mu\left(\frac{x_1}{x_2}+\frac{x_2}{x_1}\right)-\left(x_1\,x_2+\frac{1}{x_1\,x_2}\right). \tag{22}$$

This mapping also has the following properties (see (Zakaria & Tuwankotta, 2020) for how to check these properties):

- One of the fixed points is (1,1).
- It is area-preserving.
- It is reversible.
- It is symmetric.

Note that the integral in Eq. (18) is linear in μ. Thus,

$$\mu=\mu(x_1,x_2)=\frac{\left(1+x_1^2\,x_2^2\right)}{\left(x_1^2+x_2^2\right)} \tag{23}$$

for all $(x_1,x_2)\in F(x_1,x_2)=0$. Substituting the expression in Eq. (23) into the mapping in (21), we have the following linear map

$$\left(x_1',x_2'\right)=\hat{\mathbf{f}}(x_1,x_2)=(-x_2,x_1) \tag{24}$$

with the integral

$$\hat{F}(x_1,x_2)=\frac{\left(1+x_1^2\,x_2^2\right)}{\left(x_1^2+x_2^2\right)}. \tag{25}$$

The linear map $\hat{\mathbf{f}}(x_1,x_2)$ has the following properties:

- The orbits of $\hat{\mathbf{f}}(x_1,x_2)$ are four-periodic.
- The function $\hat{\mathbf{f}}(x_1,x_2)$ is area-preserving, which means that there is a density $\hat{\rho}(x_1,x_2)$ such that

$$\left|D\hat{\mathbf{f}}(x_1,x_2)\right|=\frac{\hat{\rho}(x_1,x_2)}{\hat{\rho}\left(x_1',x_2'\right)}=1 \tag{26}$$

and

$$\hat{\rho}(x_1,x_2)=\frac{1}{x_1\,x_2}\left[\frac{\partial\hat{F}(x_1,x_2)}{\partial\mu}\right]^{-1}=\frac{1}{{x_1}^2+{x_2}^2}$$

- Consider $G_1(x_1,x_2)=(x_2,x_1)$. Note that $G_1(G_1(x_1,x_2))=G_1(x_2,x_1)=(x_1,x_2)$, which implies that $G_1(x_1,x_2)^{-1}=G_1(x_1,x_2)$. Since $G_1\circ\hat{f}\circ G_1^{-1}=\hat{f}^{-1}$, G_1 is a reversing symmetry for $\hat{f}$.

- There exists a symmetry $S_1\left(x_1,x_2\right)=\left(-x_1,-x_2\right)$ such that $S_1\circ\hat{f}\circ S_1^{-1}=\hat{f}$.

In addition, another linear map can be constructed based on the map form in Eq. (21) at the fixed point (1,1). First, we find the Jacobian matrix:

$$A=\begin{pmatrix}\dfrac{2\left(\mu^2-1\right)}{\left(1-\mu\right)^2} & -1\\ 1 & 0\end{pmatrix} \tag{27}$$

Then, for the QRT mapping in Eq. (21), we have a linear map around the fixed point $\left(1,1\right)$ as follows:

$$\begin{pmatrix}x_1'\\ x_2'\end{pmatrix}=\begin{pmatrix}\dfrac{2\left(\mu^2-1\right)}{\left(1-\mu\right)^2} & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}x_1\\ x_2\end{pmatrix} \tag{28}$$

In the next section, we will use the map in Eq. (28) to construct a cryptographic algorithm for the digital image. We use Mathematica® scripts to implement our proposed encryption-description algorithm. In addition, we compare the encryption-decryption results of the map in Eq. (28) and the 2D mKdV linear map described below (see (Zakaria et al., 2021) and (Yuliani et al., 2021) for the construction of the 2D mKdV linear map):

$$\begin{pmatrix}x_1'\\ x_2'\end{pmatrix}=\begin{pmatrix}-1.68064 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}x_1\\ x_2\end{pmatrix} \tag{29}$$

3.2 Encryption-Decryption Algorithm for Image Cryptography Based on a 2D QRT Linear Map

Let us consider the two original (plain) images presented in Figure 1. The left side in Figure 1 represents a fractal image. This image was obtained from the following 2D complex computational mapping process:

$$f\ :\left(x,y\right)\mapsto\left(y,\left(\frac{\left(0.5+0.95y^2\right)}{x\left(y^2-0.95\right)}\right)^2+k\right), \tag{30}$$

where $k=a+\mathbf{i}b$ for $a\in\left[-1.25,1.25\right]$ and $b\in\left[-2.25,2.25\right]$, $\left(x_0,y_0\right)=\left(1.01,1.01\right)$, $r=\ 20$ iterations, and $\left|x\right|<3$ and $\left|y\right|<3$ at an image resolution of 200 dpi. Meanwhile, the right side in Figure 1 represents a non-fractal image (Lena.JPG).

The images in Figure 1 will be encoded using 2D linear maps (QRT in Eq. (28) and mKdV in Eq. (29)) based on the scheme in Figures 2 and 3. A Mathematica® script discussed on the Mathematica® Stack Exchange (Estner, 2019) can be used to implement QRT based on the encryption-decryption algorithm. Using the fractal and non-fractal images in Figure 1 as the two plain images, four cipher images have been obtained via QRT and mKdV. The cipher images are shown in Figures 4 and 5.

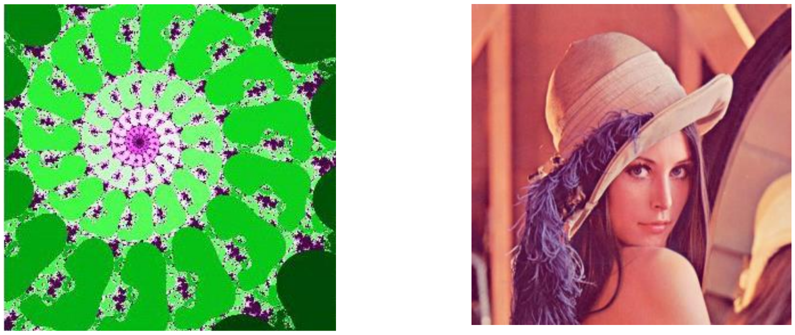

Figure 1. Examples of plain images: a fractal image (left), and a non-fractal image (right).

Consider the image encryption-decryption scheme described in Figures 2 and 3 below.

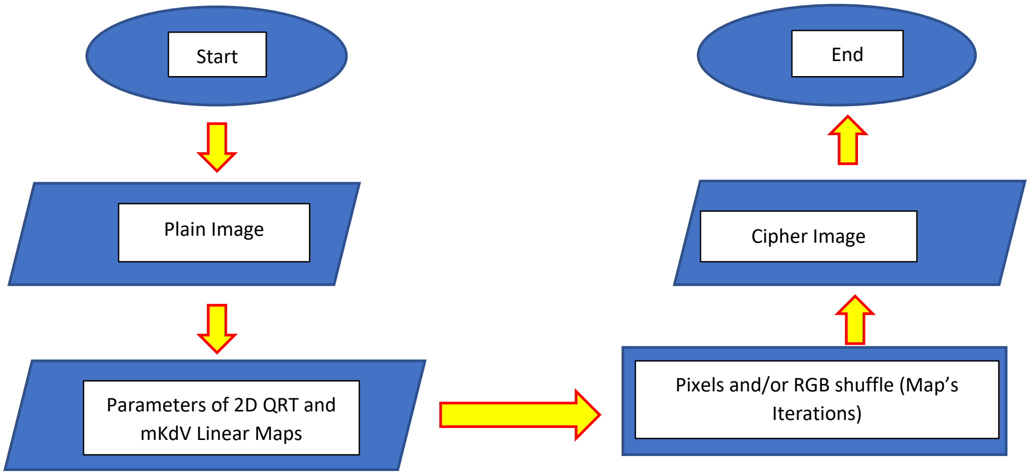
Start
Plain Image
Parameters of 2D QRT and mKdV Linear Maps
Pixels and/or RGB shuffle (Map’s Iterations)
Cipher Image
End

Figure 2. A flow chart for the proposed encryption algorithm.

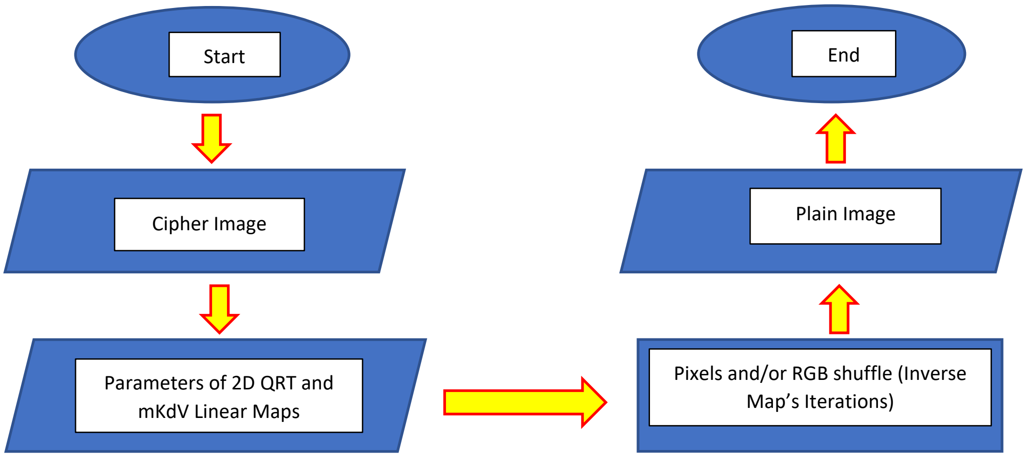
Start
Cipher Image
Parameters of 2D QRT and mKdV Linear Maps
Pixels and/or RGB shuffle (Inverse Map’s Iterations)
Plain Image
End

Figure 3. A flow chart for the proposed decryption algorithm.

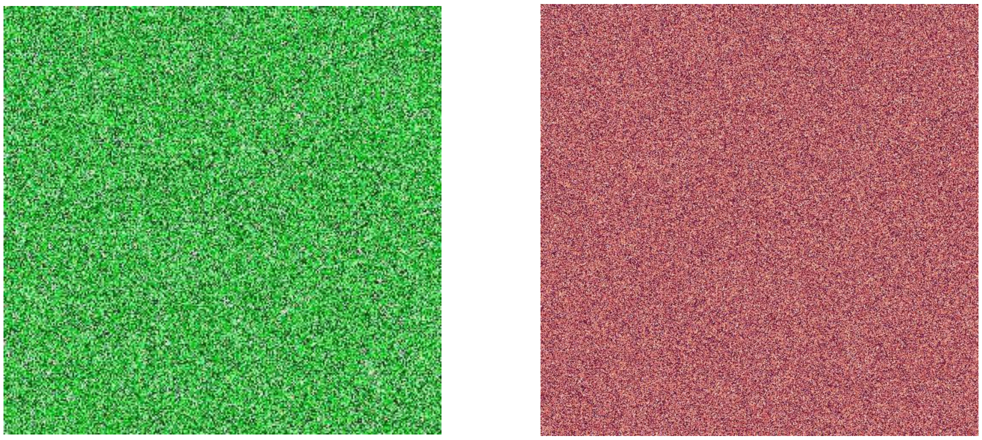

Figure 4. The cipher fractal image (left) and non-fractal image (right) from Figure 1 after using the 2D mKdV linear map in Eq. (29) for $r = 130$ iterations.

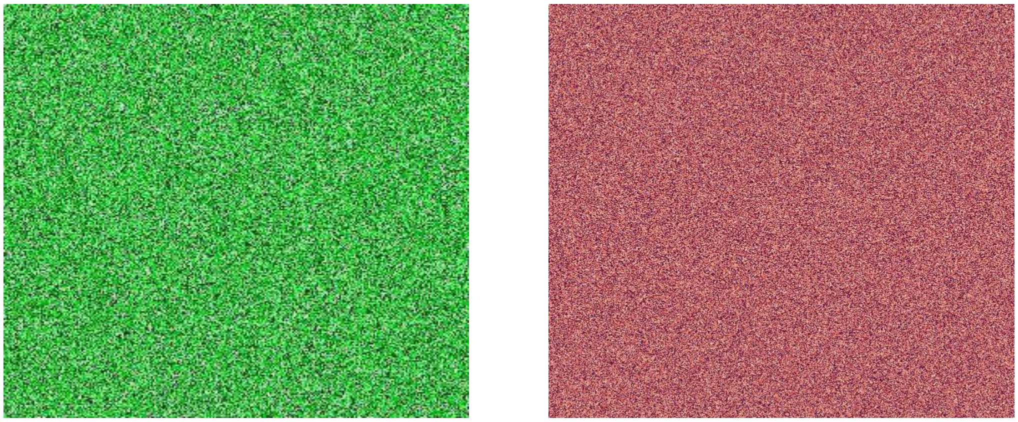

Figure 5. The cipher fractal image (left) and non-fractal image (right) from Figure 1 after using the 2D QRT linear map from Eq. (28) with $\mu = 0.15$ and $r = 130$ iterations.

3.3 Covariance, Correlation, and Histogram Computations Based on Weighted Pixel Data

There are two main tools that are used in cryptographic image data processing, i.e., the gradient and gradient orientation filters. The gradient filter provides an image corresponding to the magnitude of the image gradient, which is computed using discrete derivatives of a Gaussian of the pixel radius. Meanwhile, the gradient orientation filter provides an image corresponding to the local orientation, parallel to the image gradient, which is computed using discrete derivatives of a Gaussian of the pixel radius and returns values between $-\pi/2$ and $\pi/2$ (Wolfram Research Inc., 2019).

At first glance, the results of the randomization of the original image pixels using 2D QRT and 2D mKdV shown in Figures 4 and 5 look similar but there are differences that come to light in the pixel correlations and covariances (see Tables 1 and 2).

Table 1. Covariances and correlations for the fractal image (Figure 1 on the left side) data based on the weighted data (gradient orientation filter, gradient filter) images.

	Covariance	Correlation
Cipher Image Produced by Eq. (28) for $\mu = 1.5$	0.0005867	0.0309571
Cipher Image Produced by Eq. (28) for $\mu = 0.5$	-0.0003468	-0.0156929
Cipher Image Produced by Eq. (28) for $\mu = 0.15$	-0.0000320	-0.0014339
Cipher Image Produced by Eq. (29)	-0.0000799	0.00337083

Table 2. Covariances and correlations of the non-fractal image (Figure 1 on the right side) data based on the weighted data (gradient orientation filter, gradient filter) images.

	Covariance	Correlation
Cipher Image Produced by Eq. (28) for $\mu = 1.5$	-0.0010140	-0.0668513
Cipher Image Produced by Eq. (28) for $\mu = 0.5$	-0.0000642	-0.0038384
Cipher Image Produced by Eq. (28) for $\mu = 0.15$	0.0000115	0.0006486
Cipher Image Produced by Eq. (29)	-0.0000596	-0.0032443

The important analyses in image cryptography are the histograms, covariance, and correlation analyses. A histogram analysis is conducted to examine the pixel distribution. In general, the smaller the histogram variance, the more secure the encrypted image is. In addition, if a method has a much smaller histogram mean-variance than the other, then the method has better performance (see (Tang et al., 2019), (Fu et al., 2016) and (Gao et al., 2006)). The distribution of the image's pixel values prior to encryption is usually concentrated on the highest space value. Therefore, the best encryption systems spread the pixel values over the pixel space.

Mathematica® programming is used to produce histograms for 2D QRT and mKdV encryption. The four histograms of the weighted data for the images shown in Figure 1 are shown in Figures 6 and 7. There are differences between the histograms for the cipher images produced by QRT mapping and the images resulting from mKdV mapping in both figures. Generally, the histograms generated for the fractal image are flat (uniform).

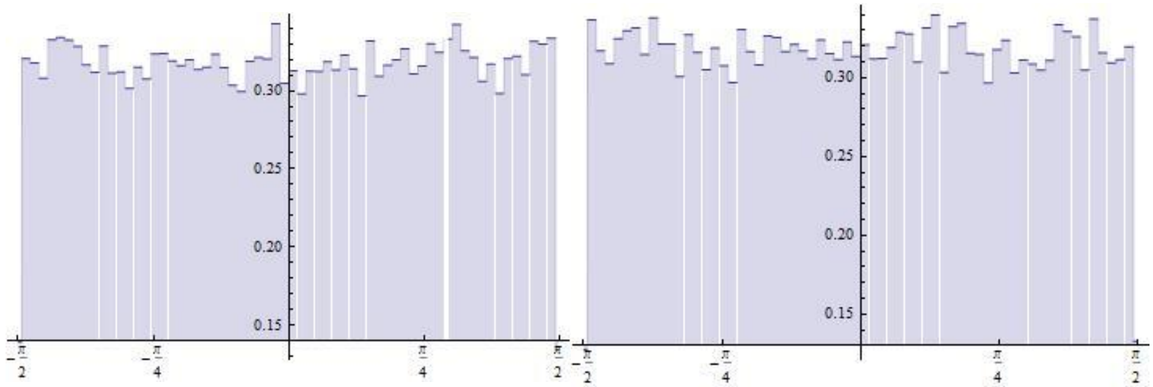

Figure 6. Cipher image histograms based on the weighted data for the fractal image (Figure 1 on the left side): after encryption with the 2D QRT linear map in Eq. (28) (left) for $\mu = 0.15$, and after encryption with the 2D mKdV linear map in Eq. (29) (right).

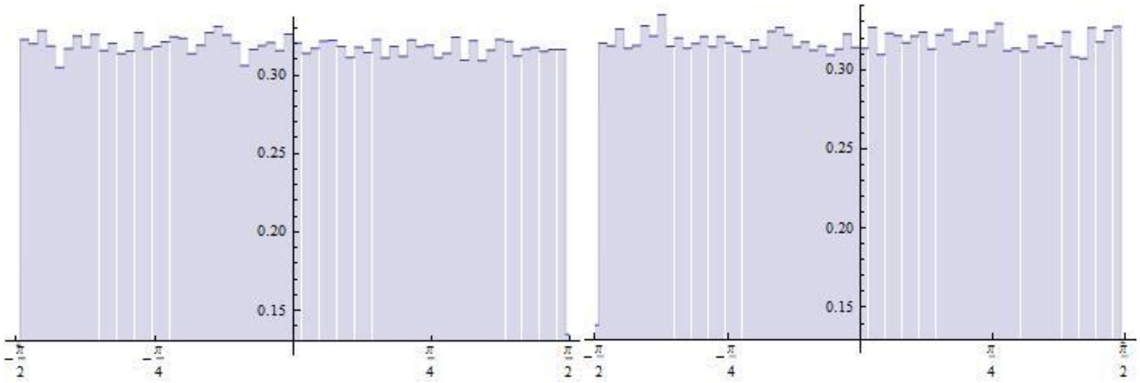

Figure 7. Cipher image histograms based on weighted data for the non-fractal image (Figure 1 on the right side): after encryption with the 2D QRT linear map in Eq. (28) (left)) for $\mu = 0.15$, and after encryption with the 2D mKdV linear map in Eq. (29) (right).

4. Conclusions

We have presented an approach using a 2D linear map scheme constructed from a second-order QRT difference equation for the cryptographic encoding of text and images. Then we have also shown that by using reversible and area-preserving mapping, the return of the encoded text is obtained quickly. In addition, the proposed 2D linear map scheme also results in better image cryptographic encoding than mKdV maps for non-fractal images based on the calculated covariance and correlation. With regard to the use of secret keys for encryption and decryption, our proposed 2D linear map scheme has used a similar secret key. Therefore, a further research idea can be carried out on using other types of secret keys, such as private keys based on the concept of a new automated cryptosystem based on Boolean algebra (see (Ahmad & Rushdi, 2018) for concept details). As for the security analysis of the proposed encryption algorithm, we will carry out crucial future work such as key sensitivity tests, statistical analysis, differential analysis, entropy analysis, and randomness analysis (see (Tang et al., 2019) for the concept of image security analysis.).

Conflict of Interest

The authors confirm that there is no conflict of interest to declare for this publication.

Acknowledgments

The first and the last authors would like to thank Universitas Lampung for the facilities, funding, and support made available through BLU Research Grant No. 1668/UN26.21/PN/2021. The first author expresses sincere thanks to Prof. La Zakaria for the valuable discussion.

References

Abbadi, N.K.E., Yahya, E., & Aladilee, A. (2017). Digital RGB image encryption based on 2D cat map and shadow numbers. *2017 Annual Conference on New Trends in Information and Communications Technology Applications, NTICT 2017, March*, pp. 162–167. https://doi.org/10.1109/NTICT.2017.7976115

Abbas, N.A. (2016). Image encryption based on independent component analysis and arnold's cat map. *March*. https://doi.org/10.1016/j.eij.2015.10.001

Ali Abaas, S., & Kareem Shibeeb, A. (2015). A new approach for video encryption based on modified AES algorithm. *IOSR Journal of Computer Engineering (IOSR-JCE)*, *17*(*3*), pp. 44–51. https://doi.org/10.9790/0661-17364451

Denning, D.E. (1982). Cryptography and data security. In *Addison-Wesley Publishing Company*. http://portal.acm.org/citation.cfm?id=SERIES11430.539308

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *196 LNCS*, pp. 10–18. https://doi.org/10.1007/3-540-39568-7_2

Estner, N. (2019). *Implementing Arnold's Cat Map*. https://mathematica.stackexchange.com/questions/164070/implementing-arnolds-cat-map

Fan, H., Li, M., Liu, D., & Zhang, E. (2018). Cryptanalysis of a colour image encryption using chaotic APFM nonlinear adaptive filter. *Signal Processing*, *143*, pp. 28–41. https://doi.org/10.1016/j.sigpro.2017.08.018

Fan, H., Zhang, C., Lu, H., Li, M., & Liu, Y. (2022). Cryptanalysis of an image encryption algorithm based on random walk and hyperchaotic systems. *Entropy*, *24*(*40*), p. 17. https://doi.org/10.3390/e24010040

Fu, C., Chen, Z., Zhao, W., & Jiang, H.Y. (2017). A new fast color image encryption scheme using chen chaotic system. In T. Hochin, H. Hirata, & N. Hiroki (Eds.), *18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing* (pp. 121–126). *IEEE Computer Society*. https://doi.org/10.1109/SNPD.2017.8022710

Fu, C., Wen, Z.K., Zhu, Z.L., & Yu, H. (2016). A security improved image encryption scheme based on chaotic Baker map and hyperchaotic Lorenz system. *International Journal of Computational Science and Engineering*, *12*(*2–3*), pp. 113–123. https://doi.org/10.1504/IJCSE.2016.076212

Gao, H., Zhang, Y., Liang, S., & Li, D. (2006). A new chaotic algorithm for image encryption. *Chaos, Solitons and Fractals*, *29*, pp. 393–399. https://doi.org/10.1016/j.chaos.2005.08.110

Hidayat, A. D., & Afrianto, I. (2017). Sistem kriptografi citra digital pada jaringan intranet menggunakan metode kombinasi chaos map dan teknik selektif. *Jurnal ULTIMATICS*, *9*(*1*), pp. 59–66. https://doi.org/10.31937/ti.v9i1.565

Li, M., Wang, P., Yue, Y., & Liu, Y. (2021). Cryptanalysis of a secure image encryption scheme based on a novel 2D sine–cosine cross-chaotic map. *Journal of Real-Time Image Processing*, *18*, pp. 1–18. https://doi.org/10.1007/s11554-021-01091-1

Li, Z., Peng, C., Li, L., & Zhu, X. (2018). A novel plaintext-related image encryption scheme using hyper-chaotic system. *Nonlinear Dyn*, *94*, pp. 1319–1333. https://doi.org/10.1007/s11071-018-4426-4

Munir, R. (2012). Robustness analysis of selective image encryption algorithm based on arnold cat map permutation. *Proceedings of 3rd Makassar International Conference on Electrical Engineering and Informatics*, *December*, pp. 1–5.

Munir, R. (2015). Algoritma enkripsi selektif citra digital dalam ranah frekuensi berbasis permutasi chaos. *Jurnal Rekayasa Elektrika*, *10*(*2*), pp. 66–72. https://doi.org/10.17529/jre.v10i2.82

Notiragayu, & Zakaria, L. (2019). The implementation of digital text coding algorithm through a three dimensional mapping derived from generalized ΔΔ-mKdV equation using mathematica. *Journal of Physics: Conference Series*, *1338*(*1*). https://doi.org/10.1088/1742-6596/1338/1/012041

Quispel, G. R. W., Capel, H. W., Papageorgiou, V. G., & Nijhoff, F. W. (1991). Integrable mappings derived from soliton equations. *Physica A*, *173*(*1–2*), pp. 243–266. https://doi.org/10.1016/0378-4371(91)90258-E

Quispel, G. R. W., & Roberts, J. A. . (1988). Reversible mappings of the plane. *Physics Letters A*, *132*(*4*), pp. 161–163. https://doi.org/10.1016/0375-9601(88)90274-5

Quispel, G. R. W., & Roberts, J. A. . (1989). Conservative and dissipative behaviour in reversible dynamical systems. *Physics Letters A*, *135*(6–7), pp. 337–342. https://doi.org/10.1016/0375-9601(89)90004-2

Revanna, C. R., & Keshavamurthy, C. (2017). A secure document image encryption using mixed chaotic system. *International Journal of Computer Science and Information Security*, *15*(*3*), pp. 263–270.

Ronsen, P., Halim, A., & Syahputra, I. (2014). Enkripsi citra digital menggunakan arnold’s cat map dan nonlinear chaotic algorithm. *JSM STMIK Mikroskil*, *15*(*2*), pp. 61–71.

Shifrin, L. (2008). *Mathematica® Programming: an Advanced Introduction*. https://www.mathprogramming-intro.org/download/MathProgrammingIntro.pdf

Soleymani, A., Nordin, M. J., & Sundararajan, E. (2014). *A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map*. *2014*, pp. 1–21. https://doi.org/10.1155/2014/536930

Tang, Z., Yang, Y., Xu, S., Yu, C., & Zhang, X. (2019). Image encryption with double spiral scans and chaotic maps. *Security and Communication Networks*, *2019*, p. 15. https://doi.org/10.1155/2019/8694678

Wellin, P. (2016). Essentials of programming in mathematica ® . In *Essentials of Programming in Mathematica* ® . https://doi.org/10.1017/cbo9781316337738

Wolfram Research Inc. (2019). Mathematica 12.0. In *Wolfram Research*.

Yuliani, E., Zakaria, L., & Asmiati, A. (2021). A two-dimensional map derived from an ordinary difference equation of mKdV and its properties. *Journal of Physics: Conference Series*, *1751*, pp. 1–5. https://doi.org/10.1088/1742-6596/1751/1/012010

Zakaria, L., & Tuwankotta, J. M. (2016). Dynamics and bifurcations in a two-dimensional map derived from a generalized ΔΔ-sine gordon equation. *Far East Journal of Dynamical Systems*, *28*(*3*), pp. 165–194. https://doi.org/10.17654/ds028030165

Zakaria, L., & Tuwankotta, J. M. (2020). Dynamics of a re-parametrization of a 2-dimensional mapping derived from double discrete sine-Gordon mapping. *International Journal of Mathematical, Engineering and Management Sciences*, *5*(*2*). https://doi.org/10.33889/IJMEMS.2020.5.2.030

Zakaria, L., Yuliani, E., & Asmiati, A. (2021). A two-dimensional mKdV linear map and its application in digital image cryptography. *Algorithms*, *14*(*4*), pp. 1–18. https://doi.org/10.3390/a14040124